CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION

УДК 004.056.53

СЕРГІЙ ГОНЧАР,
ГЕННАДІЙ ЛЕОНЕНКО

АНАЛІЗ ФАКТОРІВ ВПЛИВУ НА СТАН КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОБ'ЄКТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Виконано аналіз факторів, що впливають на стан кібербезпеки інформаційної системи об'єкту критичної інфраструктури. Розглянуто складові частини системи кіберзахисту інформаційних систем об'єктів критичної інфраструктури. Приведено модель взаємодії елементів інформаційної системи об'єкту критичної інфраструктури та здійснено аналіз їх впливу на стан кібезбезпеки даної системи. Досліджено чинники, вплив яких може спонукати інсайдера до можливого виконання ним деструктивних дій та дано рекомендації щодо мінімізації ймовірності здійснення інсайдером таких дій. Розглянуто питання нормативно-правової забезпечення кібербезпеки інформаційних систем об'єктів критичної інфраструктури. Результати проведеного аналізу можливо використати при розробці пропозицій та заходів щодо кіберзахисту інформаційних систем об'єктів критичної інфраструктури.

Ключові слова: кібербезпека, кіберзахист, критична інфраструктура, аналіз, фактори.

Постановка проблеми. Сучасний етап розвитку суспільства характеризується впровадженням новітніх технологій, що є ознакою рівня економічного розвитку країни. Зростаюча роль інформаційної сфери для економіки держави пов'язана із стрімким її входженням в комунікаційну, транспортну, енергетичну, фінансову, оборонну та інші сфери. А стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення є об'єкти критичної інфраструктури - 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 [1]. Тому, враховуючи, що у сучасному суспільстві кібератаки стають частішими та мають тенденцію чинити все значніший і триваліший вплив через підприємства на економіку країни, незаперечним є той факт, що надійний захист від кібератак активно впливає на стан економічної, політичної, соціальної, оборонної та інших складових національної безпеки держави.

Очевидним є той факт, що порушення функціонування об'єктів критичної інфраструктури держави може призвести до розвитку надзвичайних ситуацій, пов'язаних із загибеллю людей, екологічними катастрофами, заподіянням великого матеріального, фінансового, економічного збитку або великомасштабними порушеннями життєдіяльності міст та населених пунктів і т.п. У цих умовах надзвичайно важливу роль відіграє забезпечення безпеки, у тому числі і кібербезпеки об'єктів критичної інфраструктури держави.

Враховуючи зазначене вище, для розробки ефективних та адекватних пропозицій та заходів щодо кіберзахисту інформаційних систем об'єктів критичної інфраструктури необхідно здійснити аналіз факторів, що впливають на стан кібербезпеки зазначених об'єктів.

Фактори впливу на стан кібербезпеки. Проведений аналіз існуючих систем захисту інформації [2], дає змогу визначити основні складові частини системи кіберзахисту інформаційних систем об'єктів критичної інфраструктури:

- нормативно-правова;
- організаційна;

– технічна;
– підготовка, перепідготовка та підвищення кваліфікації відповідних фахівців.

Кожна із приведених вище складових частин, так чи інакше, впливає на стан кібербезпеки інформаційних систем об’єктів критичної інфраструктури.

Так, одними із актуальних питань є наявність нормативно-правової бази з питань забезпечення кібербезпеки інформаційних систем об’єктів критичної інфраструктури, приведення національної нормативно-правової бази з питань забезпечення кібербезпеки об’єктів критичної інфраструктури у відповідність з положеннями міжнародних документів; виконання узгодженості понятійного апарату, що використовується в існуючих національних законодавчих та нормативно-правових документах; доопрацювання (при необхідності - розробка) нормативних документів, вимог, методологій до оцінки загроз об’єктам, що є критичними для життєдіяльності держави, загальної методології оцінки ризиків для критично важливих об’єктів та критичної інфраструктури у цілому.

