УДК 004.056.5

С. Ф. Гончар, Г. П. Леоненко, О. Ю. Юдін
ДержНДІ спецзв'язку, Київ

ТЕОРЕТИКО-МЕТОДОЛОГІЧНИЙ АСПЕКТ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Розглянуто питання щодо методології забезпечення інформаційної безпеки об'єктів критичної інфраструктури.

Ключові слова: автоматизовані системи управління технологічними процесами, об'єкти критичної інфраструктури.

THEORETIC-METHODOLOGICAL ASPECT OF INFORMATION SECURITY SUPPORT OF THE OBJECTS OF CRITICAL INFRASTRUCTURE

In this paper considered the question of the methodology of information security critical infrastructure.

Key words: automated control system, object of critical infrastructure.

Вступ

Сучасна цивілізація значною мірою залежить від засобів автоматизації виробничих процесів, а саме – автоматизованих систем управління технологічними процесами. Атомні й гідроелектростанції, нафто- і газопроводи, національні мережі розподілу електроенергії, транспортні системи національного і світового рівня, які належать до об'єктів критичної інфраструктури, функціонують на базі таких автоматизованих систем і від захищеності систем управління цими системами залежить не тільки прибуток компаній, але й національна безпека [1, 2].

Іноземні спецслужби, а також терористичні та кримінальні структури інтенсивно вдосконалюють методи та способи використання інформаційних технологій і засобів, щоб отримати можливість здійснення деструктивних інформаційних впливів на ресурси інформаційно-телекомунікаційних систем, мереж державних і недержавних організацій. Таке застосування інформаційних технологій і засобів надає їм властивості так званої інформаційної зброї. Щоб завдати значної шкоди інтересам держави та суспільства, інформаційну зброю можуть застосувати і в мирний час, особливо терористичні організації. Тому безпеку промислових об'єктів, зокрема підприємств оборонного комплексу, необхідно розглядати в новому ракурсі, а саме: разом з класичними заходами безпеки необхідно забезпечувати інформаційну безпеку автоматизованих систем управління технологічним процесом.

Узагальнення та систематизація світового досвіду у сфері інформаційної безпеки критичної інфраструктури дає змогу констатувати, що останніми роками західні спеціалісти приділяють особливу увагу оцінці впливу на життєво важливі об'єкти своїх країн і можливих наслідків цих впливів для політичної, економічної, екологічної та інших сфер діяльності держави. Очевидно, що в умовах сучасного надзвичайно інтенсивного розвитку інфраструктури провідних зарубіжних країн існує безліч критично важливих об'єктів, таких, наприклад, як великі гідротехнічні споруди, нафто-, газо-, продуктопроводи, мережі АЕС, ТЕС, ТЕЦ, пункти зберігання стратегічних запасів нафти і газу, шкідливі хімічні виробництва, транспортні вузли, аеродроми тощо, виведення з ладу яких може призвести до непередбачуваних важких і навіть катастрофічних наслідків.

У зв'язку з цим у Сполучених Штатах Америки, Франції, Німеччині, Японії та інших країнах проведено широкі дослідження для виявлення таких об'єктів на території США, Канади, Європи, що становлять загрозу для нормальної життєдіяльності цих країн у випадку впливу на них без'ядерної високоточної зброї або в результаті терористичних (диверсійних) актів.

Також пророблялися варіанти техногенних катастроф або руйнівних стихійних лих. У перелік виявлених критично важливих об'єктів не увійшли традиційні типи військових об'єктів – ракетні бази і полігони, авіаційні бази, органи вищого військового управління, оскільки, за оцінками дослідників, ці об'єкти мають досить високий ступінь захищеності й практично є малоуразливими до впливу звичайних засобів ураження. Крім того, навіть виведення з експлуатації таких об'єктів істотно не порушить системи життєзабезпечення держави і її керованості.

