http://egap.in.ua/

ISBN 978-966-2214-78-9

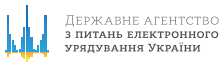
ЕЛЕКТРОННЕ УРЯДУВАННЯ *та* ЕЛЕКТРОННА ДЕМОКРАТІЯ

Навчальний посібник у 15 частинах

ЗАХИСТ ІНФОРМАЦІЇ В СИСТЕМАХ ЕЛЕКТРОННОГО УРЯДУВАННЯ

частина 13

Київ • 2017



Публікація підготовлена за підтримки Швейцарської агенції розвитку та співробітництва в рамках програми «Електронне врядування задля підзвітності влади та участі громади», що реалізується Фондом Східна Європа та Фондом InnovaBridge спільно з Державним агентством з питань електронного урядування України.

Програма EGAP спрямована на використання новітніх інформаційно-комунікаційних технологій (ІКТ), що допомагають вдосконалити якість врядування, покращують взаємодію влади та громадян та сприяють соціальним інноваціям в Україні.

Більше про програму EGAP: egap.in.ua

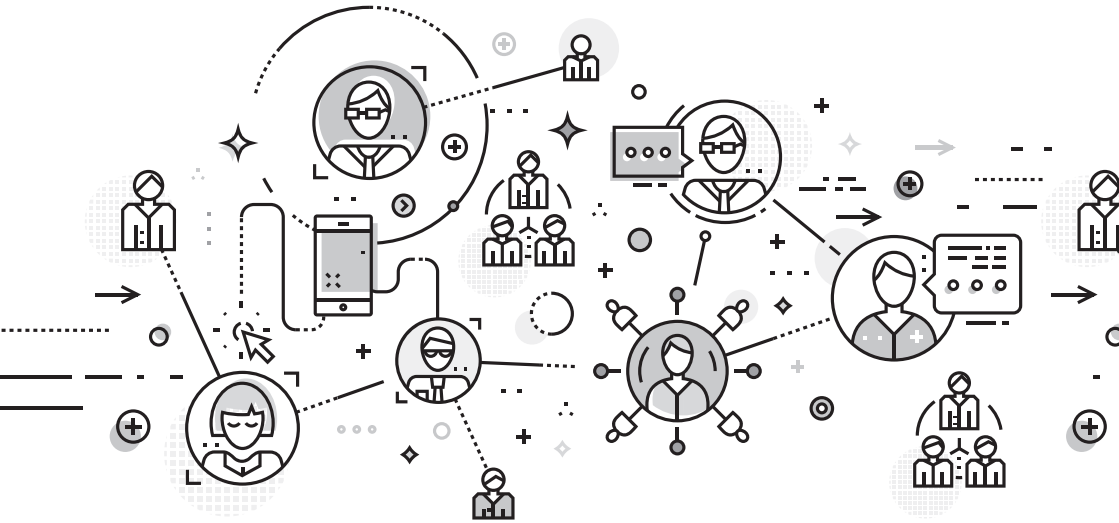
ЕЛЕКТРОННЕ УРЯДУВАННЯ *та* ЕЛЕКТРОННА ДЕМОКРАТІЯ

Навчальний посібник у 15 частинах

ЗАХИСТ ІНФОРМАЦІЇ В СИСТЕМАХ ЕЛЕКТРОННОГО УРЯДУВАННЯ

частина

13



Київ • 2017

УДК 35.078:681.518

ББК 67.400+32.81
Е45

Схвалено Вченою радою Національної академії державного управління при Президентові України (протокол № 240/11-10 від 24 листопада 2016 р.)

Рецензенти

Орлов О. В., доктор наук з державного управління, професор, завідувач кафедри інформаційних технологій і систем управління Харківського регіонального інституту державного управління НАДУ при Президентові України;

Лопушинський І. П., доктор наук з державного управління, професор, завідувач кафедри державного управління та місцевого самоврядування Херсонського національного технічного університету;

Місников Ю. Г., доктор філософії, експерт з питань електронного урядування ООН, країн Європи та СНД;

Архипська О. І., експерт з урядування, Transparency International Україна, член Координаційної ради з питань реалізації в Україні Ініціативи Партнерство «Відкритий Уряд».

Е45 **Електронне урядування та електронна демократія**: навч. посіб.: у 15 ч. / за заг. ред. А.І. Семенченка, В.М. Дрешпака. – К., 2017.
Частина 13: Захист інформації в системах електронного урядування / [О.М. Хошаба]. – К.: ФОП Москаленко О. М., 2017. – 72 с.

