ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

УДК 004.9 doi:10.20998/2413-4295.2018.16.17

ДЕЯКІ ПИТАННЯ ЗАПОБІГАННЯ ІНЦИДЕНТАМ ПРИ ЗОВНІШНІХ КІБЕРАТАКАХ НА АВТОМАТИЗОВАНУ СИСТЕМУ КЕРУВАННЯ КОТЛОАГРЕГАТОМ СИСТЕМИ ОПАЛЕННЯ

Ю. Є. ГРУДЗИНСЬКИЙ*, Д. Ю. ХАРЧЕНКО

кафедра автоматизації теплоенергетичних процесів Національного технічного університету України "Київський політехнічний інститут ім. І. Сікорського", м. Київ, УКРАЇНА
**email: jug@sonettele.com*

АННОТАЦІЯ *У даній статті розглянуто деякі питання запобігання критичних інцидентів, що можуть виникнути при впливі кібератак на автоматизовану систему керування котлоагрегатом системи опалення. Описано найважливіші параметри автоматизованої системи керування (АСК) котла. Наведено можливі види ушкоджень котлоагрегату АСК . Проведено аналіз наслідків певних ушкоджень у зв'язку з кібер-інцидентом. Було також наведено перелік профілактичних заходів для попередження ушкоджень котлоагрегату внаслідок кібер- інциденту.*
Ключові слова: *АСК ТП; безпека; котлоагрегат; бойлер; кібератака; інцидент; кібер-інцидент.*

SOME INCENDENT PREVENTION ISSUES AT EXTERNAL CYBERATTACKS ON HEATING BOILER ICS

YU. GRUDZYNSKYY*, D. KHARCHENKO

Department Automation of heat-and-power engineering processes National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, UKRAINE

ABSTRACT *This article discusses some issues of preventing critical incidents that may arise when cyberattacks are exposed to an boiler industrial control system for heating complexes. The most important parameters of the ICS boiler are described. A list of preventive measures to prevent damage to the boiler unit as a result of the cyber incident was also provided.*
For existing industrial control systems, cyberattacks that transfer the system to a previously known dangerous state are usually not expected and not compensated for normal operating parameters.
If the attacker has access to the ASC boiler, he can block its work by changing the corresponding values of the operating modes, passing the wrong statements from the sensors, or completely shutting off the boiler. Interrupting the flow of water and fuel fed into the boiler and the furnace will disrupt the combustion process and it is already a problem, but for the boiler boiling water (when turning off the feeding water) can be extremely dangerous.
That is why in this article the possible types of damage to the boiler unit ICS are given. An analysis of the consequences of certain injuries due to the cyber incident has been carried out. A list of preventive measures to prevent damage to the boiler unit as a result of the cyber incident was also provided.
Keywords: *ICS; security; boiler unit; boiler; cyber-attack; incident; cyber-incident.*

Вступ

З кожним днем стає все більше і більше фактів порушення безпеки в комп'ютерних системах автоматизованих систем керування технологічними процесами (АСК ТП). Це призводить до того, що відповідні менеджери та інженерний персонал повинні постійно та ретельно визначати, класифікувати та зменшувати ризики в системах управління з метою успішного недопущення як самих кібератак, так і швидкого подолання їх наслідків, якщо така кібератака сталася.

Як засвідчує досвід, у багатьох випадках найбільший ризик для компанії, людей, технологічних процесів та прибутку спричинюється компромісним (недосконалим) рішенням існуючого промислового управління, а не втратою чи пошкодженням даних, як в інформаційних (ІТ) системах.

Захищенність компанії вимірюється успішним вирішенням наступних питань [1]:

1. Які можливості в системі управління існують для злому?
2. Які незахищенності існують у компанії і якими можуть бути їх наслідки?
3. Який максимальний збиток може бути заподіяно, якщо станеться одне з таких порушень?
4. Які конкретні засоби безпеки захищають кожен з наявних об'єктів управління?
5. Якщо системи мають вразливі місця в кібербезпеці, то як ці вразливості впливають на цілі, пов'язані з безпекою?
6. Хто в організації відповідає за заходи безпеки? Чи працюють команди з ІТ та відділу контрольно-вимірювальних приладів та автоматизації (КВПтА) разом, щоб забезпечити максимум безпеки в організації?

