## CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION

УДК 004.056.53

СЕРГІЙ ГОНЧАР,
ГЕННАДІЙ ЛЕОНЕНКО

# НАСЛІДКИ МОЖЛИВИХ КІБЕРАТАК НА ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Життєво важливі для критичної інфраструктури галузі держави характеризуються наявністю автоматизованих систем управління технологічними процесами. Вони включають в себе системи диспетчерського управління і збору даних, системи розподіленого управління. З огляду на це виконано дослідження негативних наслідків кібератак на об'єкти критичної інфраструктури. Приведено основні категорії впливу деструктивних дій в автоматизованих системах управління технологічними процесами на об'єктах критичної інфраструктури. Показано взаємозв'язок між кібератаками на об'єкти критичної інфраструктури і наслідками у промисловому секторі. Приведено критерії, по яких формується перелік інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави. Досліджено активи об'єктів критичної інфраструктури та збитки, що можуть бути їм завдані. Результати проведеного дослідження можливо використати при оцінюванні актуальності кіберзагроз об'єктів критичної інфраструктури.

**Ключові слова:** кіберзагроза, кібератака, критична інфраструктура, наслідки, автоматизовані системи управління, технологічні процеси.

**Вступ.** В даний час автоматизовані системи управління технологічними процесами об'єктів критичної інфраструктури (далі – ОКІ), які включають в себе системи диспетчерського управління і збору даних, системи розподіленого управління та інші конфігурації систем управління використовуються в галузях, які життєво важливі для критичної інфраструктури держави. Об'єкти критичної інфраструктури – це підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення [1].

**Постановка проблеми.** В автоматизованих системах управління технологічними процесами, на відміну від традиційних систем інформаційних технологій існує досить тісний взаємозв'язок автоматизованих систем з фізичними процесами і виконавчими пристроями [2].

Таким чином, у випадку порушення безпеки інформації в автоматизованих системах управління технологічними процесами може призвести до наслідків у промисловому секторі, особливо у випадку автоматизованих систем управління небезпечними виробничими циклами або систем життєзабезпечення. Імовірні збитки від реалізації таких кіберзагроз окрім фінансових втрат будуть включати ризики репутації і ризики, пов'язані зі втратою здоров'я та життя людей, а також ризики виникнення екологічних катастроф. Навіть поодиноке порушення функціонування автоматизованих систем управління технологічним процесом може призвести до катастрофічних наслідків.

На рис. 1 приведено статистику інцидентів в автоматизованих системах управління технологічними процесами (АСУ ТП) за галузями в 2015 році [3]. Як видно із приведеної діаграми найбільша кількість інцидентів припадає на виробництво та енергетичну галузь.

Кожна кіберзагроза характеризується імовірністю її реалізації і нанесеними нею збитками [4]. Тобто, показник актуальності кіберзагрози в АСУ ТП буде пропорційний імовірності реалізації даної кіберзагрози та коефіцієнту її небезпеки.

Тоді, небезпека кіберзагрози в автоматизованих системах управління технологічними процесами буде визначатися оцінкою можливих наслідків від її реалізації з позиції впливу на функціонування автоматизованих систем управління технологічними процесами.

Враховуючи зазначене, для своєчасної та адекватної оцінки актуальності кіберзагрози безпеці інформації в автоматизованих системах управління технологічними процесами необхідно знати негативні наслідки можливої реалізації даних кіберзагроз.

**Наслідки кібератак на об'єкти критичної інфраструктури.** Під "наслідками" будемо розуміти величину і тип шкоди, нанесеної успішною кібератакою зловмисників. Для визначення величини наслідків, знову ж таки, необхідно ввести певну конкретність. Під величиною наслідків будемо розуміти очікувану величину збитків упродовж конкретного проміжку часу при заданому виді нападу, що призвів до нанесення збитків певному об'єкту: це може бути, наприклад, кількість постраждалих людей, пошкодження майна тощо).

Як зазначають деякі автори [4], збитки, завдані кіберзагрозою можуть визначатися в абсолютних одиницях: економічних втратах, часових втратах, обсязі втраченої або пошкодженої інформації.

Збитки в ІС ОКІ можуть бути класифіковані як прямі і непрямі.

Прямі збитки є витратами, які пов'язані з заміною активів. Збитки можуть мати місце за причиною фізичного пошкодження активу, в результаті втрати цілісності або доступності, переривання точної послідовності або зміни характеру процесу. Активи можуть мати порівняно низькі прямі збитки по відношенню до їх корисності, оскільки носій, який використовується для зберігання активу, як правило, має низьку вартість. Незначні пошкодження людських активів з коротким часом відновлення можуть мати низькі прямі збитки для організації, навіть у випадку довгострокових наслідків для травмованої людини.