ISBN 978-966-2214-78-9

Видання містить навчальні матеріали для викладання теми «Захист інформації в системах електронного урядування» та самостійної роботи тих, хто навчається. Розкрито поняття, сутність та завдання захисту інформації. Аналізуються загрози інформаційної безпеки в системах електронного урядування та визначаються рівні протидії таким загрозам безпеки. На прикладах розкрито підходи до реалізації політики безпеки інформації в системах е-урядування. Здійснено системний аналіз та розкрито практичні аспекти застосування засобів протидії загрозам інформаційної безпеки на законодавчому, адміністративному і процедурному рівнях. Уміщено завдання до практичних робіт, що передбачають закріплення отриманих знань щодо безпечної роботи з інформаційними ресурсами мережі Інтернет, з криптографічними, стеганографічними та антивірусними засобами захисту інформації в операційній системі Windows.

Для студентів і слухачів спеціальності «Публічне управління та адміністрування», слухачів курсів підвищення кваліфікації державних службовців і посадових осіб місцевого самоврядування, студентів та аспірантів інших спеціальностей, представників громадських організацій та бізнесу, які опановують питання електронного урядування та електронної демократії.

ISBN 978-966-2214-78-9

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АЦСК – Акредитований центр сертифікації ключів
ЄС – Європейський Союз
ЗІ – захист інформації
ІБ – інформаційна безпека
ІТКС – інформаційно-(теле)комунікаційні системи
ІР – інформаційні ресурси
ІС – інформаційна система
КСЗІ – комплексна система захисту інформації
ОПУ – органи публічного управління
ОС – операційна система
ПБ – політика безпеки
СУІБ – система управління інформаційною безпекою
ЕЦП – електронний цифровий підпис
ЦСК – Центр сертифікації ключів

ВСТУП

Сучасний стан розвитку інформаційного простору характеризується новими потребами у створенні умов для безпечного функціонування його суб'єктів, коли особливо важливими стають проблеми протидії інформаційним війнам та захист власного кіберпростору. Тому *актуальними питаннями*, що розкриті в цьому модулі, є визначення основних понять, сутності та завдань захисту інформації, ознайомлення з Концепцією технічного захисту інформації в Україні, аналіз основних загроз інформаційній безпеці в системах електронного урядування (е-урядування) та вивчення основних методів протидії їм, що надає можливість використовувати отримані знання та навички на практиці.

Ця тема дозволяє отримати необхідні *знання* щодо основних понять, сутності та завдань захисту інформації та *вміння* щодо виявлення, запобігання й подолання найбільш поширених загроз інформаційній безпеці в системах е-урядування. Питання, що розглядаються у межах цього модуля, також пов'язані з іншими темами курсу, а саме: з проблематикою безпечного використання інформаційних ресурсів мережі Інтернет під час електронної взаємодії.

Метою цього модуля є опрацювання теми захисту інформації в системах е-урядування та безпечної роботи з інформаційними ресурсами корпоративних комп'ютерних мереж та мережі Інтернет.

Досягнення поставленої мети забезпечується виконанням таких завдань:

- вивчення основних понять, сутності та завдань захисту інформації;
- визначення загроз інформаційній безпеці в системах е-урядування;
- визначення рівнів протидії загрозам інформаційній безпеці в системах е-урядування;
- опанування підходів щодо практичної реалізації політики безпеки в системах е-урядування.

Виконання практичних робіт надасть змогу набути навичок щодо безпечної роботи з інформаційними ресурсами мережі Інтернет, з криптографічними, стеганографічними та антивірусними засобами захисту інформації в операційній системі Windows.

Структура модуля передбачає вивчення трьох розділів. До кожного з них розроблено завдання для практичних занять, які проводяться як з використанням наданого матеріалу, так і інших рекомендованих джерел – наукових публікацій, ресурсів Інтернет. Опановуючи матеріали модуля «Захист інформації в системах електронного урядування», необхідно ознайомитися з основними поняттями, сутністю і завданнями захисту інформації, підходами до визначення загроз безпеці інформації в системах е-урядування та їх класифікації. Надалі треба зосередитися на вивченні відомих методів протидії загрозам безпеці інформації. Також важлива послідовність виконання практичних завдань та робіт, під час яких формуються відповідні вміння та навички.

Кожна практична робота передбачає: ознайомлення з джерелами, інформаційними ресурсами мережі Інтернет та вивчення прикладних програмних засобів, у тому числі засобів шифрування та стеганографії, антивірусних, моніторингових та інших.

Тим, хто самостійно опановує цю тему, доцільно звернути увагу на практичну частину курсу, а саме: безпечна робота з інформаційними ресурсами мережі Internet, з криптографічними, стеганографічними та антивірусними засобами захисту інформації в операційній системі Windows.