7. Чи було виділено потрібні ресурси, реалізовані правильні стандарти та придбано необхідне обладнання, щоб досягнути найкращого результату?

По-перше, для того, щоб створювати і підтримувати безпечні системи, необхідно спочатку забезпечити, щоб як самі технологічні процеси, так і зв'язок між ними були безпечними.

По-друге, треба переконатися в тому, що експлуатаційний персонал КВПтА має досвід у кібербезпеці промислових систем управління і тісно зкоординований з IT-персоналом, для того, щоб захистити усі системи та процеси.

По-третє, потрібно переконатися, що саме обладнання є безпечним і вирішує відомі проблеми кібербезпеки за допомогою використання галузевих стандартів та програм відповідності [2].

Автоматизована система керування технологічними процесами є системою, що складається з декількох компонентів, призначених для моніторингу та управління фізичними процесами та забезпечення безпечних операцій в межах конкретних відомих станів системи. Така її будова дозволяє безпечніше керувати зміною станів системи, щоб мінімізувати ризики переходів між ними. Таким чином, існуюча керованість станів та переходів призначена для захисту від випадкових збоїв одного, або декількох компонентів. Однак, для існуючих промислових систем керування направлені кібератаки, що переводять систему у заздалегідь відомий небезпечний стан, зазвичай не очікуються і не компенсуються до нормальних робочих параметрів.

Мета статі

Метою статті є висвітлення і дослідження деяких проблем кібербезпеки котлоагрегатів, а також аналіз методів запобігання їх виникненню.

Проблеми кібербезпеки котлоагрегату

Котел є закритим об’єктом під тиском, в якому вода або інша рідина використовується для підігріву води з метою подальшого обігріву будівлі конвекторами та батареями, в той час як опалювальна піч використовує тепле повітря для обігріву. При цьому, способи поширення тепла в будівлі і в першому, і в другому випадку, відрізняються один від одного. Параметри котлоагрегату та системні дані, які повинна контролювати АСК котла, наведені нижче [3]:

- температура води, що подається;
- температура димових газів;
- тиск палива;
- наявність полум'я;
- фактична пропускна здатність паливних трубопроводів;
- ефективність спалювання палива;
- обсяг газу, що спалюється;
- значення процента кисню O_2;
- питомий тиск гарячої води на виході;
- історія несправностей;
- кількість запусків котла;
- лічильник часу роботи;
- температура повітря в приміщенні.

Після того, як зловмисник отримав доступ до АСК котла, він має змогу заблокувати його роботу, змінивши відповідні значення робочих режимів, чи передавши невірні показання від датчиків, або і зовсім вимкнути котел. Переривання потоку води і палива, які подаються в котел та топку, порушить процес згоряння і само по собі, в кращому випадку, вже являє собою проблему, але для котла википання води (при відключенні живильної води) може бути надзвичайно небезпечним. Якщо подача води за якийсь час навіть і відновлюється в порожній котел, навіть невелика кількість живильної води закипає миттєво при контакті з перегрітою металевою оболонкою і призводить до сильного вибуху пари, з яким не зможуть справитися наявні запобіжні клапани для пари.

Існує два типи блокування, які можуть виникнути у котла при відключенні пристрою ручного обмеження кількості помилок (код помилки для низької води, високого або низького тиску, відсутності факела, забрудненого димоходу або низького процента кисню). Ручний перезапуск блокування вимагає, щоб оператор натиснув кнопку скидання. Автоматичне скидання блокування здійснюється самостійно, коли стан помилки очищено.

Розглянемо деякі можливі види ушкоджень котла, як результат впливу кібератаки.

Вибух котла

Звичайно, інженери вважають, що це не може відбутися через системи безпеки, призначені для запобігання катастрофі. Згадаємо, що на Чорнобильській АЕС були вимкнені функції безпеки, що і призвело до вибуху і подальшого руйнування реактра. Зловмисник теж постарається вимкнути функції безпеки без вашого відома. Відсутність в АСК котла захисту від подібної кібератаки може (і швидше за все) призведе до катастрофи. Найпоширеніші способи "знищити котел" кібератакою наведено нижче [4]:

- вибух палива;
- низький рівень води у котлі;
- неправильний розігрів котла;
- неправильний рівень тиску у котлі;
- згасання полум'я;
- надмірне полум’я.