Крім того, слід зазначити, що керівники та/або власники об’єктів критичної інфраструктури повинні усвідомлювати можливість і ймовірність здійснення кібератак та наслідки, у випадку їх реалізації. Запровадження заходів з питань забезпечення кібербезпеки потребують залучення додаткових ресурсів, на що керівники цих об’єктів не завжди згодні, а механізм, який би вимагав від даних керівників запровадження необхідних заходів, відсутній. Тому, без запровадження згаданого механізму усі стандарти, інструкції тощо з питань забезпечення кібербезпеки інформаційних систем об’єктів критичної інфраструктури будуть носити рекомендаційний характер, оскільки та інформація, яка циркулює, наприклад, в автоматизованих системах управління технологічними процесами, не відноситься ні до одного виду інформації, що підлягає захисту згідно із чинним законодавством.

Інформаційні системи об’єктів критичної інфраструктури зазвичай являються об’єктом захисту, як цілісні утворення. В той же час, їх складові елементи: обслуговуючий персонал, математичне, програмне, технічне, інформаційне забезпечення тощо можливо розглядати, як окремі об’єкти захисту від кіберзагроз.

Кіберзагрози для інформаційних систем об’єктів критичної інфраструктури можуть виходити з різних джерел: навмисних, ненавмисних, природних. Основними з них є [3]: зловмисники, оператори ботнету, злочинні групи, іноземні спецслужби, інсайдери, фішери, сніфери, спамери, автори шпигунського і шкідливого програмного забезпечення, терористи, промислові шпигуни тощо.

На рис. 1 приведена модель взаємодії елементів інформаційної системи об’єкту критичної інфраструктури. Розглянемо, яким чином впливає кожна із складових систем (організаційна, технічна, персонал) на забезпечення кібербезпеки інформаційних систем об’єктів критичної інфраструктури.

Із приведеної моделі взаємодії можна бачити, що джерела кіберзагроз для інформаційних систем об’єктів критичної інфраструктури можуть знаходитись як ззовні (зовнішній порушник) так і зсередини (інсайдер).

При цьому, кібератакам зовнішнього порушника протистоїть система захисту інформації інформаційної системи об'єктів критичної інфраструктури, до функцій якої обов'язково повинні входити:

– захист периметра мережі;
– забезпечення безпеки міжмережевих взаємодій;
– моніторинг і аудит безпеки;
– виявлення і запобігання діям атак;
– резервне копіювання і відновлення даних;
– аналіз захищеності і керування політикою безпеки;
– контроль цілісності даних;
– захист від шкідливого програмного забезпечення;
– фільтрація контенту і запобігання витоку конфіденційної інформації;
– установка оновлень програмного забезпечення;
– адміністрування безпеки.