Слухачам магістратури за спеціальністю «Публічне управління та адміністрування» рекомендуємо приділити особливу увагу вивченню законодавчого, адміністративного та процедурного рівнів протидії загрозам інформаційної безпеки в системах е-урядування.

1. ПОНЯТТЯ, СУТНІСТЬ І ЗАВДАННЯ ЗАХИСТУ ІНФОРМАЦІЇ

1.1. Основні визначення та поняття інформаційної безпеки

Згідно із Законом України «Про інформацію»[1] у його першій редакції інформація визначалася як «систематизовані, документовані, публічно оголошені або іншим чином поширені відомості про суспільне, державне життя та навколишнє природне середовище». У чинній редакції цього Закону це поняття розкрите як «будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді».

Інформація має певні властивості (рис. 1):

- *цінність* – визначається можливістю забезпечення досягнення мети, поставленої її отримувачем;
- *достовірність* – відповідність отриманої інформації реальності навколишнього світу;
- *актуальність* – відповідність цінності та достовірності отриманої інформації поточному часу.

З позиції інформаційної безпеки *інформація* має такі властивості (рис. 1):

- *конфіденційність* – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем;
- *цілісність* – означає неможливість модифікації неавторизованим користувачем;
- *доступність* – властивість інформації бути отриманою авторизованим користувачем, за наявності у нього відповідних повноважень, в необхідний для нього час.

Іноді ще визначають таку властивість інформації, як *спостережність* – властивість увесь час (на всіх етапах обробки та передавання) знаходитись під контролем *системи захисту*.

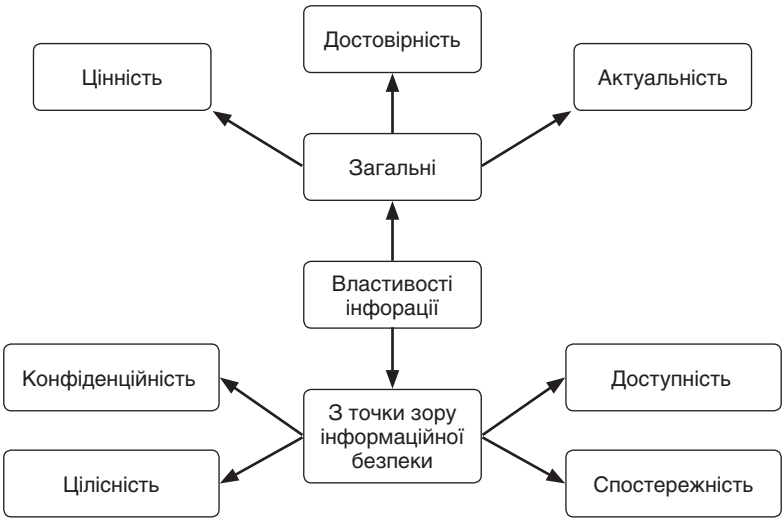


Рис. 1. Властивості інформації

Інформаційною безпекою (у контексті безпосередньої діяльності із захисту інформації) може вважатись комплекс заходів, що спрямовані на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення даних.

Інформаційну безпеку за сферою застосування можна розглядати у контексті безпеки держави, організації та особистості.

Інформаційна безпека держави – це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди. Шкода може бути заподіяна через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Інформаційна безпека організації – це цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів з досягнення стану захищеності інформаційного середовища організації. Така діяльність повинна забезпечувати нормальне функціонування і динамічний розвиток організації.

Інформаційна безпека особистості характеризується як стан її безпосередньої захищеності від негативних інформаційних впливів, а також впливів на її власну здатність шукати, збирати, обробляти та використовувати інформацію. Інформаційна безпека особистості також передбачає відповідну захищеність різноманітних соціальних груп та об'єднань людей, до яких вона входить.

Згідно з українським законодавством[2], вирішення проблеми *інформаційної безпеки* на рівні *держави* має здійснюватися за допомогою:

- створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;
- підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їхніх наслідків, здійснення міжнародного співробітництва з цих питань;
- вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;
- розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація.

Вирішення проблеми *інформаційної безпеки* на рівні *держави* має здійснюватися за допомогою:

- законодавчих, нормативно-правових та нормативних актів щодо інформаційної безпеки;
- міжнародними стандартами ISO;
- власними розробками.

Для *реалізації* законодавчих, нормативно-правових та нормативних актів щодо *інформаційної безпеки* повинна створюватись комплексна система захисту інформації (КСЗІ).

Для *реалізації* міжнародних стандартів ISO щодо інформаційної безпеки повинна створюватись система управління інформаційною безпекою (СУІБ).