Найбільш небезпечною ситуацією є вибух палива в бойлері або топці котла. Умови для вибуху можуть бути створені зловмисником, який примусово змінює профіль конфігурації (робочі параметри) системи, тому АСК ТП "вважає", що бойлер або топка працюють належним чином, коли насправді параметри вже давно вийшли за виробничі налаштування. Сигнал тривоги при цьому звучати не буде. Зловмисник може викликати вибух котла кількома способами [5]:

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

• ***надлишок паливної суміші***: зловмисник може використовувати АСК для створення високих концентрацій незгорілого палива, вимикаючи полум'я чи, навпаки, перекриваючи автоматичне вимикання, що дозволяє продовжувати безперервну подачу палива. Коли полум'я знову запалюється, це накопичене незгоріле паливо спалахує і призводить до сильного вибуху. Суміш, багата на паливо, також може виникнути, коли недостатньо повітря (кисню) для повного спалення палива. Зловмисник розраховує, при цьому, на відповідні дії обслуговуючого персоналу, який буде намагатися посилити потік повітря у зону згоряння топки, що призведе до величезного вибуху;

• ***погана фрагментація мазутного палива*:** накопичення будь-якого незгорілого палива в топці може призвести до вибуху. Котли вибухали через недостатню фрагментацію мазуту, що призводить до його неповного згоряння, що у свою чергу спричиняє скупчення незгорілого палива в топці. Зловмисник досягає такого ефекту, збільшуючи тиск пари (або повітря) і збільшуючи тиск подачі палива набагато вище рекомендацій виробника котлоагрегату.

• ***недостатнє очищення топки***: вибух виникає після проблем з горінням, що спричиняється відсутністю факела. Зловмисник може загасити полум'я. Відділ технічного обслуговування намагатиметься відновити полум'я, а весь цей час паливо активно розпилялося у топці. Незгоріле паливо, що накоплюється внизу гарячої топки, випускає горючі гази. Коли обслуговуючий персонал нарешті запалить пальник, спалахне велика кількість неспалених горючих газів у топці, внаслідок чого станеться величезний вибух.

Катастрофі можна запобігти, *ретельно очищуючи топку,* перш ніж намагатись поновлювати горіння. Це особливо важливо, якщо паливо вже попало в топку. Чистка повинна знижувати будь-яку кількість незгорілих горючих газів у топці до концентрації нижче вибухонебезпечної.

Вибух гарячого бойлера

Пожежні підрозділи знайомі з вибуховим потенціалом навіть невеликого гарячого бойлера. Якщо зловмисник стане причиною того, що водяний резервуар бойлера, що знаходиться під значним тиском, вибухне при 167 °С, вибух буде мати величезну силу. Декілька кімнат від місця вибуху перетвориться в пил, а люди в них чи поряд будуть вбиті чи поранені. Важливо пам'ятати, що енергія вибуху із котельної проходить через будівельні канали конструкцій будинку.

Прикладом руйнівної сили вибуху котла високого тиску є вибух на амфібійному десантному кораблі ВМС США Iwo Jima [6]. У жовтні 1990 року судно вже працювало в Перській затоці приблизно два місяці, і виникли деякі витікання води з парогенератора корабля.

Було заплановано технічне обслуговування, в тому числі капітальний ремонт головного парового клапана, що постачає пару одній з турбін електрогенераторів корабля. Цей клапан може розглядатися як запірний. Коли було запущено другий генератор турбін, і нещодавно відремонтований клапан було відкрито, щоб дозволити парі при тиску 270 кг на квадратний дюйм і 450 °С проходити, то протягом декількох хвилин цей клапан дуже сильно пропускав пару.

До того, як капітан зміг зупинити корабель і вимкнути подачу пари, кришка клапану повністю відлетіла і пара від двох великих котлів була уся скинута до котельні. Всі десять членів екіпажу в котельній були вбиті. Причиною цієї катастрофічної аварії стало використання вугілля неналежної якості. Підвищення тиску котла вище максимального дасть такий ж фатальний результат.

