УДК 004.9 doi:10.20998/2413-4295.2018.16.18

ОСОБЛИВОСТІ ОЦІНКИ РИЗИКУ В АВТОМАТИЗОВАНИХ СИСТЕМАХ КЕРУВАННЯ ТЕХНОЛОГІЧНИМИ ПРОЦЕСАМИ

Ю. Є. ГРУДЗИНСЬКИЙ*, А. М. ШУЛЕПА

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 наведено особливості оцінювання ризиків, що виникають при впливі кібератак на автоматизовані системи керування технологічними процесами (АСК ТП). Описані відмінності при оцінці ризиків типових ІТ-систем та АСК ТП. Наведено потенційні наслідки інцидентів у АСК ТП. Проведено аналіз наслідків порушення технологічного процесу в АСК ТП у зв'язку з кібер-інцидентом. Обґрунтовано важливість врахування нецифрових (аналогових) складових АСК ТП при оцінці впливу кібер-інциденту. Проаналізовано важливість врахування розповсюдження впливу на пов'язані системи та процеси.*
Ключові слова: *АСК ТП; безпека; ризик; оцінка ризику; інцидент; кібер-інцидент.*

SPECIAL CONSIDERATIONS FOR DOING RISK ASSESSMENT OF INDUSTRIAL CONTROL SYSTEMS

YU. GRUDZYNSKYY*, A. SHULEPA

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

ABSTRACT *This paper provides special considerations that organizations have to pay attention for while doing risk assessment. The culture of safety and safety assessments is well established within the majority of the Industrial Control Systems (ICS) user community. Information security risk assessments should be seen as complementary to such assessments though the assessments may use different approaches and cover different areas. Safety assessments are concerned primarily with the physical world. Information security risk assessments primarily look at the digital world. However, in an ICS environment, the physical and the digital are intertwined and significant overlap may occur. It is important that organizations consider all aspects of risk management for safety (e.g., risk framing, risk tolerances), as well as the safety assessment results, when carrying out risk assessments for information security. The personnel responsible for the information security risk assessment must be able to identify and communicate identified risks that could have safety implications. Conversely, the personnel charged with safety assessments must be familiar with the potential physical impacts and their likelihood developed by the information security risk assessment process. This paper describes potentional physical impacts of an ISC incident, shows impact, physical disruption of an ICS process can made. It demonstrates importancy of incorporating non-digital aspects of ICS into impact evaluations, provides main categories of non-digital ICS control component and shows basic considerations when considering the possible mitigation effects of non-digital control mechanisms. Also, this paper considering the propagation of impact to connected systems.*
Keywords: *ICS; security; risk; risk assessement; incident; cyber-incident.*

Вступ

На початковому етапі автоматизовані системи керування технологічними процесами (АСК ТП) мало нагадували традиційні системи інформаційних технологій (ІТ), тому що АСК ТП були ізольованими системами з власними протоколами управління, що використовували спеціалізоване обладнання та програмне забезпечення. Багато компонентів АСК ТП перебували на фізично захищених ділянках, а самі компоненти не були підключені до ІТ-мереж або систем. Сьогодні, оскільки АСК ТП все більше використовують ІТ-рішення для можливості підключення до корпоративних бізнес-систем та використання віддаленого доступу, то вони починають нагадувати ІТ-системи у сфері кібербезпеки. Ця інтеграція підтримується новими можливостями ІТ, але вона забезпечує значно меншу ізоляцію АСК ТП від зовнішнього світу, порівняно з попередніми системами, що створює підвищену потребу в безпеці цих систем. Незважаючи на те, що типові рішення вже були раніше розроблені для вирішення проблем безпеки в ІТ-системах, слід застосовувати спеціальні запобіжні заходи при впровадженні цих самих рішень для середовищ АСК ТП. У деяких випадках потрібні нові рішення безпеки, більш пристосовані до АСК ТП.