До *державних органів* забезпечення інформаційної безпеки відносяться:

- відповідні підрозділи спецслужб держави;
- спеціально уповноважений орган держави з питань захисту інформації: Державна служба спеціального зв'язку та захисту інформації України;
- Національний координаційний центр кібербезпеки;
- Міжвідомча комісія з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України.

З 1 липня 2015 року у Державній службі спеціального зв'язку та захисту інформації України розпочав роботу Державний центр кіберзахисту та протидії кіберзагрозам. Його створено на базі Державного центру захисту інформаційно-телекомунікаційних систем Держспецзв'язку.

До органів забезпечення інформаційної безпеки в *системі е-урядування* належать:

- Державне агентство з питань електронного урядування України;
- Державна служба спеціального зв'язку та захисту інформації України;
- Міністерство юстиції України (в частині роботи з електронними цифровими підписами (ЕЦП);
- підрозділ з інформаційного забезпечення органу публічного управління, який серед інших завдань також має займатися створенням і підтриманням систем управління інформаційною безпекою та використовує комплексну систему захисту інформації в системі електронного урядування, що використовується.

Необхідно також визначити, що у *Стратегії кібербезпеки України* підкреслено, що мають бути створені умови для залучення підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інфраструктури, до забезпечення кібербезпеки України. Також мають бути врегульовані питання щодо обов'язковості вжиття ними заходів із забезпечення *захисту інформації* та кіберзахисту відповідно до вимог законодавства, а також щодо сприяння ними державним

органам у виконанні завдань із забезпечення кібербезпеки та кіберзахисту. Держава має сприяти залученню наукових установ, навчальних закладів, організацій, громадських об'єднань і громадян до розробки та реалізації заходів із кібербезпеки і кіберзахисту.

1.2. Сутність захисту інформації

Термін «*захист інформації*» (або англ. *Data protection*) визначає сукупність методів і засобів, що забезпечують *цілісність*, *конфіденційність* і *доступність* інформації за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації[3].

У широкому розумінні *захист інформації* являє собою протистояння *користувачів*, *володільців інформації* і *зловмисників*. Щодо певної інформації *зловмисник* виступає як суб'єкт, який незаконним шляхом намагається добути, змінити або знищити інформацію користувачів.

З позицій забезпечення захисту інформації в інформаційно-телекомунікаційних системах (ІТКС) до *суб'єктів захисту* відносять володільців інформації, власників системи, користувачів та спеціально уповноважений центральний орган виконавчої влади[4].

До *об'єктів захисту* в ІТКС відносять безпосередньо інформацію та програмне забезпечення, яке призначене для обробки цієї інформації.

Вважається що *захист інформації* має слабкі у формальному плані завдання, тобто завдання, що не мають відомих формальних методів вирішення, і характеризується таким:

- велика або іноді важко встановлювана кількість факторів, що впливають на побудову ефективного захисту;
- відсутність точних вихідних або вхідних даних;
- у більшості випадків відсутність адекватних математичних методів досягнення оптимального результату за сукупністю вихідних даних.

Тому вважається[5], що жодна *система захисту* не може тривалий час протистояти цілеспрямованим діям озброєного сучасними технологіями кваліфікованого *зловмисника*. Важливо розуміти, що *система захисту інформації* не може забезпечити стовідсотковий ефект. При

цьому визначається певний рівень *інформаційної безпеки*, який відображає припустимий ризик її спотворення, знищення, несанкціонованого доступу та витоку. Тому основне завдання *захисту інформації* полягає в тому, щоб злам системи відбувся якомога пізніше та/або не мав суттєвих наслідків для її функціонування й використання інформації, що нею циркулює.

Це правило існує роками і має універсальний характер. Воно не залежить від рівня *системи захисту*, сумлінності користувачів та адміністраторів, апаратного та програмного забезпечення. Правило стверджує, що проблема полягає не в тому, чи подолають зловмисники *систему захисту*, а в тому, коли це відбудеться і чи матиме це суттєве значення для системи і її володільців, власників, користувачів.

Основною *метою захисту інформації в системах е-урядування* є забезпечення *інформаційної безпеки* безпосередньо цих систем, публічних службовців і громадян, що ними користуються, та системи публічного управління в цілому. *Інформаційна безпека* у цьому контексті є станом захищеності систем обробки та зберігання даних, при якому забезпечується конфіденційність, доступність і цілісність інформації. Його може бути досягнуто завдяки застосуванню комплексу заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення даних.