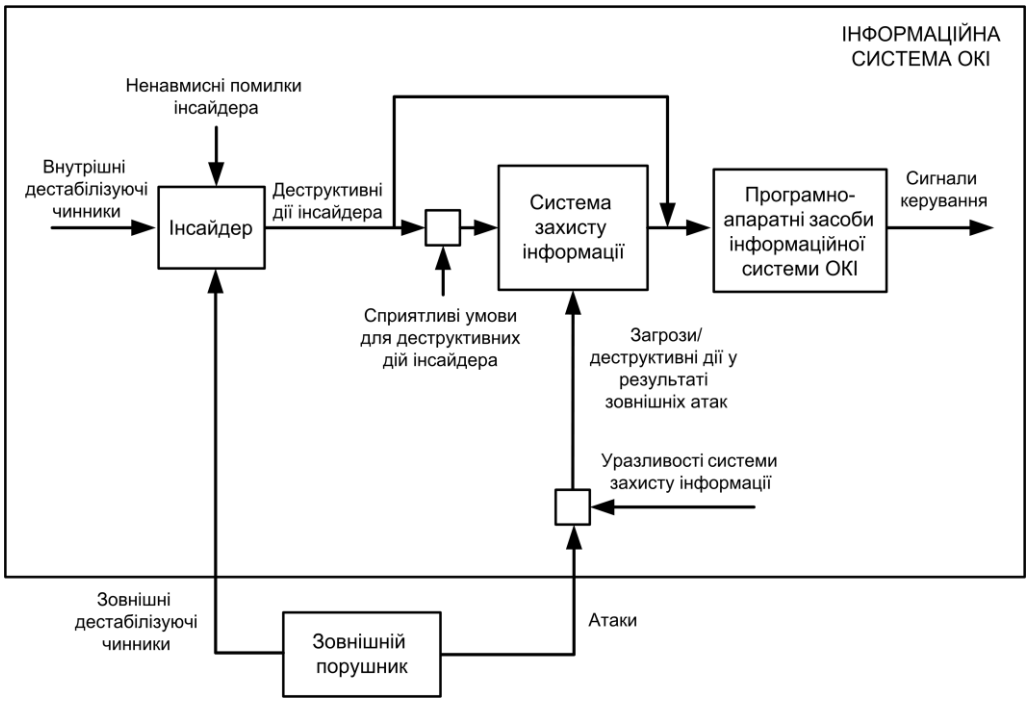

Рисунок 1 – Модель взаємодії елементів інформаційної системи об’єкту критичної інфраструктури.

За результатами проведеного аналізу загроз та уразливостей [4], можливо зазначити, що захист таких систем повинен розглядатися по наступних напрямках:

– захист інформаційних і фізичних компонентів інформаційної системи об’єктів критичної інфраструктури;

– технічний захист інформації інформаційних систем об'єктів критичної інфраструктури;

– захист процесів, процедур і програм обробки інформації інформаційних систем об’єктів критичної інфраструктури;

– захист каналів зв'язку інформаційних систем об’єктів критичної інфраструктури;

– придушення побічних електромагнітних випромінювань;

– керування та контроль системою захисту.

Однак, основна відмінність інсайдера від зовнішнього порушника полягає у тому, що інсайдер має легітимний доступ до системи. В той час, як зовнішній порушник прикладає зусилля, щоб подолати систему захисту, прагнучи отримати доступ до інформації, інсайдер отримує цю інформацію абсолютно безперешкодно в межах своєї компетенції або незаконно розширюючи свої права і можливості. Тому, будь-який захист системи від зовнішнього порушника виявляється неефективним проти інсайдера. При цьому, зовнішній порушник може здійснювати кібератаки на програмно-апаратну складову інформаційної системи, використовуючи уразливості системи захисту інформації інформаційної системи об’єкту критичної інфраструктури, або чинити інформаційно-психологічний вплив на інсайдера (зовнішні дестабілізуючі чинники).

Окрім зовнішніх дестабілізуючих чинників до можливих деструктивних дії інсайдера можуть спонукати внутрішні дестабілізуючі чинники - людські потреби, через захищеність яких може розкриватися забезпечення кібербезпеки інформаційної системи об’єкта критичної інфраструктури, а також власні ненавмисні помилки.

Внутрішніми дестабілізуючими чинниками можуть бути [5]:

– фізіологічні (природні): їжа, одежа, житло, відпочинок, комфорт, екологія тощо;

– потреби в безпеці: комфорт, постійність умов життя тощо;

– пізнавальні: активність, навички, уміння, діяльність, ініціатива, дослідницький пошук тощо;

– наукові: освіта (знання), виховання, мислення, цінна інформація, самосвідомість, істина тощо;

– соціальні: соціальні зв'язки, спілкування, увага до себе, спільна діяльність тощо;

– престижні: самоповага, повага зі сторони інших, визнання, досягнення успіху і високої оцінки, службове зростання тощо;

– духовні: щастя, свобода совісті, цілісність світогляду, доброта, честь тощо.

У залежності від того, які чинники спонукають інсайдера на деструктивні дії, останніх поділяють на типи. Ці типи розділяються у залежності від мети, мотивації і послідовності дій інсайдерів.

Необхідно відмітити, що якщо інсайдер отримує доступ до активів інформаційної системи об'єкта критичної інфраструктури незаконно розширюючи свої права та можливості, то для цього може бути необхідна наявність сприятливих умов. У випадку отримання інсайдером доступу до активів інформаційної системи об'єкта критичної інфраструктури у межах своєї компетенції необхідності у сприятливих умовах немає. Крім цього, при цьому обходиться система захисту інформації.

