УДК 004.056.53
DOI: 10.15587/2312-8372.2016.75118

Сидоренко В. В.,
Буравченко К. О.

РОЗРОБКА СПОСОБУ ОРГАНІЗАЦІЇ ЗАХИЩЕНОГО КАНАЛУ ПЕРЕДАЧІ ДАНИХ У СИСТЕМІ ДИСПЕТЧЕРИЗАЦІЇ ВОДОПОСТАЧАННЯ

У роботі розроблено спосіб організації захищеного каналу передачі даних про стан об'єкта водопостачання у реальному часі з використанням бездротових технологій. Продемонстровано можливість роботи системи диспетчеризації з використанням лише однієї глобальної статичної IP-адреси у сервера збору даних. Запропоновано використовувати одноплатний комп'ютер з операційною системою на точці збору сигналів.

Ключові слова: *диспетчеризація, система водопостачання, бездротовий зв'язок, одноплатний комп'ютер.*

1. Вступ

Для забезпечення заданих показників технологічного процесу системи водопостачання оснащують автоматизованими системами керування. До задач системи керування водопостачанням входять стабілізація тиску та подачі води, рівнів у резервуарах, які довільно змінюються під дією випадкових факторів, оптимізація режимів роботи насосних станцій (зменшення витрати енергії, збільшення моторесурсу та ін.), реакція на аварійні ситуації і т. д. Важливими факторами, при автоматизації системи водопостачання є:

— високий ступінь відповідальності;
— робота системи в умовах змінного навантаження;
— розподілена у просторі система та необхідність координації із центру;
— складність технологічного процесу водопостачання, обумовленого стохастичним споживанням води, запізненням сигналу керування, недостатністю інформації про стан об'єкту;
— необхідність забезпечення економної роботи насосних агрегатів;
— необхідність збереження функціонування системи в цілому у випадках аварій окремих ланок.

Важливого значення для системи керування водопостачанням набуває система диспетчеризації технологічного процесу, як складова АСК ТП водопостачання. Своєчасне отримання інформації про стан системи дозволяє збільшити оперативність роботи водоканалів, зменшити витоки води, швидко ліквідувати аварійні ситуації, тощо. В умовах густого заселення міст та розподіленої структури системи водопостачання, для передачі даних все частіше використовується бездротовий зв'язок [1]. З масовим поширенням GSM, 3G та стандарту IEEE 802.11 зв'язку, такий спосіб є значно дешевшим та швидшим для впровадження у порівнянні з дротовим зв'язком. Недоліком таких систем є те, що дані проходять через сервери провайдерів і можливе їх перехоплення у радіо ефірі зловмисниками. Актуальною задачею є впровадження засобів захисту інформації у системах диспетчеризації технологічними процесами водопостачання з використанням сучасного обладнання.

2. Об'єкт дослідження та його технологічний аудит

Об'єкт дослідження — процес збору інформації про стан об'єкту водопостачання. Система водопостачання є розподіленою у просторі системою, яка вимагає складної системи збору інформації про її стан [2]. В загальному випадку насосні станції виконують задачу підтримання тиску у системі водопостачання для забезпечення споживачів водою [3].

Для збору інформації використовують структуру наступного виду (рис. 1).

Рис. 1. Структурна схема системи збору даних про стан системи водопостачання

Недоліком такої системи є те, що при передачі інформації через мережу Інтернет вона передаються у незахищеному вигляді і може бути перехоплена зловмисниками. Крім того обчислювальні ресурси, що використовуються на точках збору сигналів не дозволяють реалізувати сучасні стійкі до атак алгоритми шифрування.

3. Мета та задачі дослідження

Метою дослідження є забезпечення захисту інформації у системі диспетчеризації технологічним процесом водопостачання, яка передається у бездротових мережах.

Для досягнення поставленої мети необхідно виконати *такі задачі*:

— дослідити архітектуру системи диспетчеризації водопостачання;

— розробити архітектуру системи передачі даних у бездротовій мережі, яка забезпечує захист конфіденційної інформації від зловмисників.