1.3. Завдання у сфері захисту інформації

До основних *завдань у сфері захисту інформації (ЗІ)* в інформаційно-телекомунікаційних системах у цілому належать:

- керування доступом користувачів до інформаційних ресурсів систем з метою захисту від неправомірного випадкового або навмисного втручання у роботу і несанкціонованого (із перевищенням наданих повноважень) доступу до програмних і апаратних ресурсів як персоналу, так і сторонніх осіб;
- захист даних, що передаються каналами зв'язку;
- *захист інформації* з обмеженим доступом від витоку;
- *захист інформації* від спеціальних впливів;
- реєстрація, збереження і надання даних про події, що відбувалися у системі і стосувалися *інформаційної безпеки (ІБ)*;

- контроль роботи користувачів системи адміністраторами та обов'язкове повідомлення адміністратора безпеки про будь-які спроби несанкціонованого доступу до ресурсів системи;
- контроль і підтримка цілісності критичних ресурсів *системи захисту* і середовища виконання прикладних програм;
- забезпечення функціонування програмно-технічних комплексів з метою *захисту інформації* від впровадження у роботу потенційно небезпечних програм і засобів подолання *системи захисту*;
- керування та моніторинг засобів *захисту інформації.*

Вищезазначені завдання у сфері *захисту інформації* та *інформаційної безпеки* покладені в основу Концепції технічного захисту інформації в Україні[6], яка є складовою забезпечення національної безпеки України.

Концепція технічного захисту інформації визначає основи державної політики у сфері захисту інформації інженерно-технічними заходами. *Технічний захист інформації в Україні* – це діяльність, що спрямована на забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності (унеможливлення блокування) інформації з обмеженим доступом, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави. Концепція технічного захисту інформації також визначає загрози безпеці інформації, стан її технічного захисту та систему технічного захисту інформації як сукупність суб'єктів, об'єднаних цілями та певними завданнями. У *Концепції технічного захисту інформації* зазначені принципи формування і проведення державної політики у цій сфері, описані основні функції організаційних структур.

Конкретні завдання у сфері захисту інформації, що розробляються на рівні певної організації, системи публічного управління чи держави в цілому, мають підпорядковуватися заздалегідь визначеній стратегії у цій сфері. Стратегія *захисту інформації* є основою для побудови комплексу заходів щодо *інформаційної безпеки*. Суть організації стратегії захисту інформації визначається як пошук оптимального компромісу між необхідністю використання конкретних засобів захисту і наявними ресурсами для реалізації цього захисту. У стратегії захисту інформації визначаються мета, критерії, принцип і процедури, необхідні для побудови надійної системи[7]. Таким чином, важливою особливістю загальної стратегії захисту інформації є проектування системи інформаційної безпеки, де визначаються напрями:

визначення мети та задач захисту інформації, цільової установки об'єктів та суб'єктів захисту інформації; визначення загроз інформаційної безпеки; визначення рівнів протидії загрозам та побудова політики інформаційної безпеки.

Висновки

1. Інформація має такі властивості як цінність, достовірність та актуальність. Доцільно розглядати такі властивості як загалом, так і з точки зору захисту інформації. З точки зору захисту інформації ще існують такі властивості як конфіденційність, цілісність, доступність та спостережність.

2. Інформаційну безпеку за сферою застосування необхідно розглядати у контексті безпеки держави, організації та особистості. Для реалізації законодавчих, нормативно-правових та нормативних актів щодо інформаційної безпеки повинна створюватись комплексна система захисту інформації.

3. Захист інформації охоплює сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації. У широкому розумінні захист інформації являє собою протистояння користувачів, володільців інформації і зловмисників.

4. Концепція технічного захисту інформації в Україні є складовою забезпечення національної безпеки України та визначає основи державної політики у сфері захисту інформації інженерно-технічними засобами. Стратегія захисту інформації визначає основу для побудови комплексу заходів щодо інформаційної безпеки, передбачаючи необхідні, конкретні засоби захисту, які є найбільш дієвими з точки зору наявних інформаційних, фінансових та людських ресурсів.

Запитання для самоконтролю

1. Які властивості має інформація? Наведіть приклади.
2. Які властивості має інформація з позиції інформаційної безпеки? Наведіть приклади.

3. Як визначається інформаційна безпека у контексті національної безпеки держави, організації та особистості?
4. Для чого необхідні комплексна система захисту інформації (КСЗІ) та система управління інформаційною безпекою (СУІБ)?
5. Які державні органи та органи в системі е-урядування забезпечують інформаційну безпеку в Україні?
6. Яке значення має термін «захист інформації»?
7. Чому жодна система захисту не може тривалий час протистояти діям зловмисників?
8. Які існують завдання у сфері захисту інформації в інформаційно-телекомунікаційних системах?
9. Що визначає Концепція технічного захисту інформації?

