Oorschot P. C., Vanstone S. A. Handbook of Applied Cryptography. – CRC Press, 2001. – 816 p. ***3.*** *Fiat A., Shamir A. How to Prove Yourself: Practical Solutions to Identification Signature Problems // Proceedings of Advances in Cryptology CRYPTO '86, Springer-Verlag, 1987. – P. 186–194.* ***4.*** *Feige U., Fiat A., Shamir A. Zero Knowledge Proofs of Identity // Proceedings of the lPth Annual ACM Symposium on the Theory of Computing, 1987. – P. 210–217.* ***5.*** *Guillou L.C., Quisquater J.-J. A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Transmission and Memory // Proceedings of Advances in Cryptology EUROCRYPT'88, Springer-Verlag, 1988. – P. 123–128.* ***6.*** *Schnorr C.P. Efficient Signature Generation for Smart Cards // Proceedings of Advances in CRYPTO '89, Springer-Verlag, 1990. – P. 239–252.* ***7.*** *Яремчук Ю. Є. Метод автентифікації сторін взаємодії на основі рекурентних послідовностей // Сучасний захист інформації. – №1, 2013. – С. 4–10.* ***8.*** *Яремчук Ю. Є. Можливість автентифікації сторін взаємодії на основі рекурентних послідовностей // Захист інформації. – Том 15, №4, 2013. – С. 394–398.* ***9.*** *Патент України на корисну модель № 84271, (51) МПК (2013.01) H03M 13/00. Спосіб автентифікації сторін взаємодії на основі електронного коду / Ю. Є. Яремчук. – № заявки u2013 06319; заявл. 22.05.2013; опубл. 10.10.2013, бюл. №19.* ***10.*** *Яремчук Ю. Є. Методи автентифікації на основі рекурентних послідовностей // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Випуск 1(25), 2013. – С. 39–49.* ***11.*** *NIST SP 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications / A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo. – National Institute of Standards and Technology, 2010. – 131 p.* ***12.*** *Иванов М. А., Чугунков И. В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с.*

Юрій Васильєв
ДержНДІ Спецзв'язку

УДК 004.056

АНАЛІЗ МІЖНАРОДНОГО ДОСВІДУ ЩОДО ВИЗНАЧЕННЯ КЛЮЧОВИХ СИСТЕМ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Анотація: ***Наведено міжнародний досвід у нормативному визначені ключових системам інформаційної інфраструктури.***
Summary: ***Regulatory identify systems of key information infrastructure.***
Ключові слова: ***Інформація, інформаційна безпека, ключові системи інформаційної інфраструктури***

I Вступ

У кожному суспільстві можливо виділити сектори, системи або мережі, від яких життєво залежить суспільство і порушення функціонування яких може привести до колапсу на загальнодержавному, регіональному або місцевому рівні. Комплекс цих секторів, систем або мереж почали називати ключовими або критичними системами інформаційної інфраструктури (далі - КСІІ).

Багато держав, а також терористичних та кримінальних структур інтенсивно вдосконалюють методи і способи використання інформаційних технологій та засобів для деструктивних інформаційних впливів на інформаційні ресурси інформаційно-телекомунікаційних систем і мереж державних та недержавних організацій. Таке застосування інформаційних технологій та засобів надає їм властивості так званої інформаційної зброї. Для нанесення значного збитку інтересам держави і суспільства інформаційна зброя може бути застосована і в мирний час, особливо терористичними організаціями. При цьому порушення функціонування КСІІ може призвести до розвитку надзвичайних ситуацій, пов'язаних із загибеллю людей, екологічними катастрофами, нанесенням великої матеріальної, фінансової, економічної шкоди або великомасштабними порушеннями життєдіяльності міст та населених пунктів і т.п. У цих умовах важливу роль відіграє державне регулювання діяльності щодо забезпечення безпеки інформації в КСІІ.

Необхідно зазначити, що на даний час в Україні проблематика, що пов'язана з визначенням КСІІ, оцінюванням актуальних загроз безпеки, побудовою систем захисту та нормативно-правовим забезпеченням цих процесів знаходяться на початковому рівні та наполегливо потребує розвитку.