4. Аналіз літературних даних

Автором [4] наведено огляд популярних сьогодні промислових стандартів бездротової передачі даних. Акцентовано увагу на стандарті ZigBee, як найбільш економному та надійному способі створення великої та простої бездротової мережі. У роботах [5, 6] наведено методи побудови захищеної системи передачі даних у Scada системах водопостачання. Розглянуто атаки на процес регулювання тиску, шляхом підміни даних від датчиків. Крім того розглянуто методи захисту інформації у промислових системах контролю та автоматики на основі моделі спостерігачів. Кожен спостерігач налаштовано на виявлення тільки одного типу атаки, що є економічно вигідним у порівнянні з іншими методами. У статі [7] приведено структуру системи визначення pH води у реальному часі за допомогою передачі даних по GSM. Використано смартфони для збору даних з датчиків pH. Переваги запропонованого способу в тому, що ціна такої системи дуже низька. Принципи захисту промислових систем автоматики від кібератак та шляхи їх впровадження розглянуті у роботах [8–10].

5. Матеріали та методи дослідження

Методи дослідження, використані в роботі, базуються на положеннях теорії захисту інформації при дослідженні та аналізі системи диспетчеризації водопостачання. Зокрема обрано алгоритм асиметричного шифрування RSA з відкритим ключем, який є широко уживаним та відкритим, а також реалізується на операційних системах.

6. Результати дослідження

Сучасний розвиток технологій бездротової передачі даних дозволяє отримувати інформації про стан системи водопостачання у реальному часі. Існує велика кількість промислових модемів [13], які підтримують стандарти GSM, 3G та 4G. Передача даних відбувається за допомогою частотної модуляції і цифровим каналам [14]. Впровадження таких систем передачі даних у промисловості у порівнянні з дротовими є більш дешевим та займає менше часу.

Недоліком є те, що проблемі захисту інформації у бездротових мережах, які використовуються у автоматизації технологічних процесів приділено не достатньо уваги.

У статі запропоновано метод організації безпечного каналу передачі даних в системі диспетчеризації технологічними процесами з використанням бездротової мережі GSM.

Розглянемо систему збору даних від датчиків (рис. 2).

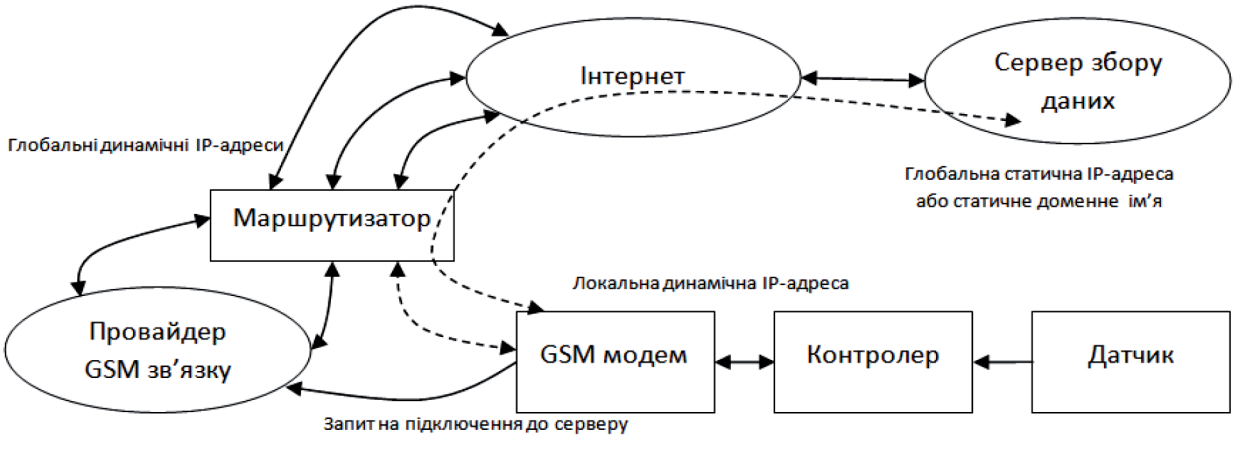

Рис. 2. Структурна схема системи збору даних від датчиків на базі GSM зв'язку

У роботах [11, 12] показано вектори атак на системи керування технологічними процесами та причини їх виникнення.

Аналіз літератури показує, що переважна більшість авторів зосереджується на виявлені атак на систему зі сторони зловмисників та методи їх попередження, мало уваги у роботах приділено проблемі захисту інформації за допомогою шифрування. Проблема в тому, що сучасні промислові Scada системи та обладнання передачі даних створено без урахування потенційних загроз перехоплення інформації. Недостатньо розглянуто проблему захисту інформації про стан промислових систем, які розподілені у просторі, зокрема, систем водопостачання, а дані в них передаються по бездротових системах.