Рекомендована література

1. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII, із змінами. – Режим доступу: zakon2.rada.gov.ua/laws/show/2657-12. – Назва з екрану.
2. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94-вр, із змінами. – Режим доступу: zakon5.rada.gov.ua/laws/show/80/94-вр. – Назва з екрану.
3. Про Положення про технічний захист інформації в Україні: Указ Президента України від 27.09.1999 р. № 1229/99. – Режим доступу: zakon3.rada.gov.ua/laws/show/1229/99. – Назва з екрану.
4. Про затвердження Концепції технічного захисту інформації в Україні: постанова Кабінету Міністрів України від 08.10.1997 р. № 1126, із змінами. – Режим доступу: zakon3.rada.gov.ua/laws/show/1126-97-п. – Назва з екрану.
5. Остапов С.Е. Технології захисту інформації: навч. посіб. / С.Е. Остапов, С.П. Євсеєв, О.Г. Король. – Х.: ХНЕУ, 2013. – 476 с.

2. ВИЗНАЧЕННЯ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ В СИСТЕМАХ ЕЛЕКТРОННОГО УРЯДУВАННЯ

2.1. Основні проблеми безпечного функціонування систем електронного урядування

Практика впровадження *систем електронного урядування* в різних країнах світу існує понад два десятиліття[8]. За цей час накопичено істотний як позитивний, так і негативний досвід. Правильне використання узагальнених результатів таких впроваджень дозволяє економити фінансові та людські ресурси, зменшити кількість помилок, розв'язати проблеми стандартизації, уніфікації та взаємодії національних систем електронного урядування з міжнародними.

Під час побудови сучасних систем з *електронного урядування* необхідно враховувати досвід різних країн світу у впровадженні подібних систем в галузі основних принципів, підходів та методів створення корпоративних інформаційних структур.

Серед *загальних проблем*, з якими зіткнулись країни під час впровадження електронного урядування були різні підходи щодо вирішення різних труднощів. Так, наприклад, для більшості країн однією з головних проблем було забезпечення сумісності різнорідних інформаційних систем, що створювались в різні роки, за різними принципами, на різних технологічних платформах.

Системи електронного урядування працюють на основі інформаційних систем, що побудовані на корпоративних комп'ютерних мережах. Тому, на функціонування *систем електронного урядування* мають вплив також проблеми, характерні для корпоративних структур. З цими проблемами доводиться стикатися як фахівцям у галузі технічного обслуговування, так і службам інформаційної безпеки у сфері публічного управління. До основних причин, що призводять до виникнення таких проблем, можна віднести такі:

1. Складність і різнорідність програмного та апаратного забезпечення, що використовуються в системах електронного урядування.

У практиці побудови систем електронного урядування для реалізації важливих завдань використовуються різні операційних системи. Робочі місця публічних службовців найчастіше оснащені операційною системою (ОС) Windows, обробка інформації в системах електронного документообігу та важливі інформаційні ресурси зберігаються в базах даних, які знаходяться в ОС Linux, FreeBSD, Solaris. Усе частіше публічні службовці використовують портативні мобільні пристрої (планшети, смартфони), які працюють в ОС Android та iOS. У даному випадку проблема полягає в технічному обслуговуванні (управлінні конфігураціями і оновленнями програмних засобів) та проведенні стандартних, базових заходів у галузі інформаційної безпеки.

2. Велика кількість вузлів в системах електронного урядування.

Велика кількість вузлів корпоративної мережі в *системах електронного урядування*, їх територіальна розподіленість і відсутність часу для контролю конфігураційних параметрів основних програмних засобів створюють значну проблему. Часто вузли, в яких відбувається обробка важливої інформації, об'єднані в корпоративну мережу *системи електронного урядування*, розташовані у різних місцях не тільки в межах міста, але й регіону або навіть країни. Ця особливість, а також відсутність часу на контроль необхідних налаштувань програмних засобів, не дозволяє технічному персоналу своєчасно контролювати діяльність і безпеку користувачів у розподілених системах електронного урядування.

3. Наявність зовнішнього доступу до системи електронного урядування.

Однією з важливих проблем, що виникають внаслідок експлуатації *системи електронного урядування* є підключення зовнішніх користувачів (підприємств, організацій, окремих громадян) до відкритих сервісів і надання прав персоналу органу публічного управління щодо віддаленої роботи з внутрішніми інформаційними ресурсами, з одного боку, і збільшення загальної кількості вразливостей, що постійно з'являються у корпоративній мережі, з іншого. Вразливості, що існують в програмному забезпеченні *системи електронного урядування* можуть призводити до несанкціонованого доступу до інформаційних ресурсів. Тому для їх усунення та забезпечення належного рівня захищеності інформації в *системах електронного урядування* застосовуються різні механізми і засоби забезпечення безпеки. Відповідне налаштування таких засобів залежить від технології обробки інформації, що прийнята в системах публічного адміністрування.