Хоча деякі характеристики між обома типами систем схожі, проте АСК ТП мають і власні особливості, які сильно відрізняють їх від традиційних систем обробки інформації. Багато з цих відмінностей обумовлено тим фактом, що логіка, яка виконується в АСК ТП, безпосередньо впливає на фізичний світ.

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

Деякі з цих характеристик включають значний ризик для здоров'я та безпеки людського життя та серйозну шкоду для навколишнього середовища, а також серйозні фінансові наслідки для організації, такі як втрати виробництва, негативний вплив на економіку країни та компрометація приватної інформації [1]. АСК ТП мають унікальні вимоги до продуктивності та надійності, часто використовують операційні системи та програми, які можуть вважатися нетрадиційними для типового IT-персоналу [2]. Окрім цього, цілі безпеки та ефективності IT-рішень іноді суперечать безпеці при розробці та експлуатації АСК ТП.

Програми кібербезпеки АСК ТП завжди повинні бути частиною більш широких програм безпеки і надійності як окремого підприємства, так і в корпоративних програмах кібербезпеки усієї організації, оскільки кібербезпека має важливе значення для безпечної та надійної роботи сучасних технологічних процесів [3]. Загрози для систем керування можуть надходити з численних джерел, включаючи ворожі уряди [4], терористичні групи, незадоволені працівники, зловмисники, складності, аварії та стихійні лиха, а також зловмисні чи випадкові дії інсайдерів [5]. Пріорітети доступності (надійності роботи) та цілісності, за якими вже слідує конфіденційність, повинні передувати іншим цілям безпеки АСК ТП.

З самої природи АСК ТП випливає (оскільки вплив кібер-інциденту в АСК ТП може включати як фізичні, так і цифрові ефекти), що коли проводиться оцінка ризику впливу кібер-інциденту на систему керування та довкілля, можуть існувати додаткові міркування, які відсутні при проведенні оцінки ризиків традиційної IT-системи.

Мета статі

Метою статті є намагання показати, які саме чинники і зв'язок між ними слід враховувати при оцінці ризику для АСК ТП при можливих кібератаках на неї.

Захист в межах оцінки ризику інформаційної безпеки АСК ТП

Оцінки безпеки стосуються перш за все фізичного світу. Оцінки ризику інформаційної безпеки в першу чергу розглядають цифровий світ. Проте в середовищі АСК ТП фізичний та цифровий світ тісно переплетені, і може відбуватися їх значне взаємопроникнення.

Важливим є те, що організації повинні враховувати всі аспекти керування ризиками для захисту (наприклад, розробка ризиків, стійкість до ризику), а також результати оцінки захисту при проведенні оцінки ризиків інформаційної безпеки. Персонал, відповідальний за оцінку ризику інформаційної безпеки, повинен мати можливість ідентифікувати усі виявлені ризики, які можуть мати наслідки для безпеки та повідомляти про них. І навпаки, персонал, на який покладено оцінку безпеки, повинен бути в курсі потенційних фізичних впливів, розроблених процесом оцінки ризику інформаційної безпеки, та їх вірогідності [6].

Потенційні фізичні наслідки інцидентів в АСК ТП

Оцінка потенційного фізичного збитку від кібер-інциденту повинна включати до себе наступні питання [7]:

- як інцидент може змінювати роботу датчиків та виконавчих механізмів для впливу на фізичне середовище;
- які резервні елементи керування існують в АСК ТП для запобігання впливу;
- як може виникнути фізичний інцидент на основі цих умов.

Фізичний вплив може негативно позначитися на довкіллі багатьма засобами, включаючи викид небезпечних матеріалів (наприклад, сирої нафти), пошкодження за допомогою кінетичних сил (наприклад, вибухів) та впливу джерел енергії (наприклад, електроенергії, пари). Фізичний інцидент може негативно вплинути і на саму АСК ТП та підтримку прилеглої інфраструктури: вплинути на різні технологічні процеси, якими керує АСК ТП, або на довкілля. Оцінка потенційних фізичних впливів повинна включати в себе всі частини АСК ТП, починаючи з оцінки потенційного впливу на підключені датчики та приводи. Кожна з цих частин буде розглянута нижче.