У зв'язку з нарощуванням з 1998-го року загрози тероризму в розвинених країнах почалися дискусії про уразливість національних інфраструктур. Аналізи були направлені не тільки на кібернетичні інфраструктурні системи, але і на решту областей і секторів забезпечення життя суспільства. У США PRESIDENTIAL DECISION DIRECTIVE/NSC-63 [1] визначили КСІІ як основні системи, які можуть мати матеріальну або кібернетичну платформу і мають дію на функціональність економіки держави. Ці основні системи вбирали в

себе системи телекомунікації, енергосистеми, банківський і фінансовий сектори і служби, транспортну систему, постачання водою і рятувальні служби.

ІІ Основна частина

Питаннями КСІІ на національному рівні почали з 1998-го року займатися і європейські держави. Суспільним знаменником цієї діяльності було, перш за все, надання особливого значення охороні інформаційних і комунікаційних технологій.

В Європі проблематикою КСІІ раніше всіх почали займатися у Великобританії, де в кінці 1999-го року була визначена ключова система національної інфраструктури як система, спадкоємність якої важлива для функціонування держави, втрата або порушення якої мало б або могло б піддавати загрозі життя громадян, могло б нанести серйозні негативні економічні або соціальні наслідки для суспільства чи її крупної частини. У таку систему були включені державне управління, запасні служби, енергетика і паливо, подача води, телекомунікації, забезпечення продовольством, санітарія, фінанси і економіка, комунікаційні мережі і служби, юстиція і захист громадського порядку, соціальне обслуговування, освіта, наука, а також, прогноз погоди.

В результаті терористичних нападів на об'єкти в США, які відбулися 11.09.2001, проблематика КСІІ і їх захист прийняли новий об'єм і масштаб. У лютому 2003-го року в США була прийнята Національна стратегія фізичної охорони критичної інфраструктури і ключових споруд (National Strategy for Physical Protection of Critical Infrastructure and Key Assets) [2], в якій критична інфраструктура визначена як системи устаткування, матеріальні і віртуальні, які життєво важливі для США і пошкодження або руйнування яких мав би вплив на зменшення безпеки, національної економічної безпеки, національного суспільного здоров'я, або на будь-яку їх комбінацію. До секторів критичної інфраструктури були віднесені: сільське господарство, продовольство, вода, здоровий спосіб життя, запасні (рятувальні) служби, бази оборонної промисловості, телекомунікації, енергетика, транспорт, банківська справа і фінанси, хімічна промисловість і небезпечні речовини, поштове обслуговування. До ключового устаткування були віднесені національні культурні пам'ятники, ядерні електростанції, дамби (греблі), урядові і комерційні будівлі і інші місця, де концентрується велика кількість людей.

Голландський уряд прийняв в 2001 році план боротьби проти тероризму, складовою частиною якого є — проект захисту КСІІ. Після проведення аналізів ідентифіковано 11 секторів КСІІ, а саме: енергогосподарство, телекомунікації, питна вода, продукти, санітарія, фінанси, відведення поверхневої води, загальний порядок і безпека, законність, суспільні органи і транспорт.

У Чеській Республіці до 2002 року проблематика КСІІ зосереджувалася, перш за все, на комп'ютерних мережах. Під КСІІ в Чеській Республіці розуміються системи, руйнування або зменшення функціональності яких мав би серйозний вплив на економічну і суспільну стабільність, обороноздатність, безпеку і функціонування держави. У 2002 році були визначені сектори національної критичної інфраструктури, особливо комплекс силового обслуговування, комплекс подачі води, комплекс баластного господарства, транспортна мережа, комунікаційні і інформаційні системи, банковий і фінансовий сектор, запасні служби, публічні служби, державне управління і самоврядування.

У Польщі критична інфраструктура була визначена як функціонально сполучені засоби виробництва, інститути, служби, що є ключовими для безпека країни і її громадян, для забезпечення правильного функціонування як державних і самокерованих органів і установ, так і комерційного (приватного) сектора.