Детальний аналіз наукової розробленості проблеми забезпечення інформаційної безпеки критичної інфраструктури держави у вітчизняній та зарубіжній науці показує, що проблема формування та своєчасного оновлення концептуальних, доктринальних та нормативно-правових засад інформаційної безпеки критичної інфраструктури держави належить до найгостріших проблем сучасності. Вітчизняні та зарубіжні дослідники зайняті осмисленням інформаційної безпеки критичної інфраструктури держави як системи. Інакше кажучи, в низці робіт досліджуються основні елементи інформаційної безпеки критичної інфраструктури держави в їх єдності, тобто цілісно: принципи, категорії, закони, ідеї. Проте комплексних досліджень з проблематики забезпечення інформаційної безпеки критичної інфраструктури сьогодні обмаль, що не дає змоги сформувати панорамне бачення управлінських проблем у зазначеній сфері.

Крім того, розбіжності у вживанні понять і термінів, їх нез'ясованість, нерозмежованість за обсягом та значенням, як у наукових дослідженнях, так і у міжнародно-правових актах, свідчать про те, що осмислення основних понять, складових елементів системи забезпечення інформаційної безпеки критичної інфраструктури з їх багатогранними проявами та наслідками ще не завершено. Так, сьогодні провідні країни світу проходять шлях стандартизації термінології та підходів у сфері захисту критичної інфраструктури, зокрема, ці процеси активно відбуваються в США [3].

Аналіз нормативних документів

Проведені дослідження показують явну недостатність стандартів з аналізу ризиків в Україні порівняно з провідними країнами і, головне, слабку узгодженість понятійного апарату, що використовується. Практичне вирішення проблем стандартизації, сертифікації забезпечення якості та ефективності систем комплексної безпеки в Україні сьогодні гостро затребуване, і з кожним роком з розвитком автоматизованих систем управління об'єктами критичної інфраструктури буде ще більше затребуване та потребуватиме гармонізації з міжнародними стандартами.

Стандарти з питань забезпечення інформаційної безпеки об'єктів критичної інфраструктури є базовими документами, які вводять загальні поняття і містять загальні вимоги до:

- політики безпеки;
- організації інформаційної безпеки (управління, узгодженість, розподіл відповідальності, процеси авторизації для уможливлення обробки інформації, угоди про конфіденційність, виявлення ризиків, пов'язаних із зовнішніми організаціями тощо);
- управління ресурсами (відповідальність ресурсів: облікові записи, права користування, без дозволу; класифікація інформації: рекомендації щодо класифікації, маркування та поводження з інформацією);
- безпека людських ресурсів;
- фізична безпека та безпека навколишнього середовища;
- управління виробництвом і засобами зв'язку;
- контроль доступу;
- системи збору інформації, розроблення і експлуатації;
- керування інцидентами інформаційної безпеки;
- безперервність управління виробництвом.

Складові частини систем захисту

Аналіз наявних систем, зокрема систем захисту інформації [4], дає змогу визначити основні складові частини систем захисту інформації об'єктів критичної інфраструктури:

- законодавча, нормативно-правова, науково-методична база;
- організаційна структура і завдання органів державної влади, підрозділів організацій, які повинні забезпечувати інформаційну безпеку об'єктів критичної інфраструктури;
- організаційно-технічні та режимні заходи та методи (політика інформаційної безпеки);
- технічні програмно-апаратні методи і засоби захисту інформації;
- підготовка, перепідготовка та підвищення кваліфікації відповідних фахівців у сфері забезпечення інформаційної безпеки об'єктів критичної інфраструктури.

Основні завдання із забезпечення інформаційної безпеки

Основні завдання із забезпечення безпеки інформації на об'єктах критичної інфраструктури держави такі:

- нормативне, правове регулювання у сфері забезпечення безпеки інформації в критичній інфраструктурі держави;
- визначення загроз безпеки інформації та виявлення уразливостей у програмному та апаратному забезпеченні об'єктів критичної інфраструктури держави;
- оцінка реальної захищеності критичної інфраструктури держави;
- розроблення вимог щодо забезпечення безпеки інформації в критичній інфраструктурі держави;
- розроблення та реалізація заходів для убезпечення інформації в критичній інфраструктурі держави;
- підготовка фахівців із забезпечення безпеки інформації в критичній інфраструктурі держави;
- здійснення контролю і нагляду в галузі забезпечення безпеки інформації в критичній інфраструктурі держави;
- інформаційне, матеріально-технічне і науково-технічне забезпечення безпеки інформації в критичній інфраструктурі держави.