Оцінка впливу кібер-інциденту на фізичне середовище має зосереджуватися на потенційному нанесенні шкоди безпеки людини, природного довкілля та інших прилеглих критичних інфраструктур. Наслідки впливу на безпеку людини повинні оцінюватися на основі того, чи це можлива травма, чи професійне захворювання, або навіть смерть від відмови АСК ТП. Також до оцінки повинні включатися будь-які раніше проведені оцінки впливу на безпеку, що проводяться організацією стосовно як працівників, так і широкої громадськості. Необхідно також вирішити вплив на довкілля. Цей аналіз повинен включати будь-які доступні оцінки впливу на довкілля, що проводиться організацією для визначення того, як цей інцидент може вплинути на природні ресурси та дику природу в короткостроковій та довгостроковій перспективі. Крім того, слід зазначити, що АСК ТП може не розташовуватися в одному контрольованому місці, а може бути розподіленою на великій території та знаходитися у неконтрольованому середовищі. Нарешті, вплив на фізичне середовище має досліджувати, наскільки інцидент може спричинити шкоду інфраструктурі, що оточує АСК ТП (наприклад, виробництво/передача електроенергії, транспортна інфраструктура та послуги з водопостачання).

Оцінка впливу порушення технологічного процесу в АСК ТП

Окрім впливу на фізичне середовище, оцінка ризику також повинна включати можливі наслідки для технологічного процесу, що виконується розглянутою АСК ТП, а також іншими системами. Інцидент, який впливає на АСК ТП та порушує залежний процес, може спричинити каскадний вплив на інші процеси, пов'язані з АСК ТП, та на широку громадськість, що залежить від виду отримуваних продуктів та послуг. Вплив на пов’язані процеси АСК ТП може включати в себе як системи, так і процеси в організації (наприклад, процес виробництва, який залежить від процесу, що керується розглянутою системою), або системи та процеси, не пов'язані з організацією (наприклад, комунальне підприємство, що продає вироблену електроенергію найближчому заводу).

Кібер-інцидент також може негативно вплинути і на саму фізичну АСК ТП. Цей тип впливу в першу чергу включає в себе фізичну інфраструктуру заводу (наприклад, резервуари, клапани, двигуни) разом із цифровими та аналоговими механізмами керування (наприклад, кабелі, ПЛК, манометри). Фізичне пошкодження АСК ТП, або заводу може спричинити як короткострокові, так і довгострокові збої в залежності від ступеня інциденту. Прикладом кібер-інциденту, який таким чином вплинув на АСК ТП, є шкідливе програмне забезпечення Stuxnet, яке нанесло фізичну шкоду центрифугам, а також порушило залежні процеси [8].

Включення аналогових аспектів АСК ТП до оцінок впливу

Вплив на АСК ТП не може бути адекватно визначений, зосереджуючись лише на цифрових аспектах системи, оскільки існують аналогові механізми, що забезпечують відмовостійкість та запобігають функціонуванню АСК ТП за межами прийнятних параметрів. Ці механізми можуть допомогти зменшити будь-який негативний вплив, який може мати цифровий інцидент на АСК ТП, і повинні бути включені до процесу оцінки ризику. Наприклад, АСК ТП часто має аналогові керуючі механізми, які можуть перешкодити АСК ТП працювати поза безпечними межами, і тим самим обмежити вплив атаки (наприклад, механічний запобіжний клапан тиску). Крім того, аналогові механізми (наприклад, лічильники, сигналізатори) можуть використовуватися для спостереження за станом фізичної системи, щоб забезпечити операторам надійні дані, якщо цифрові показники недоступні або пошкоджені. У таблиці нижче наведено категорію аналогових механізмів керування, які можуть допомогти зменшенню впливу інциденту на АСК ТП [9].