У Російської Федерації відповідно до доручення Президента РФ від 28.09.2006 №Пр-1649 «Основы государственной политики в области обеспечения безопасности населения РФ и защищенности критически важных и потенциально опасных объектов от угроз техногенного, природного характера и террористических актов» затверджено розпорядженням Уряду РФ № 411-РС от 23.03.06 «Перечень критически важных объектов Российской Федерации» та розроблено ряд нормативних документів щодо забезпечення захисту КСІІ:

- «Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007);
- «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007);
- «Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007);
- «Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 19.11.2007);

Об'єднання народних економік держав ЄС, їх взаємозалежність, але і необхідність протистояти сумісним або подібним погрозам, відбилися в ухваленні документа Critical Infrastructure protection in the fight against

terrorism [3]. У цьому документі КСІІ визначена як фізичні засоби виробництва, інформаційні технології, мережі (транспортні, енергетичні і т. п.), служби і інші активи, розлад або руйнування яких мало б серйозні впливи на здоров'я, охорону, надійність або життєвий рівень громадян або на штатне функціонування урядів в цих державах.

Виходячи з аналізу світового досвіду до КСІІ входять:

- енергетичні об'єкти і мережі, наприклад, електричні розподільні мережі, газопроводи, нафтопроводи, збірки пального і т. п.;
- комунікаційні і інформаційні технології (наприклад, телекомунікації, радіомовні і телевізійні передавачі і мережі, інтернет);
- фінансова система (банкова справа, ринки капіталу, інвестування);
- охорона здоров'я, особливо лікарні, поліклініки, установи постачання крові, лабораторії, сантехнічна рятувальна служби;
- харчова промисловість, сільське господарство, торгівля і постачання продовольством;
- вода, особливо греблі, гідроресурси;
- транспорт, особливо авіаційний, шосейний, залізничний, комбінований, комунікаційні вузли, а також системи управління транспортом;
- виробництво, зберігання і транспорт небезпечних товарів, особливо хімічних, біологічних, радіологічних ядерних матеріалів;
- державне управління, зокрема критичні служби і установи, інформаційні мережі, важливі економічні об'єкти, стратегічні об'єкти, а також культурні пам'ятники.

Критеріями того, чи можна дану систему інформаційної інфраструктури визначити як ключову, є:

- територіальна досяжність негативних результатів, наприклад транснаціональний, народний, регіональний, локальний (місцевий) і т. п.;
- велика кількість наслідків, наприклад, гуманітарних, матеріальних, економічних, політичних або збитки і втрати відносно навколишнього середовища;
- часовий ефект наслідків, особливо коли з'являться негативні наслідки (наприклад: негайно, за 24 год.) і як довго можуть продовжуватися (наприклад: до 24 годин, до 3 днів і т. п.).

Захист КСІІ можемо визначити як сукупність заходів, які плануються і виконуються з метою:

- визначати і захищати ті системи інформаційної інфраструктури держави, що є ключовими з погляду збереження їх безпеки, функціональності, економічної і суспільної стабільності, причому необхідно рівноцінно оцінювати як державну, так і приватну сферу;
- забезпечити функціональність системи раннього попередження появи кризових ситуацій і захист тієї системи інформаційної інфраструктури, яка важлива для вирішення кризових ситуацій.

Мова йде, перш за все, про КСІІ, які є важливими з точки зору:

- забезпечення правильного функціонування уряду, органів державного управління і самоврядування, переважно в області безпеки і забезпечення основних (життєвих) товарів і послуг;
- функціональності державної і приватної сфери при забезпеченні правильного ходу економіки і функціонування суспільних служб;
- забезпечення внутрішнього порядку, суспільної стабільності і безпеки громадян.

Захист КСІІ виконуватиметься завжди як результат аналітичного процесу, зміст якого складається з:

- ідентифікації КСІІ на національному, регіональному і локальному рівні;
- ідентифікації релевантних ризиків для КСІІ;
- аналізу уразливості окремих КСІІ;
- оцінки ризиків порушення або знищення КСІІ;
- ухвалення відповідних запобіжних заходів.

Система захисту КСІІ представляє сукупність організаційних і технічних заходів для забезпечення захисту КСІІ від різних загроз (терористів, диверсантів, екстремістів), у разі появи надзвичайних або кризових ситуацій, та і від наслідків ненавмисних дій, які могли б нанести збитки для критичної інфраструктури.