Непрямі збитки є збитками завданими внаслідок втрати активів. Вони можуть включати в себе збитки, пов'язані з процесом простою, переробки або інші виробничі витрати через втрату активів.

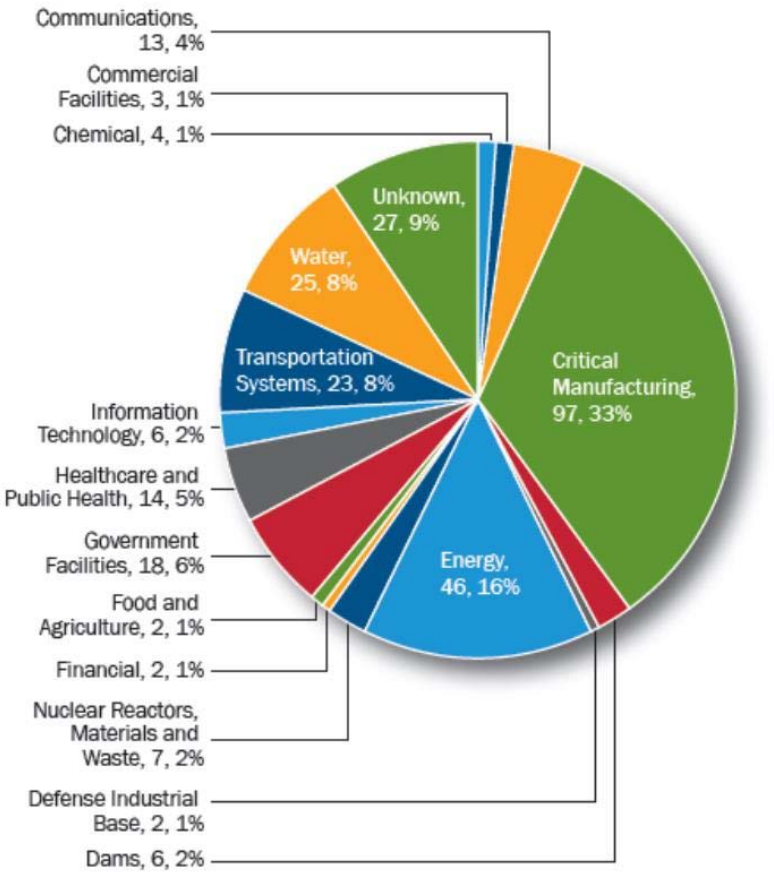


Рисунок 1 – Інциденти в АСУ ТП за галузями в 2015 році

Для фізичних активів непрямі збитки, як правило, включають наслідки, які виникають через втрату компонентів. Непрямі збитки від пошкодження обладнання можуть призвести до ремонту, реінжинірингу або інших зусиль для відновлення контролю над промисловим процесом. Водночас непрямі збитки часто можуть бути дуже великими. Вони включають в себе втрату довіри громадськості, втрату ліцензії на діяльність, втрату конкурентних переваг від випуску інтелектуальної власності, як наприклад конфіденційний процес, нові технології тощо.

В автоматизованих системах управління технологічними процесами збитки виникають через порушення конфіденційності, цілісності, доступності та неспростовності інформації у результаті деструктивних дій при реалізації кіберзагроз.

Основними категоріями впливу деструктивних дій в автоматизованих системах управління технологічними процесами є [5]:

– фізичний вплив – включає в себе безліч прямих наслідків аварій автоматизованих систем управління технологічними процесами. Найважливішими потенційними наслідками є такі, які можуть призвести до травм і загибелі людей. Інші наслідки включають втрату майна (включаючи дані) і потенційні збитки навколишньому середовищу;

– економічні впливи – наслідки другого порядку від фізичних впливів, що є похідними від аварій автоматизованих систем управління технологічними процесами. Фізичний вплив може призвести до наслідків для системи, що, у свою чергу може нанести більший економічний збиток підприємству чи організації. У великих масштабах, ці наслідки можуть негативно позначитися на місцевому, регіональному, національному рівнях, а можливо і для глобальної економіки;

– екологічна вплив – вплив на населення та навколишнє природне середовище;

– політичний вплив – вплив на впевненість та дієздатність влади;

– соціальні впливи – наслідки другого порядку, які є похідними від втрати державної або громадської довіри в організації.