Сигнал від датчику обробляється контролером, до якого підключено GSM модем. Дані передаються за допомогою модему по GSM зв'язку, використовуючи GPRS. Провайдер мобільного зв'язку дозволяє отримати доступ до мережі Інтернет і створити TCP-сесію з сервером. Маршрутизатор провайдера забороняє вхідні підключення з зовнішніх IP. А модем отримує тільки локальну IP-адресу у мережі провайдера. Для віддаленого збору інформації по такій схемі необхідне створення TCP тунелю. Протокол TCP/IP має клієнт-серверну модель і для організації сесії сервер повинен мати статичну IP адресу або статичне доменне ім'я. Можливі два варіанти організації збору інформації з датчиків: коли вузол збору є TCP-клієнтом або вузол збору є TCP-сервером.

Для організації передачі даних запропоновано використати один сервер збору інформації, на якому встановлено базу даних. До серверу асинхронно підключаються клієнти і по протоколу TCP/IP передають пакети. Формат пакету залежить від набору параметрів, які були отримані з датчиків тиску. Асиметричне шифрування RSA [15] дозволяє забезпечити захист інформації від зловмисників. Спосіб дозволяє, використовуючи одноплатний комп'ютер, наприклад, Raspberry Pi, з встановленою операційною системою Linux організувати захищений канал збору даних від віддалених пристроїв.

У операційній системі Linux не складно за допомогою різноманітних бібліотек реалізувати алгоритм шифрування даних і згодом розшифрувати їх на сервері.

Функціональна схема системи передачі даних наведена на рис. 3.

безперервну передачу даних у реальному часі. Спосіб, який використовує одноплатний комп'ютер у якості контролера є кросплатформеним і не залежить від реалізації операційної системи. Для побудови системи збору даних використовується лише одна статична IP-адреса або доменне ім'я.

Недоліком системи передачі даних на основі бездротових технологій є ненадійність передачі даних у місцях, де є низький рівень сигналу базових станцій оператора мобільного зв'язку. Крім того для реалізації алгоритмів шифрування необхідна наявність обчислювальних потужностей та додаткові економічні витрати.

Можливості. Для зменшення вартості такої системи доцільно провести дослідження на можливість реалізації алгоритмів шифрування на мікроконтролерах, які не потребують використання операційної системи.