Напрями забезпечення інформаційної безпеки

Визначаючи основні напрями забезпечення інформаційної безпеки об'єктів критичної інфраструктури, можна зазначити, що першочерговим є завдання створення дієвого механізму координації зусиль органів влади та підрозділів організацій, які повинні забезпечувати інформаційну безпеку відповідних об'єктів.

Крім того, необхідно впроваджувати істотні заходи на державному, регіональному та галузевому рівнях з організаційного, нормативно-правового та науково-методичного забезпечення, а саме:

- здійснення загального керівництва у сфері забезпечення інформаційної безпеки критичної інфраструктури держави загалом;
- здійснення законодавчого регулювання відносин у сфері забезпечення інформаційної безпеки критичної інфраструктури держави;
- розроблення Стратегії забезпечення інформаційної безпеки критичної інфраструктури держави;
- розроблення і виконання державних цільових програм забезпечення інформаційної безпеки критичної інфраструктури;
- розроблення та затвердження Державного реєстру об'єктів критичної інформаційної інфраструктури;
- виконання загальнодержавних заходів щодо забезпечення сталого функціонування об'єктів критичної інформаційної інфраструктури;
- координація та контроль діяльності органів державної влади, органів місцевого самоврядування щодо забезпечення належного функціонування та захисту об'єктів інформаційної безпеки критичної інфраструктури;

- здійснення державного контролю за станом забезпечення інформаційної безпеки об'єктів критичної інфраструктури;
- здійснення методичного керівництва щодо забезпечення належного функціонування об'єктів критичної інформаційної інфраструктури;
- здійснення інформаційного, матеріально-технічного і науково-технічного забезпечення безпеки інформації в критичній інфраструктурі держави.

Як показує досвід розвинених країн, дослідження механізмів захисту інформації об'єктів критичної інфраструктури передбачає на перших кроках етап ідентифікації (визначення) елементів, які повинні розглядатися як об'єкти критичної інфраструктури. Разом з тим важливим напрямом забезпечення захисту інформації на об'єктах критичної інфраструктури є запровадження відповідного управлінського впливу, який передбачається здійснювати в декілька етапів [5]:

- ідентифікація елементів критичної інфраструктури;
- оцінка загроз інформаційній безпеці об'єктів критичної інфраструктури;
- формування системи забезпечення інформаційної безпеки об'єктів критичної інфраструктури;
- оцінка стану та можливостей системи забезпечення інформаційної безпеки об'єктів критичної інфраструктури;
- розроблення та впровадження інструментарію системи забезпечення інформаційної безпеки об'єктів критичної інфраструктури;
- моніторинг, спостереження та контроль.

Щодо захисту автоматизованих систем управління технологічними процесами, за результатами проведеного аналізу загроз та уразливостей [6], можливо зазначити, що захист цих систем повинен розглядатися у таких напрямах:

- захист інформаційних і фізичних компонентів автоматизованих систем управління технологічними процесами;
- технічний захист інформації на об'єктах автоматизованих систем управління технологічними процесами;
- захист процесів, процедур і програм обробки інформації в автоматизованих системах управління технологічними процесами;
- захист каналів зв'язку в автоматизованих системах управління технологічними процесами;
- придушення побічних електромагнітних випромінювань;
- керування системою захисту та контроль.

Етапи створення систем захисту

Аналіз відомих методик (послідовностей) проведення робіт із формування складових частин систем захисту інформації об'єктів критичної інфраструктури, таких як організаційно-технічні та режимні заходи та методи (політика інформаційної безпеки), програмно-технічні методи і засоби захисту інформації, надає змогу виділити основні етапи їх створення:

- визначення інформаційних і технічних ресурсів, а також об'єктів інформаційних систем, які підлягають захисту – об'єктів захисту;
- формування переліку потенційно можливих загроз і каналів витоку інформації на об'єктах критичної інфраструктури;
- оцінка ризиків завдання збитків компонентам системи за наявності уразливостей, загроз, сприятливих умов для реалізації цих загроз, а також каналів витоку інформації;
- визначення вимог до системи захисту інформації;
- здійснення вибору засобів захисту інформації та їх характеристик;
- упровадження і організація використання вибраних заходів, способів і засобів захисту;
- здійснення контролю цілісності та керування системою захисту.