Ефективна система захисту КСІІ повинна успішно протистояти різним загрозам при адекватному рівні охоронних заходів, залежно від значення КСІІ, потенційних загроз і їх можливих наслідків.

Загальні вимоги спрямовані на забезпечення діяльності в цій області органів виконавчої влади, органів місцевого самоврядування, підприємств і організацій (господарюючих суб'єктів), у віданні яких перебувають КСІІ .

Основними завданнями щодо забезпечення безпеки інформації в КСІІ є:

- нормативне правове регулювання в галузі забезпечення безпеки інформації в КСІІ;

- визначення загроз безпеки інформації і виявлення вразливостей в програмному і апаратному забезпеченні КСІІ;
- оцінка реальної захищеності КСІІ;
- розробка вимог щодо забезпечення безпеки інформації в КСІІ;
- розробка та реалізація заходів щодо забезпечення безпеки інформації в КСІІ;
- підготовка фахівців у галузі забезпечення безпеки інформації в КСІІ;
- здійснення контролю та нагляду в галузі забезпечення безпеки інформації в КСІІ;
- інформаційне, матеріально-технічне та науково-технічне забезпечення безпеки інформації в КСІІ.

При цьому, зазначені завдання можуть вирішуватися на діючих КСІІ, при модернізації, а також в ході їх проектування та створення. Загальні вимоги щодо забезпечення безпеки інформації в КСІІ розглядаються з урахуванням необхідності вирішенні цих завдань.

До КСІІ відносяться інформаційно-керуючі або інформаційно-телекомунікаційні системи, які безпосередньо здійснюють управління критично важливими об'єктами та (або) інформаційне забезпечення управління такими об'єктами. КСІІ можуть входити до складу наступних сегментів інформаційної інфраструктури:

- системи органів державної влади;
- системи органів управління правоохоронних структур;
- системи фінансово-кредитної і банківської діяльності;
- системи попередження і ліквідації надзвичайних ситуацій;
- географічні та навігаційні системи;
- мережі зв'язку загального користування на ділянках, що не мають резервних або альтернативних видів зв'язку;
- супутникові системи, що використовуються для забезпечення органів управління і в спеціальних цілях;
- системи управління транспортуванням нафти, нафтопродуктів і газу;
- програмно-технічні комплекси центрів управління взаємно зв’язаної мережі зв'язку;
- системи управління водопостачанням;
- системи управління енергопостачанням;
- системи управління транспортом (наземним, повітряним, морським);
- системи управління потенційно небезпечними об'єктами;
- системи, які не відносяться до вищевказаних, але порушення штатного режиму функціонування яких може призвести до порушення функцій управління чутливими для держави процесами зі значними негативними наслідками.

До основних особливостей КСІІ, які суттєво впливають на зміст вимог щодо забезпечення безпеки інформації, можливо віднести такі:

- технологічна інформація (забезпечує управління технологічними або чутливо важливими процесами), програмно-технічна інформація (програми системного і прикладного характеру, що забезпечують функціонування КСІІ) , командна (керуюча) та вимірювальна інформація, яка не відноситься до інформації з обмеженим доступом (якщо в таких системах циркулює інформація з обмеженим доступом, то вона підлягає захисту відповідно до діючих вимог та норм з технічного захисту інформації);
- управління безперервними технологічними процесами, що обумовлює значно жорсткіші вимоги до часу і порядку виконання автоматизованих функцій, неможливість відключення на період проведення контрольних заходів в інтересах забезпечення безпеки інформації та оцінки їх реальної захищеності від негативних інформаційних впливів;
- різноманітність КСІІ, наявність в них різнорідних, територіально та просторово розподілених елементів з поєднанням різноманітних інформаційних технологій;
- надзвичайна небезпека наслідків виведення з ладу та (або) порушення функціонування КСІІ;
- широке застосування операційних систем реального часу, необхідність адаптації програмних та програмно-апаратних засобів захисту до цих операційних систем;
- неможливість відключення систем для проведення заходів щодо забезпечення безпеки інформації.