Низький рівень води в барабані котла

Серйозні пошкодження котла стають результатом низького рівня води в барабані котла, оскільки типова температура топки перевищує 900 °С, а міцність сталі зменшується, коли вона перевищує 430 °С. Наявність води у всіх трубах топки є єдиним, що дозволяє котлу витримувати високу температуру. За низького рівня води сталевий котел може зруйнуватися. Сучасний котел обладнаний автоматичним вимикачем низького рівня води, який відключає пальник і вмикає примусовий вентилятор. Це припиняє доступ тепла. Якщо зловмисник зможе отримати доступ до цього вимикача, у вас станеться вибух.

Зловмисник може створювати ці умови низького рівня води за допомогою будь-яких з наступних дій: відключення насоса живильної води; відкрити випускний клапан управління; втрата води в системі деаератора або в системі повторного запуску; відключення контролера рівня в барабані; втрата тиску повітря у приводі керуючого клапана; піднімання запобіжного клапана; велика раптова зміна споживання пари.

На жаль, котли, оснащені автоматичним вимикачем низького рівня води, руйнуються кожен рік, тому що обслуговуючий персонал намагається відключити цю схему, щоб зменшити кількість докучливих повідомлень [7]. Встановлення пристрою самоконтролю з наступним автоматичним рутинним тестуванням дозволить двом незалежним схемам перевірити, чи функціонує вимірювальний електрод правильно.. Перша схема буде виробляти головний сигнал тривоги коли виявляється низький рівень води. Друга схема встановлюється повністю незалежною від АСК котла, вона теж фіксує низький рівень води, і якщо так, то вона буде безпечно вимикати котел.

Вирішення проблем

Пошук і усунення несправностей є формою вирішення проблем, що стосуються ремонту несправного обладнання або систем. Логічно, що систематичний пошук джерела проблеми, призводить

до того, що вона може бути вирішена, і обладнання або система можуть бути введені в дію. У разі кібератаки проти обладнання або системи, симптоматика проблеми може бути доволі великою [8]. Для довільної системи керування очікується, що вхідні сигнали системи будуть генерувати відповідні результуючі вихідні сигнали. Будь-яка несподівана або небажана поведінка може бути ознакою атаки. Проста заміна зламаної частини обладнання, такої як насос або двигун, буде марною без відновлення нормального функціонування програмної частини «хакнутої» АСК ТП [9].

Багато АСК ТП можуть генерувати звіти в процесі своєї роботи, що є дуже корисним при усуненні неполадок. Якщо проблема помічена, то важливо подивитися на всі початкові налаштування і будь-які можливі подальші перевизначення параметрів, щоб чимскоріше визначити причину. Використання таких функцій в АСК ТП, як моніторинг даних, пов'язаних із керуванням енергоспоживання будівлі, буде корисним, але слід мати на увазі, що і ця функція теж може бути «скомпрометованою» Таким чином, показання енергоспоживання можуть здаватися абсолютно нормальними, коли насправді фактичне споживання енергії може бути значно вище [10].

Кроки вирішення проблем

КРОК 1. Впевнитися в тому, що подія є кібератакою

КРОК 2. Старатися стримувати атаку, виходячи з того, що АСК ТП вже не під вашим контролем.

КРОК 3. Зупинити атаку.

КРОК 4. Оцінити пошкодження у всьому несправному обладанні, вважаючи що все обладнання було «хакнуте».

КРОК 5. Замінити заражені сервери та відновити пошкоджене обладнання.

КРОК 6. Перезавантажити систему керування та перезапустити автоматичне керування.