До функцій системи захисту інформації об'єктів критичної інфраструктури повинні обов'язково входити:

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

Класифікація наслідків порушення інформаційної безпеки

Небезпека загроз та атак в автоматизованих системах управління технологічними процесами визначається оцінкою можливих наслідків їх реалізації з позиції впливу на функціонування автоматизованих систем управління технологічними процесами, а рівень тяжкості таких наслідків – коефіцієнтом небезпеки цієї атаки, який визначається експертним методом. Одним із варіантів є класифікація важкості можливих наслідків за такими показниками [7]:

- фізичний вплив – вплив на населення, кількість постраждалих, загиблих, травмованих осіб, а також чисельність евакуйованого населення;
- економічний вплив – вплив на ВВП, розмір економічних втрат – як прямих, так і непрямих;
- екологічний вплив – вплив на населення та навколишнє природне середовище;
- політичний вплив – вплив на впевненість та дієздатність влади;
- взаємозв'язок з іншими елементами критичної інфраструктури та тривалість впливу.

Враховуючи наведені вище категорії впливу порушення інформаційної безпеки об'єктів критичної інфраструктури, 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 бренда або довіри клієнтів.

Зазначимо, що елементи наведеного переліку не є незалежними. Очевидно, що один з наслідків може призвести до іншого.

Висновки

Враховуючи викладене, можна сформулювати такі висновки:

- проблема формування та своєчасного оновлення законодавчих, організаційних, нормативно-правових, методично-наукових засад інформаційної безпеки об'єктів критичної інфраструктури, а також удосконалення кадрового механізму належить до актуальних проблем сучасності;
- досліджено ступінь наукової розробленості проблем забезпечення інформаційної безпеки критичної інфраструктури держави у вітчизняній та зарубіжній науці;

- показано явну недостатність стандартів з аналізу ризиків в Україні порівняно з провідними країнами і, головне, слабку узгодженість понятійного апарату, що використовується;
- дослідження вітчизняних та зарубіжних фахівців показують необхідність підходів до розроблення та впровадження систем захисту інформації на об'єктах критичної інфраструктури як системи;
- наведено методологічні засади щодо розроблення та впровадження систем захисту інформації на об'єктах критичної інфраструктури;
- сформульовано основні завдання із забезпечення безпеки інформації на об'єктах критичної інфраструктури держави.

1. Гончар С. Ф. Шляхи удосконалення державної політики забезпечення інформаційної безпеки критичної інфраструктури України: матеріали круглого столу "Державне реагування на загрози національним інтересам України: актуальні проблеми та шляхи їх розв'язання", 19 лютого 2014 р., Київ, НАДУ при Президентові України (кафедра національної безпеки). – 2014. – С. 92–95. 2. Леоненко Г. П., Юдин А. Ю. Проблемы обеспечения информационной безопасности систем критически важной информационной инфраструктуры Украины // Information Technology and Security. – 2013. – Вип. 1(3). – С. 44. 3. Юдин А. Ю., Пирогов Г. В. Анализ и оценка нормативных документов, применяемых для обеспечения информационной безопасности Smart Grid систем / А. Ю. Юдин // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2013. – №1. – С. 88. 4. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты. – К: ООО "ТИД "ДС", 2002 – 688 с. 5. Шевченко М. М. Методика системно-комплексного дослідження державного управління забезпеченням національної безпеки / М. М. Шевченко // Вісник Національної академії оборони України. – 2010. – № 4. – С. 235–240. 6. Гончар С. Ф. Аналіз ймовірності реалізації загроз захисту інформації в автоматизованих системах управління технологічним процесом / С. Ф. Гончар // Захист інформації. – 2014. – Том 16, № 1. – С. 40–46. 7. Council Directive 2008/114/EC "On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection" [Електронний ресурс]. – Режим доступу: http://eurlex.europa.eu.