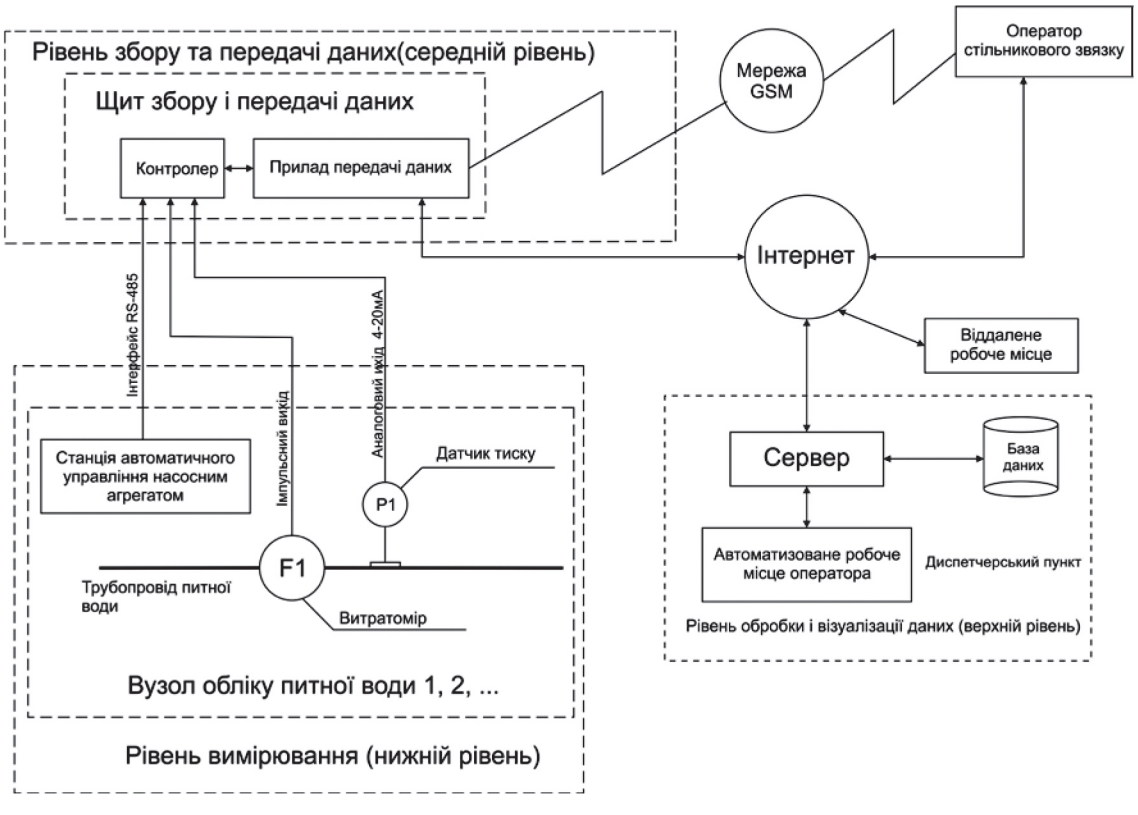

Рис. 3. Структурна схема диспетчерського контролю системи водопостачання

За допомогою датчику тиску та витратоміра води контролер отримує інформацію про поточний розбір води споживачами, а зі станції автоматичного керування визначається споживання електричної енергії, частоту обертів насосу, задачу тиску та ін. Масив даних потрапляє на контролер і за допомогою приладу передачі даних передається через GSM зв'язок до мережі Інтернет. На сервері дані обробляються та зберігаються у базу.

7. SWOT-аналіз результатів дослідження

Переваги. На відміну від існуючих систем диспетчеризації водопостачання канал передачі даних шифрується за допомогою асиметричного шифрування з відкритим ключем. Використання технологій пакетної передачі GPRS та 3G на відміну від CSD дозволяє створити

Загрози. Використання одноплатних комп'ютерів у системах диспетчеризації технологічними процесами не є дуже великим. Здебільшого перевагу віддають програмованим логічним контролерам та Scada системам, що є більш надійними, широко розповсюдженими та уніфікованими.

8. Висновки

У результаті проведених досліджень вирішено наступні задачі:

1. Досліджено архітектуру систем диспетчеризації водопостачання і показано, що на даний час більш прийнятним для використання каналу передачі даних є бездротовий канал.

2. Для забезпечення захищеного каналу передачі даних запропоновано використовувати одноплатні

комп'ютери з операційною системою на точках збору сигналів та шифрувати дані на основі асиметричного шифрування.