Ключові системи різняться між собою:

- за функціональним призначенням;
- за належністю до сфери діяльності держави, суспільства (міністерству, відомству);
- за перевагою у розмірі збитку у разі виведення з ладу (порушення функціонування);
- за ступенем однорідності системи;
- за ступенем розподіленості системи;
- з базування елементів.

Залежно від призначення, складу, розміщення та особливостей функціонування КСІІ розрізняється склад актуальних загроз безпеки інформації, а, отже, і зміст пропонованих вимог щодо забезпечення безпеки інформації. Загрози безпеці інформації виникають при появі джерела загроз і вразливостей в КСІІ. Джерелами загроз безпеки інформації в КСІІ можуть бути:

- іноземні розвідувальні та спеціальні служби у разі недружньої політики іноземних держав, у тому числі в області поширення нових інформаційних технологій з різного роду обмеженнями на постачання сучасних технологій;
- терористичні організації та кримінальні структури;
- окремі сторонні особи або групи осіб з корисливими чи іншими інтересами (хакери тощо);
- представники конкуруючих фірм і організацій, іноземних економічних структур, діяльність яких спрямована проти інтересів державних структур, великих компаній, організацій і підприємств;
- обслуговуючий персонал КСІІ, у функціональні обов'язки якого не входять питання, пов’язані з функціонуванням системи (електрики, техніки, прибиральниці та інший персонал обслуговуючих підрозділів).

Вразливості КСІІ можуть мати місце в охороні системи та її елементів, в системному і прикладному програмному забезпеченні (у тому числі через помилки при його створенні і установці, неправильної конфігурації і т. п.), у процедурах доступу до оброблюваної інформації та контролю такої обробки.

Реалізовані при цьому загрози можуть бути спрямовані:

- на умисне або ненавмисне знищення або модифікацію даних, її системного і прикладного програмного забезпечення;
- на розкрадання (копіювання, крадіжку), розголошення інформації, яка може бути використана для порушення функціонування ключової системи;
- на реалізацію збоїв в роботі апаратного та програмного забезпечення шляхом навмисного або випадкового електромагнітного впливу на елементи КСІІ;
- на руйнування носіїв інформації, елементів комунікації КСІІ .

ІІІ Висновки

З урахуванням викладеного, метою формування вимог щодо забезпечення безпеки інформації в КСІІ є регламентація діяльності господарюючих суб'єктів у сфері забезпечення безпеки інформації в КСІІ в інтересах протидії можливим загрозам безпеки інформації або мінімізації збитків від їх реалізації та збереження тим самим стійкого і безпечного функціонування КСІІ в умовах можливих деструктивних інформаційних впливів:

- організації забезпечення безпеки інформації в КСІІ і дій, пов’язаних з виникненням надзвичайних ситуацій;
- програмного і апаратного забезпечення безпеки інформації в КСІІ, в тому числі в інтересах збереження цілісності та доступності критично важливої інформації, її реєстрації та обліку;
- забезпечення безпеки при взаємодії КСІІ з відкритими (загального користування) інформаційними системами та мережами;
- забезпечення безпеки інформації при захисті від шкідливих програм;
- дій, пов’язаних з обслуговуванням і модернізацією КСІІ, процедур проведення огляду (атестації) організацій на право діяльності з надання державних послуг в галузі забезпечення безпеки інформації в КСІІ, здійснення державного контролю (нагляду) у галузі забезпечення безпеки інформації в КСІІ, оцінки відповідності забезпечення безпеки інформації в КСІІ встановленим вимогам.

Список використаної літератури: ***1.*** *Presidential Decision Directive/NSC-63 [Електронний ресурс]. – Режим доступу: https://www.fas.org/irp/offdocs/pdd/pdd-63.htm* ***2****. National Strategy for Physical Protection of Critical Infrastructure and Key Assets [Електронний ресурс]. – Режим доступу: http://www.dhs.gov/national-strategy-physical-protection-critical-infrastructure-and-key-assets* ***3****. Critical Infrastructure protection in the fight against terrorism [Електронний ресурс]. – Режим доступу: http://europa.eu/legislation_summaries/justice_ freedom_security/fight_against_terrorism/l33259_en.htm*