Таблиця 1 – Категорії аналогових компонентів керування АСК ТП, що повинні бути взяті до уваги при оцінці ризику

Тип системи	Опис
Аналогові реєстратори чи сигналізатори	Аналогові механізми, які вимірюють і відображають стан фізичної системи (наприклад, температуру, тиск, напругу, струм) і можуть забезпечити оператора точною інформацією в ситуаціях, коли цифрові дисплеї недоступні або пошкоджені. Інформація може бути надана оператору на деякому аналоговому індикаторі (наприклад, термометри, манометри) та через звукові сигнали.
Механізми ручного керування	Ручні механізми керування (наприклад, ручні елементи управління клапанами, фізичні вимикачі) надають операторам можливість ручного керування виконавчим механізмом, не покладаючись на цифрову систему керування. Це гарантує, що приводом можна керувати, навіть якщо система управління недоступна або пошкоджена.
Аналогові системи керування	Аналогові системи керування використовують нецифрові датчики та виконавчі механізми для контролю та керування фізичним процесом. Вони можуть запобігти виходу фізичного процесу в небажаний стан у ситуаціях, коли цифрова система керування недоступна або пошкоджена. Аналогові системи керування включають у себе такі пристрої, як регулятори, обмежуючі пристрої та електромеханічні реле.

Визначення потенційної шкоди, який кібер-інцидент може нанести АСК ТП, має включати аналіз усіх аналогових механізмів керування та ступінь, до якого вони можуть пом'якшити можливі негативні наслідки для АСК ТП. При розгляді можливих ефектів пом'якшення наслідків аналоговими механізмами керування, варто враховувати багато факторів, серед яких [10]:

- аналогові механізми керування можуть вимагати додаткового часу та залучення людей для виконання необхідних функцій моніторингу або керування, і ці зусилля можуть бути суттєвими. Наприклад, такі механізми можуть вимагати від

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

операторів переміщення на віддалену ділянку для виконання певних керуючих функцій. Такі механізми також можуть залежати від часу реагування людини, який може бути довшим, ніж час автоматичного керування;

- ручні та аналогові системи можуть не забезпечувати можливості моніторингу та керування з таким же ступенем точності та надійності, що й цифрова система керування. Це може чинити ризик (якщо основна система керування недоступна або пошкоджена) зниження якості, безпеки або ефективності усієї системи. Наприклад, захисне цифрове реле забезпечує більшу точність і надійність виявлення несправностей, ніж аналогові/статичні реле, тому, якщо цифрові реле недоступні, то у системі можуть бути хибні спрацювання релейних схем.

Включення впливу самої системи безпеки в оцінку ризику

Системи захисту також можуть зменшити вплив кібер-інцидентів на АСК ТП. Системи захисту часто використовуються для виконання спеціальних функцій моніторингу та керування для гарантування безпеки людей, навколишнього середовища, параметрів технологічного процесу та самої АСК ТП. Незважаючи на те, що ці системи традиційно впроваджуються таким чином, щоб бути повністю дублюючими до основних АСК ТП, вони можуть не забезпечувати повного резервування при кібер-інциденті, зокрема, у випадку, коли цей інцидент чинить досвідчений атакуючий. Вплив впроваджених заходів безпеки на систему захисту також має бути оцінено, щоб переконатися в тому, що при всіх випадках вони не стануть негативно впливати на систему.