Література

1. Романов, В. О. Розподілена система збору і обробки інформації на базі інтелектуальних портативних приладів [Текст] / В. О. Романов, І. Б. Галелюка, В. М. Груша, П. П. Чернега // Комп'ютерні засоби, мережі та системи. — 2009. — № 8. — С. 64–72.
2. Сидоренко, В. В. Аналіз причин коливання тиску у системах водопостачання з метою їх мінімізації [Текст] / В. В. Сидоренко, К. О. Буравченко // Збірник наукових праць Національного університету кораблебудування імені адмірала Макарова. — 2015. — № 28(460). — С. 113–117.
3. Буравченко, К. О. Дослідження та аналіз динаміки процесу регулювання насосним агрегатом [Текст] / К. О. Буравченко // Технологічний аудит та резерви виробництва. — 2016. — № 3/2(29). — С. 15–19. doi:10.15587/2312-8372.2016.71878
4. Козлов, А. Промышленные стандарты беспроводной передачи данных [Текст] / А. Козлов // Chip News Украина. — 2008. — № 7. — С. 18–21.
5. Amin, S. Cyber Security of Water SCADA Systems — Part I: Analysis and Experimentation of Stealthy Deception Attacks [Text] / S. Amin, X. Litrico, S. Sastry, A. M. Bayen // IEEE Transactions on Control Systems Technology. — 2013. — Vol. 21, № 5. — P. 1963–1970. doi:10.1109/tcst.2012.2211873
6. Amin, S. Cyber Security of Water SCADA Systems — Part II: Attack Detection Using Enhanced Hydrodynamic Models [Text] / S. Amin, X. Litrico, S. S. Sastry, A. M. Bayen // IEEE Transactions on Control Systems Technology. — 2013. — Vol. 21, № 5. — P. 1679–1693. doi:10.1109/tcst.2012.2211874
7. Hossain, M. A. Early warning smartphone diagnostics for water security and analysis using real-time pH mapping [Text] / M. A. Hossain, J. Canning, S. Ast, P. J. Rutledge, A. Jamalipour // Photonic Sensors. — 2015. — Vol. 5, № 4. — P. 289–297. doi:10.1007/s13320-015-0256-x
8. Morris, T. H. Industrial control system cyber attacks [Text] / T. H. Morris, G. Wei // Proceedings of the 1st International Symposium on ICS & SCADA Cyber Security Research 2013. — BCS, 2013. — P. 22–29.
9. Peng, Y. Industrial control system cybersecurity research [Text] / Y. Peng, C. Q. Chang, F. Xie, Z. H. Dai et al. // Journal of Tsinghua University Science and Technology. — 2012. — Vol. 52, № 10. — P. 1396–1408.
10. Zheng, Y. Cyber Security Risk Assessment for Industrial Automation Platform [Text] / Y. Zheng, S. Zheng // 2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP). — Institute of Electrical & Electronics Engineers (IEEE), 2015. — P. 341–344. doi:10.1109/iih-msp.2015.58
11. Pasqualetti, F. Attack Detection and Identification in Cyber-Physical Systems [Text] / F. Pasqualetti, F. Dorfler, F. Bullo // IEEE Transactions on Automatic Control. — 2013. — Vol. 58, № 11. — P. 2715–2729. doi:10.1109/tac.2013.2266831
12. Pasqualetti, F. Secure control systems: A control-theoretic approach to cyber-physical security [Electronic resource]: A Dissertation submitted in partial satisfaction of the requirements for the degree of Doctor of Philosophy in Mechanical Engineering / F. Pasqualetti. — Santa Barbara: University of California, September 2012. — Available at: \www/URL: http://www.dsi.unifi.it/users/chisci/essc/phd-Pasqualetti-sep12.pdf. — 11.07.2016.
13. Nirmal, S. A. Location Based Industrial Monitoring & System Using 3G Wireless Technology [Text] / S. A. Nirmal, A. W. Mudasser, S. V. Altaf // International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering. — January 2014. — Vol. 2, № 1. — Available at: \www/URL: http://www.ijireeice.com/upload/2014/january/IJIREEICE2D_s_sanket_LOCATION.pdf. — 11.07.2016.
14. Benedetto, S. Principles of Digital Transmission: With Wireless Applications [Text] / S. Benedetto, E. Biglieri. — Springer Science & Business Media, 2002. — 855 p. doi:10.1007/b117711
15. Jonsson, J. Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1 [Electronic resource]: Report / J. Jonsson, B. Kaliski. — February 2003. — Available at: \www/URL: https://www.rfc-editor.org/rfc/rfc3447.txt. doi:10.17487/rfc3447

РАЗРАБОТКА СПОСОБА ОРГАНИЗАЦИИ ЗАЩИЩЕННОГО КАНАЛА ПЕРЕДАЧИ ДАННЫХ В СИСТЕМЕ ДИСПЕТЧЕРИЗАЦИИ ВОДОСНАБЖЕНИЯ

В работе разработан способ организации защищенного канала передачи данных о состоянии объекта водоснабжения в реальном времени с использованием беспроводных технологий. Продемонстрирована возможность работы системы диспетчеризации с использованием только одного глобального статического IP-адреса у сервера сбора данных. Предложено использовать одноплатный компьютер с операционной системой на точке сбора сигналов.

Ключевые слова: диспетчеризация, система водоснабжения, беспроводная связь, одноплатный компьютер.

Сидоренко Володимир Володимирович, *доктор технічних наук, професор, кафедра програмування та захисту інформації, Кіровоградський національний технічний університет, Україна.*

Буравченко Костянтин Олегович, *асистент, кафедра програмування та захисту інформації, Кіровоградський національний технічний університет, Україна,* ***e-mail: buravchenkok@gmail.com****.*

Сидоренко Владимир Владимирович, *доктор технических наук, профессор, кафедра программирования и защиты информации, Кировоградский национальный технический университет, Украина.*

Буравченко Константин Олегович, *ассистент, кафедра программирования и защиты информации, Кировоградский национальный технический университет, Украина.*

Sydorenko Volodymyr, *Kirovohrad National Technical University, Ukraine.*

Buravchenko Kostyantyn, *Kirovohrad National Technical University, Ukraine,* ***e-mail: buravchenkok@gmail.com***