Тому, проведений аналіз показує, що з метою мінімізації ймовірності здійснення інсайдером деструктивних дій необхідно:

– вчасно виявляти та вживати певних заходів для зменшення впливу внутрішніх дестабілізуючих чинників;

– покращувати відбір співробітників на етапі прийняття на роботу та вживати відповідних заходів щодо підвищення їх фахового рівня для недопущення або мінімізації ненавмисних помилок.

Статистика кіберзагроз за даними Kaspersky Security Network (див. рис. 2), показує, що в Україні за третій квартал 2015 року у 33,7% випадків джерелом кіберзагроз був зовнішній порушник. В той же час, у 54,5% випадків кіберзагрози виникали через знімні носії.

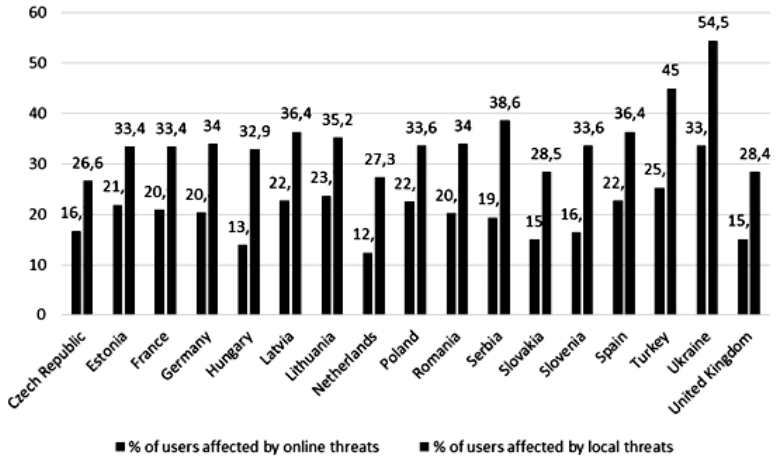

Рисунок 2 – Статистика кіберзагроз

Таким чином, із урахуванням викладеного можна зазначити, що на стан забезпечення кібербезпеки інформаційної системи об'єкта критичної інфраструктури впливають такі фактори:

– наявність необхідної та достатньої нормативно-правової бази з питань забезпечення кібербезпеки інформаційних систем об'єктів критичної інфраструктури;

– наявність джерел кіберзагроз, їх можливості, тип, вид, мета, мотиви, зацікавленість у здійсненні кібератак;

– наявність уразливостей у системах кіберзахисту, які можуть використовуватися при здійсненні кібератак;

– наявність чи відсутність сприятливих умов для реалізації кіберзагроз;

– привабливість активів, на які власне і спрямовуються кібератаки;

– наслідки від можливої реалізації кіберзагроз;

– рівень фахової підготовки співробітників, відповідальних за кібербезпеку на всіх рівнях: організація, підприємство, галузь, відомство тощо.

Також, одним із таких показників, на нашу думку може бути кількість кібератак за певний інтервал часу – рік, півріччя, квартал, місяць.

Крім того, одним із суттєвих показників може бути спрямованість кібератак – органи державної влади, енергетика, банківська сфера, силові відомства, дипломатичні установи тощо.

Корисним для оцінки та аналізу стану кібербезпеки може бути поєднання кількості кібератак за певний інтервал часу з урахуванням їх спрямованості. Це дасть змогу визначити вектор зацікавленості зловмисника та їх мету – кібердиверсія, кіберрозвідка, кібершпигунство тощо по відношенню до кожного напрямку.

Перелік показників, однозначно, може бути розширений з урахуванням досвіду та аналізу статистичних даних щодо приведених вище факторів.

Висновки. Виконано аналіз факторів, що впливають на стан кібербезпеки інформаційної системи об’єкту критичної інфраструктури. Результати проведеного аналізу можливо використати при розробці пропозицій та заходів щодо кіберзахисту інформаційних систем об’єктів критичної інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 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: Серп. 02, 2016.

[2] В.В. Домарев, *Безопасность информационных технологий. Методология создания систем защиты*. Киев, Украина: ООО “ТИД “ДС”, 2002.