Врахування розповсюдження впливу на пов’язані системи (каскадний ефект)

Оцінка впливу інциденту також повинна включати до себе і оцінку того, як вплив від АСК ТП може поширюватися на пов’язані з нею АСК ТП, або фізичні системи. АСК ТП можуть бути взаємопов'язані з іншими системами таким чином, що збої в одній системі або технологічному процесі можуть легко каскадно поширюватись на інші системи всередині або поза межами організації. Поширення впливу може відбутися завдяки фізичним і логічним залежностям. Своєчасна передача результатів оцінки ризиків операторам пов’язаних або взаємозалежних систем та технологічних процесів є одним із засобів пом'якшення наслідків шкоди від дії кібератаки.

Пошкодження пов'язаної АСК ТП може виникнути, якщо кібер-інцидент поширюється на пов’язані системи керування. Яскравим прикладом може бути поширення вірусу або черв'яка на підключену АСК ТП, і подальше нанесення шкоди вже цій системі. Фізична шкода також може поширюватися на інші залежні АСК ТП. Якщо інцидент впливає на фізичне середовище АСК ТП, він також може вплинути і на інші пов'язані з нею фізичні зони. Наприклад, вплив може призвести до фізичної небезпеки, яка погіршує навколишні фізичні умови. Крім того, вплив може також послабити загальні спільні залежності (наприклад, енергопостачання) або призвести до дефіциту матеріалу, необхідного для виконання пізнішого етапу в промисловому технологічному процесі.

Висновки

Таким чином, в даній статті показано, що при розробці оцінки ризику в АСК ТП слід враховувати:

- оцінку впливу кібер-інциденту на захист та використання загальних оцінок безпеки;
- фізичний вплив кібер-інциденту на АСК ТП, включаючи як саме довкілля, так і вплив на керований технологічний процес;
- наслідки оцінки ризику не цифрових (аналогових) компонентів керування в межах АСК ТП.

Список літератури

1. **Patrice, B.** Ukrainian power grids cyberattack. A forensic analysis based on ISA/IEC 62443 / **B. Patrice, J.-P. Hauet, R. Françoise, R. Foley** // *InTech Magazine.* – 2017. – 3-4.
2. **Марков, А. С.** Организационно - технические проблемы защиты от целевых вредоносных программ типа Stuxnet / **А. С. Марков, А. А. Фадин** // *Вопросы кибербезопасности.* – 2013. – 28-36.
3. **Behr, P.** SECURITY: Utilities look back to the future for hands-on cyberdefense / **P. Behr, B. Sobczak** // *E&E News*. – 2016. – 7.
4. **Goedeker, M.** Результаты предварительного расследования и реинжиниринга зловредов, использованных в кибератаке класса "Обрушение" в Украине / **M. Goedeker.** – 2015. – 11. URL: https://socprime.com/blog-ru/results-of-initial-investigation-and-malware-reverse-analysis-of-fire-sale-ukraine-2/
5. **Ніколайчук, С.** Хакерська атака в Україні: як працює вірус Petya.A і що робити? / **С. Ніколайчук.** – 2017. – 6. URL: https://24tv.ua/hakerska-ataka-v-ukrayini-virus-petya-a-yak-pratsyuye-i-shho-robiti-n835033
6. 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
7. **Ackerman, P.** Industrial Cybersecurity / **P. Ackerman** // Birmingem: Packt Publishing, 2017. – p. 515.
8. **Ayala, L.** Cyber-Physical Attack Recovery Procedures. A Step-by-Step Preparation and Response Guide / **L. Ayala** // New York: Shpringer Apress, 2016. – p.176.
9. **Macaulay, T.** Cybersecurity for Industrial Control Systems. SCADA, DCS, PLC, HMI and SIS / **T. Macaulay, B. Synger** // New York: CRC Press, 2011. – p. 330.
10. **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.