Сукупність таких правил, законів і практичних рекомендацій описується в політиці безпеки, яка охоплює різні особливості процесу обробки інформації. До засобів, що забезпечують політику безпеки і, відповідно, ефективний захист технологій обробки інформації, можна віднести: міжмережеві екрани, системи виявлення атак, системи шифрування трафіку, системи контролю «мобільного коду» (Java, ActiveX) та інші засоби.

4. Функціонування груп технічного обслуговування та інформаційної безпеки.

У *системах електронного урядування* група технічного обслуговування в основному займається вирішенням питань системного і мережевого адміністрування. Група інформаційної безпеки займається питаннями, пов'язаними з процесами у галузі інформаційної безпеки на адміністративному, організаційному, технічному та інших рівнях. При цьому виникає проблема чіткого розмежування функціональних обов'язків персоналу цих груп, який обслуговує технічний рівень. Наприклад, обслуговування віддаленого доступу користувачів до інформаційних ресурсів системи електронного урядування; робота з основними службами і сервісами корпоративної мережі: DNS, електронна пошта; прикладні системи; електронного документообігу тощо.

Таким чином, під час створення та використання *системи електронного урядування* потрібне вирішення важливих проблем як з її технічного обслуговування, так і щодо інформаційної безпеки.

2.2. Поняття та види загроз інформаційній безпеці

У *Стратегії кібербезпеки України* сказано, що загрози кібербезпеці актуалізуються через дію деяких чинників, зокрема, як:

- невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам;
- недостатній рівень захищеності критичної інформаційної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, від кіберзагроз;
- безсистемність заходів кіберзахисту критичної інформаційної інфраструктури;
- недостатній розвиток організаційно-технічної інфраструк-

тури забезпечення кібербезпеки та кіберзахисту критичної інформаційної інфраструктури та державних електронних інформаційних ресурсів;

- недостатня ефективність суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру;
- недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки.

У *Стратегії національної безпеки України* підкреслено, що загрози інформаційній безпеці складають ведення інформаційної війни проти України, відсутність цілісної комунікативної політики держави та недостатній рівень медіа-культури суспільства.

До *загроз інформаційній безпеці* відносять сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам суспільства, держави та особистості. Загалом під *загрозою інформаційній безпеці*[9] прийнято розуміти потенційно можливу подію, дію, процес або явище, які можуть призвести до нанесення шкоди системі. За більш деталізованим визначенням, *загроза інформаційній безпеці системи* – це можливість реалізації впливу на інформацію, що призводить до порушення *конфіденційності, цілісності* або *доступності* даних, а також можливість впливів на компоненти системи, які можуть призводити до *втрати* або *знищення* інформації чи збою функціонування ІС.

Класифікація *загроз інформаційній безпеці* може бути здійснена за багатьма ознакам. Наведемо найпоширеніші з них (рис. 2).

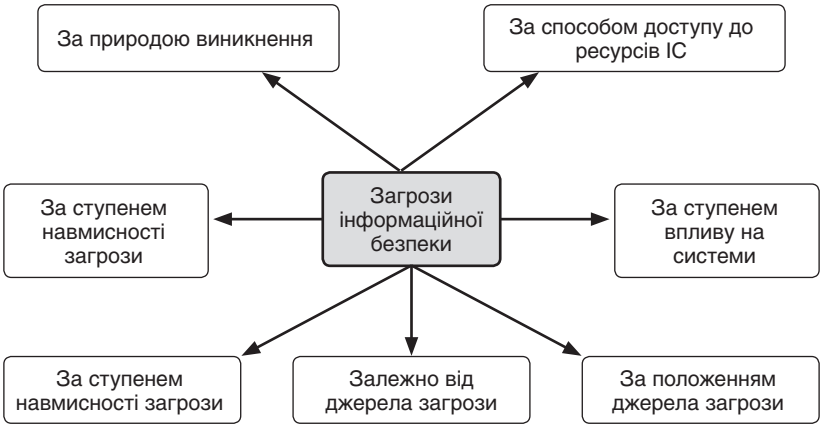


Рис. 2. Класифікація загроз інформаційній безпеці

1. За природою виникнення:

1.1. Природні – загрози, що виникли в результаті дії на ІС об'єктивних фізичних процесів або стихійних природних явищ, що не залежать від людини (природними загрозами можуть бути пожежі, повені, цунамі, землетруси, техногенні збої). Неприємна особливість таких загроз – надзвичайна складність або, навіть, неможливість їх прогнозування.

1.2. Штучні загрози – такі, що викликані дією людського фактора.