– взаємозв’язок з іншими елементами критичної інфраструктури та тривалість впливу.

Враховуючи приведені вище категорії впливу порушення безпеки інформації в автоматизованих системах управління технологічними процесами можливо навести перелік наслідків цих впливів:

– порушення національної безпеки;
– сприяння вчиненню акту тероризму;
– втрата або скорочення виробництва;
– травми або смерть людей;
– пошкодження обладнання;
– викид (витікання, випаровування) або крадіжка небезпечних матеріалів;
– екологічні збитки;
– кримінальні або цивільно-правові зобов’язання;
– втрата приватної або конфіденційної інформації;
– втрата іміджу бренду або довіри клієнтів.

Слід зазначити, що елементи приведеного переліку не є незалежними. Очевидно, що один з наслідків може призвести до іншого.

Крім того, на сьогоднішній день, визначається перелік інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави. Зазначений перелік формується з урахуванням негативних наслідків, до яких може призвести кібератака на інформаційно-телекомунікаційну систему [1]:

– виникнення надзвичайної ситуації техногенного характеру та/або негативний вплив на стан екологічної безпеки держави (регіону);

– негативний вплив на стан енергетичної безпеки держави (регіону);

– негативний вплив на стан економічної безпеки держави;

– негативний вплив на стан обороноздатності, забезпечення національної безпеки та правопорядку у державі;
– негативний вплив на систему управління державою;
– негативний вплив на суспільно-політичну ситуацію в державі;
– негативний вплив на імідж держави;
– порушення сталого функціонування фінансової системи держави;
– порушення сталого функціонування транспортної інфраструктури держави (регіону);
– порушення сталого функціонування інформаційної та/або телекомунікаційної інфраструктури держави (регіону), в тому числі її взаємодії з відповідними інфраструктурами інших держав.

Дослідження інформації з відкритих джерел показують, що останнім часом у світі значно посилилась спрямованість кібератак на комп'ютерні мережі енергетичного сектору, дипломатичного корпусу, силових відомств, оборонного комплексу, державних підприємств, медіа компаній. Метою таких кібератак, в першу чергу, є нанесення шкоди критичній інфраструктурі держави. Крім того, протягом останніх років у світі спостерігається стійка тенденція до збільшення кількості цілеспрямованих кібератак на об'єкти критичної інфраструктури.

Тому, враховуючи можливі негативні наслідки у разі реалізації кібератак, необхідно зазначити, що ефективне функціонування системи кіберзахисту країни залишається пріоритетним завданням і з кожним роком стає все більш актуальним.

**Висновки.** Виконано дослідження негативних наслідків кібератак на об'єкти критичної інфраструктури. Результати проведеного дослідження можливо використати при оцінці актуальності кіберзагроз об'єктів критичної інфраструктури.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Кабінет міністрів України. (2016, Серп. 23). *Постанова № 563, Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави*. [Електронний ресурс]. Доступно: http://zakon.rada.gov.ua/laws/show/563-2016-%D0%BF. Дата звернення: Груд. 18, 2015.

[2] С.Ф. Гончар, "Особенности обеспечения кибербезопасности индустриальных систем управления", на *Міжнародній науково-практичній конференції Проблеми та перспективи розвитку енергетики, електротехнологій та автоматики в АПК*, Київ, Україна, 2013, с. 36-37.

[3] ICS-CERT Monitor 2015. [Online]. Available: http://ics-cert.us-cert.gov/monitors. Accessed on: Dec. 18, 2015.

[4] В.В. Домарев, *Безопасность информационных технологий. Методология создания систем защиты*. Київ, Україна: ООО "ТИД "ДС", 2002.

[5] Council of the European Union. (2008, Dec. 08). *Directive 2008/114/EC, On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.* [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32008L0114. Accessed on: Dec. 18, 2015.

Стаття надійшла до редакції 25.02.2016.

## REFERENCES

[1] Cabinet of Ministers of Ukraine. (2016, Aug. 23). *Resolution number 563, Approval the order of formation of the list of information and telecommunication systems акщь from the objects of critical infrastructure of the government* [Online]. Available: http://zakon.rada.gov.ua/laws/show/563-2016-%D0%BF. Accessed on: Dec. 18, 2015.