Обговорення результатів

Наступні заходи повинні бути дотримані, щоб перешкодити зловмисникам зруйнувати котел [3]:

• обов'язково досліджувати і перевірити причину аварії, перш ніж намагатися знову запалити топку котла;

• періодично спостерігати за полум'ям пальника, щоб своєчасно дізнаватися про проблеми згоряння;

• перед розпалюванням котла, завжди треба продувати топку повністю, щоб видути незгорілі гази. Це особливо важливо, якщо попередньо було зафіксовано виток палива;

• слід переконатися, що система очищення води працює належним чином;

• ніколи не відключати індикатори низького рівня води в котлі;

• слід переконатися в тому, що вода покидає деаератор вільною від кисню, і що деаератор працює при належному тиску, а також і в тому, що бак для зберігання води знаходиться при температурі насичення. Безперервна вентиляція деаератора необхідна для продування незконденсованих газів;

• слід постійно стежити за якістю конденсату для того, щоб забезпечити своєчасний виток конденсату в разі катастрофічної відмови технологічного обладнання;

• ніколи не продувати стінки топки в той час як котел працює;

• крива розігріву котла повинна бути строго дотримана (зазвичай, швидкість підвищення температури в барабані котла не повинна бути більшою за 40 °C / годину);

• слід переконатися, що випускний клапан барабану котла відкривається, коли тиск в котлі стає менше технологічно коректного значення.

Висновки

Таким чином, в даній статті показано, що для запобігання кібер-інцидентам у АСК ТП котлоагрегату слід враховувати:

- можливі види ушкоджень внаслідок кібератаки;
- шляхи вирішення проблем;
- профілактичні заходи, які зменшать вірогідність кібер-інциденту.

Список літератури

1. NIST Special Publication 800-82 rev. 2. Guide to Industrial Control Systems (ICS) Security, 2015, 5, URL: https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final
2. **Ackerman, P.** Industrial Cybersecurity / **P. Ackerman** // Birmingem: Packt Publishing. – 2017, p. 515.
3. **Ayala, L**. Cyber-Physical Attack Recovery Procedures. A Step-by-Step Preparation and Response Guide / **L. Ayala** // New York: Shpringer Apress. – 2016, p. 176.
4. **Macaulay, T.** Cybersecurity for Industrial Control Systems. SCADA, DCS, PLC, HMI and SIS / **T. Macaulay, B. Synger** // New York: CRC Press. – 2011, p. 330.
5. **Knapp, E. D.** Industrial Network Security. Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems / **E. D. Knapp** // New York: Syngress. – 2011, p. 360.
6. **Peterson, D.** Anatomy of a Catastrophic Boiler Accident. 82nd General Meeting Speaker Presentation. / **D. Peterson** // *National Board of Boiler and Pressure Vessel Inspectors*. 2013. URL: http://www.nationalboard.org/ PrintPage.aspx?NewsPageID=521.
7. **Mochizuki, A.** On experimental verification of model based white list for PLC anomaly detection / **A. Mochizuki, K. Sawada, S. Shin, S. Hosokawa** // *Control Conference (ASCC) 2017 11th Asian*. – 2017. - p. 1766-1771.
8. **Pollitt, M. M.** A Cyberterrorism Fact or Fancy? / **M. M. Pollitt** // *Proceedings of the 20th National Information Systems Security Conference*. – 1997. – p. 285–289.
9. **Neumann, P**. Computer-Related Risk / **P. Neumann** // ACM Press. Addison Wesley. – 1995, p. 300.

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

10. **Li, X.** Asset-Based Dynamic Impact Assessment of Cyberattacks for Risk Analysis in Industrial Control Systems / **X. Li, Ch. Zhou, Yu-Chu Tian, N. Xiong, Yu. Qin** // *Industrial Informatics IEEE Transactions on*. – 2018. – Vol. 14. – p. 608-618.

Bibliography (transliterated)