Bibliography (transliterated)

1. **Patrice, B., Hauet, J.-P. Françoise, R., Foley, R.** Ukrainian power grids cyberattack. A forensic analysis based on ISA/IEC 62443, *InTech Magazine*, 2017, 3-4.
2. **Markov, A. S., Fadin, A. A.** Organizatsionno-tekhnicheskie problemy zashhity ot tselevyh vredonosnyh program tipa Stuxnet, *Voprosy kiberbezopasnosti*, 2013, 28-36.
3. **Behr, P., Sobczak**, **B.** SECURITY: Utilities look back to the future for hands-on cyberdefense, *E&E News*, 2016, 7.
4. **Goedeker, M.** Rezul'taty predvaritel'nogo rassledovaniya I reinzheniringa zlovredov, ispol'zovannyh v kiberatake klassa "Obrushenie" v Ukraine, 2015, 11. Available at: https://socprime.com/blog-ru/results-of-initial-investigation-and-malware-reverse-analysis-of-fire-sale-ukraine-2/
5. **Nikolaychuk, S.** Hakerc'ka ataka v Ukraini: yak pratsyue virus Petya A I shho robyty, 2017, 6. Available at: https://24tv.ua/hakerska_ataka_v_ukrayini_virus_petya_a_yak_pratsyuye_i_shho_robiti_n835033.
6. 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.
7. **Ackerman, P.** Industrial Cybersecurity. Birmingem: Packt Publishing, 2017, p. 515.
8. **Ayala, L.** Cyber-Physical Attack Recovery Procedures. A Step-by-Step Preparation and Response Guide, New York: Shpringer Apress, 2016, p.176.
9. **Macaulay, T., Synger, B.** Cybersecurity for Industrial Control Systems. SCADA, DCS, PLC, HMI and SIS, New York: CRC Press, 2011, p. 330.
10. **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.

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.

Шулепа Андрій Миколайович – Національний технічний університет України «Київський політехнічний інститут ім. І. Сікорського», магістр кафедри автоматизації теплоенергетичних процесів, м. Київ, Україна; e-mail: shulepaa@gmail.com.

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

Будь ласка, посилайтесь на цю статтю наступним чином:

Грудзинський, Ю. Є. Особливості оцінки ризику в автоматизованих системах керування технологічними процесами / **Ю. Є. Грудзинський, А. М. Шулепа** // *Вісник НТУ «ХПІ», Серія: Нові рішення в сучасних технологіях*. – Харків: НТУ «ХПІ». – 2018. – № 16 (1292). – С. 117-121. – doi:10.20998/2413-4295.2018.16.18.

Please cite this article as:

Grudzynskyy, Yu., Shulepa, A. Special considerations for doing risk assessment of industrial control systems. *Bulletin of NTU "KhPI". Series: New solutions in modern technologies*. – Kharkiv: NTU "KhPI", 2018, **16**(1292), 117-121, doi:10.20998/2413-4295.2018.16.18.

Пожалуйста, ссылайтесь на эту статью следующим образом:

Грудзинский, Ю. Е. Особенности оценки риска в автоматизированных системах управления технологическими процессами / **Ю. Е. Грудзинский, А. М. Шулепа** // *Вестник НТУ «ХПИ», Серия: Новые решения в современных технологиях*. – Харьков: НТУ «ХПИ». – 2018. – № 16 (1292). – С. 117-121. – doi:10.20998/2413-4295.2018.16.18.

АННОТАЦИЯ *В данной статье приведены особенности оценки рисков, возникающих при воздействии кибератак на автоматизированные системы управления технологическими процессами (АСУ ТП). Описанные различия при оценке рисков типовых ИТ-систем и АСУ ТП. Приведены потенциальные последствия инцидентов в АСУ ТП. Проведен анализ последствий нарушения технологического процесса в АСУ ТП в связи с кибер-инцидентом. Обоснована важность учета нецифровых (аналоговых) составляющих АСУ ТП при оценке влияния кибер-инцидента. Проанализированы важность учета распространения влияния на связанные системы и процессы.*

Ключевые слова: *АСУ ТП; безопасность; риск; оценка риска; инцидент; кибер-инцидент.*

Поступила (received) 08.05.2018