[2] S.F. Honchar, “Features of cybersecurity industrial control systems”, in *Proc. International Scientific Conference Problems and prospects of power engineering, electrotechnology and automation in agriculture*, Kyiv, Ukraine, 2013, pp. 36-37.
[3] ICS-CERT Monitor 2015. [Online]. Available: http://ics-cert.us-cert.gov/monitors. Accessed on: Dec. 18, 2015.
[4] V.V. Domarev, *Safety of information technologies. Methodology of creation of systems of protection*. Kyiv, Ukraine: OOO “TYD “DS”, 2002.
[5] Council of the European Union. (2008, Dec. 08). *Directive 2008/114/EC, On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.* [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32008L0114. Accessed on: Dec. 18, 2015.

СЕРГЕЙ ГОНЧАР,
ГЕННАДИЙ ЛЕОНЕНКО

**ПОСЛЕДСТВИЯ ВОЗМОЖНЫХ КИБЕРАТАК НА ОБЪЕКТЫ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ**

Жизненно важные для критической инфраструктуры отрасли государства характеризуются наличием автоматизированных систем управления технологическими процессами. Они включают в себя системы диспетчерского управления и сбора данных, системы распределенного управления. Исходя из этого, выполнено исследование негативных последствий кибератак на объекты критической инфраструктуры. Приведены основные категории влияния деструктивных действий в автоматизированных системах технологическими процессами на объектах критической инфраструктуры. Показана взаимосвязь между кибератаками на объекте критической инфраструктуры и последствиями в промышленном секторе. Приведены критерии, по которым формируется перечень информационно-телекоммуникационных систем объектов критической инфраструктуры государства. Рассмотрены активы объектов критической инфраструктуры и ущерб, который может быть им причинен. Результаты проведенного исследования можно использовать при оценке актуальности киберугроз объектов критической инфраструктуры.

**Ключевые слова:** киберугроза, кибератака, критическая инфраструктура, последствия, автоматизированные системы управления, технологические процессы.

SERHII HONCHAR,
HENNADII LEONENKO

**CONSEQUENCES OF POSSIBLE CYBERATTACKS ON OBJECTS OF THE CRITICAL INFRASTRUCTURE**

Vital government areas for critical infrastructures defined by availability of automatic control systems of process industries. They include supervisory control and data acquisition systems, distributed control system. In this basis research of negative consequences possible cyberattacks on objects of a critical infrastructure is executed. The basic categories of influence of destructive actions in the automated systems by technological processes on objects of a critical infrastructure are resulted. The concept of object of a critical infrastructure reveals. The interrelation between cyberattacks on object of a critical infrastructure and consequences in industrial sector is shown. Criteria on which the list of information-telecommunication systems of objects of a critical infrastructure of the state is formed are resulted. Actives of objects of a critical infrastructure and a damage which can be caused them are considered. The statistics of incidents on objects of a critical infrastructure on branches for previous year is resulted. The diagram is resulted, where it is shown, that the greatest quantity of incidents is necessary on manufacture and power branch. The concept of a direct and indirect damage to information system of objects of a critical infrastructure reveals.It is shown, that recently in the world cyberattacks are directed on computer networks of power sector, a diplomatic corps, power departments, a defensive complex, the state enterprises, media of the companies. It is shown, that the

purpose such cyberattacks, first of all, drawing of a damage to a critical infrastructure of the state. Results of the carried out research can be used at an urgency estimation cyberthreats objects of a critical infrastructure.

**Keywords:** cyberthreat, cyberattack, critical infrastructure, consequences, automatic control system, process industries.

**Сергій Феодосійович Гончар**, кандидат технічних наук, заступник начальника центру, Державний науково-дослідний інститут спеціального зв'язку та захисту інформації, Київ, Україна.

E-mail: sfgonchar@gmail.com.

**Геннадій Павлович Леоненко**, кандидат технічних наук, старший науковий співробітник, учений секретар, Державний науково-дослідний інститут спеціального зв'язку та захисту інформації, Київ, Україна.

E-mail: leonenko2014@ukr.net.

**Сергей Феодосьевич Гончар**, кандидат технических наук, заместитель начальника центра, Государственный научно-исследовательский институт специальной связи и защиты информации, Киев, Украина.

**Геннадий Павлович Леоненко**, кандидат технических наук, старший научный сотрудник, ученый секретарь, Государственный научно-исследовательский институт специальной связи и защиты информации, Киев, Украина.

**Serhii Honchar**, candidate of technical sciences, deputy head of centre, State research institute for special telecommunication and information protection, Kyiv, Ukraine.

**Hennadii Leonenko**, candidate of technical sciences, senior researcher, scientific secretary, State research institute for special telecommunication and information protection, Kyiv, Ukraine.