1. NIST Special Publication 800-82 rev. 2. Guide to Industrial Control Systems (ICS) Security, 2015, 5. Available at: https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final
2. **Ackerman, P.** Industrial Cybersecurity. Birmingem: Packt Publishing, 2017, p. 515.
3. **Ayala, L.** Cyber-Physical Attack Recovery Procedures. A Step-by-Step Preparation and Response Guide. New York: Shpringer Apress, 2016, p.176.
4. **Macaulay, T., Synger, B.** Cybersecurity for Industrial Control Systems. SCADA, DCS, PLC, HMI and SIS. New York: CRC Press, 2011, p. 330.
5. **Knapp, E. D.** Industrial Network Security. Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. New York: Syngress, 2011, p. 360.
6. **Peterson, D.** Anatomy of a Catastrophic Boiler Accident. 82nd General Meeting Speaker Presentation. *National Board of Boiler and Pressure Vessel Inspectors,* 2013. Available at: http://www.nationalboard.org/PrintPage.aspx?NewsPageID=521.
7. **Mochizuki, A., Sawada, K., Shin, S., Hosokawa, S.** On experimental verification of model based white list for PLC anomaly detection. *Control Conference (ASCC) 2017 11th Asian*, 2017, p. 1766-1771.
8. **Pollitt, M. M.** A Cyberterrorism Fact or Fancy? Proceedings of the 20th National Information Systems Security Conference, 1997, 285–289.
9. **Neumann, P**. Computer-Related Risk. ACM Press. Addison Wesley, 1995.
10. **Li, X., Zhou, Ch., Tian, Y.-C., Xiong, N., Qin, Yu.** Asset-Based Dynamic Impact Assessment of Cyberattacks for Risk Analysis in Industrial Control Systems. *Industrial Informatics IEEE Transactions on*, 2018, **14**, 608-618.

Відомості про авторів (About authors)

Грудзинський Юліан Євгенович – Національний технічний університет України «Київський політехнічний інститут ім. І. Сікорського», старший викладач кафедри автоматизації теплоенергетичних процесів, м. Київ, Україна; e-mail: jug@sonettele.com.

Yulian Grudzynskyy – Senior Teacher, Department of Automation of Heat-Power Processes, National Technical University of Ukraine “Igor Sikorskyy Kyiv Polytechnic Institute”, Kyiv, Ukraine; e-mail: jug@sonettele.com.

Харченко Денис Юрійович – Національний технічний університет України «Київський політехнічний інститут ім. І. Сікорського», магістр кафедри автоматизації теплоенергетичних процесів, м. Київ, Україна; e-mail: denisxar@gmail.com.

Denys Kharchenko –Master Student, Department of Automation of Heat-Power Processes, National Technical University of Ukraine “Igor Sikorskyy Kyiv Polytechnic Institute”, Kyiv, Ukraine; e-mail: denisxar@gmail.com.

Будь ласка, посилайтесь на цю статтю наступним чином:

Грудзинський, Ю. Є. Деякі питання запобігання інцидентам при зовнішніх кібератаках на автоматизовану систему керування котлоагрегатом системи опалення / **Ю. Є. Грудзинський, Д. Ю. Харченко** // *Вісник НТУ «ХПІ», Серія: Нові рішення в сучасних технологіях*. – Харків: НТУ«ХПІ». – 2018. – №16 (1292). – С.112-116. – doi:10.20998/2413-4295.2018.16.17.

Please cite this article as:

Grudzynskyy, Yu., Kharchenko, D. Some incendent prevention issues at external cyberattacks on heating boiler ICS. *Bulletin of NTU "KhPI". Series: New solutions in modern technologies*. – Kharkiv: NTU "KhPI", 2018, **16**(1292), 112-116, doi:10.20998/2413-4295.2018.16.17.

Пожалуйста, ссылайтесь на эту статью следующим образом:

Грудзинский, Ю. Е. Некоторые вопросы предотвращения инцидентов при внешних кибератаках на автоматизированную систему управления котлоагрегатом системы отопления / **Ю. Е. Грудзинский, Д. Ю. Харченко** // *Вестник НТУ «ХПИ», Серия: Новые решения в современных технологиях*. – Харьков: НТУ «ХПИ». – 2018. – № 16 (1292). – С. 112-116. – doi:10.20998/2413-4295.2018.16.17.

АННОТАЦИЯ *В этой статье обсуждаются некоторые проблемы предотвращения инцидентов, которые могут возникнуть при проведении кибератаки на систему управления котлоагрегатом в системах отопления. Описаны наиболее важные для системы управления параметры котла. В этой статье приводятся возможные типы повреждений для ICS котла, проведен анализ их последствий. Представлен перечень превентивных мер по предотвращению повреждения котельного агрегата в результате кибер-инцидента.*

Ключевые слова: *АСУ ТП; безопасность; котлоагрегат; бойлер; кибератака; инцидент; кибер-инцидент.*

Надійшла (received) 07.05.2018