[3] С.Ф. Гончар, Г.П. Леоненко, та О.Ю. Юдін, “Анализ угроз и уязвимостей индустриальных автоматизированных систем управления”, *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, № 2 (26), с. 9-14, 2013.

[4] International Electrotechnical Commission. 2009. *IEC 62443-1-1, Industrial communication network – Network and system security. Part 1-1: Terminology, concepts and models*. [Online]. Available: https://webstore.iec.ch/publication/7029. Accessed on: Aug. 02, 2016.

[5] Д.А. Ловцов, и Н.А. Сергеев, *Управление безопасностью эргасистем*. Москва, Россия: РАУ-Университет, 2001.

Стаття надійшла до редакції 20.09.2016.

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: Aug. 02, 2016.

[2] V.V. Domarev, *Safety of information technologies. Methodology of creation of systems of protection*. Kyiv, Ukraine: OOO “TYD “DS”, 2002.

[3] S.F. Honchar, H.P. Leonenko, and O.Y. Yudin, “Analysis of threats and vulnerabilities of industrial control systems”, *Legal, regulatory and metrological support of information security in Ukraine*, iss. 2 (26), pp. 9-14, 2013.

[4] International Electrotechnical Commission. 2009. *IEC 62443-1-1, Industrial communication network – Network and system security. Part 1-1: Terminology, concepts and models*. [Online]. Available: https://webstore.iec.ch/publication/7029. Accessed on: Aug. 02, 2016.

[5] D.A. Lovtsov, and N.A. Sergeev, *Control of ergasystems security*. Moscow, Russia: RAU-Universitet, 2001.

СЕРГЕЙ ГОНЧАР,
ГЕННАДИЙ ЛЕОНЕНКО

АНАЛИЗ ФАКТОРОВ ВЛИЯНИЯ НА СОСТОЯНИЕ КИБЕРБЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОБЪЕКТА КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Выполнен анализ факторов, влияющих на состояние кибербезопасности информационной системы объекта критической инфраструктуры. Рассмотрены составляющие системы киберзащиты информационных систем объектов критической инфраструктуры. Приведена модель взаимодействия элементов информационной системы объекта критической инфраструктуры, а также выполнен анализ их влияния на состояние кибезбезопасности данной системы. Проведено исследование факторов, влияние которых может побудить инсайдера к возможному выполнению им деструктивных действий, а также даны рекомендации по минимизации вероятности осуществления инсайдером таких действий. Рассмотрен вопрос нормативно-правового обеспечения кибербезопасности информационных систем объектов критической инфраструктуры. Результаты проведённого анализа можно использовать при разработке предложений и мероприятий по киберзащите информационных систем объектов критической инфраструктуры.

Ключевые слова: кибербезопасность, киберзащита, критическая инфраструктура, анализ, факторы.

SERHII HONCHAR,
HENNADII LEONENKO

ANALYSIS OF THE FACTORS INFLUENCING CONDITION CYBERSECURITY OF INFORMATION SYSTEM OF OBJECT OF THE CRITICAL INFRASTRUCTURE

The analysis of the factors influencing condition cybersecurity of information system of object of a critical infrastructure is made. Integral parts of systems of cyber protection of information systems of objects of a critical infrastructure are considered. The model of interaction of elements of information system of object of a critical infrastructure is resulted, and also the analysis of their influence on a condition of cybersecurity the given system is made. Functions which the system of cyber protection of information system of objects of a critical infrastructure necessarily should possess are resulted. Research of the factors which influence can induce insider to possible performance of destructive actions is carried out, and also recommendations about minimization of probability of realization by insider such actions are given. The concept of internal destabilizing factors is opened. Directions on which it should be considered cyber protection of information systems of objects of a critical infrastructure are formulated. The question of is standard-legal maintenance cybersecurity of information systems of objects of a critical infrastructure is considered. Some features in actions of insider information systems of objects of a critical infrastructure are considered. Results of the spent analysis can be used by working out of offers and actions on cyber protection of information systems of objects of a critical infrastructure.

Keywords: cybersecurity, cyber protection, critical infrastructure, analysis, factors.

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.