2. За ступенем навмисності загрози:

2.1. Випадкові – обумовлені халатністю або ненавмисними помилками персоналу. Як приклади випадкових загроз можна привести ненавмисне введення помилкових даних, ненавмисне псування устаткування.

2.2. Навмисні – зазвичай виникають у результаті цілеспрямованої діяльності зловмисника. Приклад навмисної загрози – під час роботи з Web-інтерфейсом інформаційної системи на базу даних може бути використана атака за допомогою SQL-ін'єкцій з метою зміни або вилучення важливих даних.

3. Залежно від джерела загрози:

3.1. Загрози, джерелом яких є природне середовище. Приклади таких загроз – різке підвищення (пониження) температури атмосфери, геомагнітні аномалії, повені, буревії, інші стихійні лиха.

3.2. Загрози, джерелом яких є людина. Прикладом такої загрози може служити влаштування недержавною організацією своїх довірених осіб, які діють в її інтересах, на посади, що займаються обслуговуванням державних ІС.

3.3. Загрози, джерелом яких є санкціоновані програмно-апаратні засоби. Приклад такої загрози – некомпетентне використання системних утиліт.

3.4. Загрози, джерелом яких є несанкціоновані програмно-апаратні засоби. До таких загроз можна віднести, наприклад, інсталяцію в систему кейлогерів. Використання особистих носіїв (флешок, MP3-плеєрів, мобільних телефонів) можуть містити шкідливе програмне забезпечення.

4. За положенням джерела загрози:

4.1. Загрози, джерело яких розташоване зовні контрольованої

зони. Приклади таких загроз – перехоплення побічних електромагнітних випромінювань або перехоплення даних, що передаються каналами зв'язку; дистанційна фото- і відеозйомка; перехоплення акустичної інформації з використанням направлених мікрофонів.

4.2. Загрози, джерело яких розташоване в межах контрольованої зони. Прикладами подібних загроз може бути застосування пристроїв для підслуховування або розкрадання носіїв, що містять конфіденційну інформацію.

5. За ступенем впливу на системи:

5.1. Пасивні загрози – при реалізації не здійснюють ніяких змін у складі та структурі ІС. Прикладом пасивної загрози може бути несанкціоноване копіювання файлів з даними.

5.2. Активні загрози. Реалізація активних загроз порушує структуру ІС. Наприклад, проникнення зловмисника до інформаційних ресурсів системи електронного урядування з метою моніторингу та перегляду вмісту мережевого трафіку для перехоплення паролів або інших важливих даних.

6. За способом доступу до ресурсів ІС:

6.1. Загрози, що використовують стандартний доступ. Приклад такої загрози – несанкціоноване отримання пароля шляхом підкупу, шантажу, необережного зберігання, або фізичного насильства щодо законного власника.

6.2. Загрози, що використовують нестандартний шлях доступу. Приклад такої – використання незадекларованих можливостей засобів захисту.

Класифікацію загроз можна продовжувати, проте на практиці частіше за все використовується класифікація загроз, яка ґрунтується на трьох згаданих раніше базових властивостях інформації (рис. 3), що захищається.

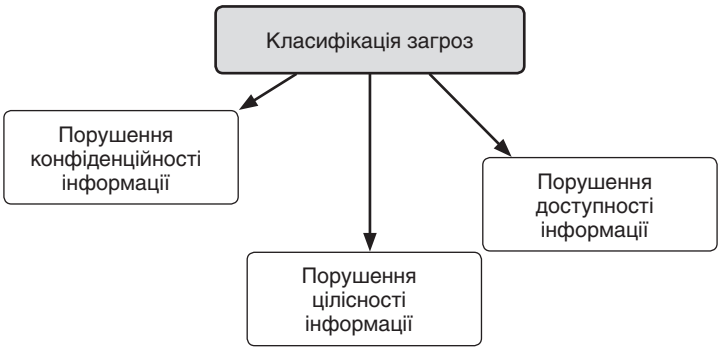


Рис. 3. Класифікація загроз, що ґрунтується на базових властивостях інформації

Властивість 1. Загрози порушення конфіденційності інформації, у результаті реалізації яких інформація стає доступною суб'єкту, що не володіє повноваженнями для ознайомлення з нею.

Властивість 2. Загрози порушення цілісності інформації, до яких відноситься будь-яке зловмисне спотворення інформації, яка обробляється з використанням ІС.

Властивість 3. Загрози порушення доступності інформації, що виникають у тих випадках, коли доступ до деякого ресурсу ІС для легальних користувачів блокується. Відзначимо, що реальні загрози інформаційній безпеці далеко не завжди можна однозначно віднести до якоїсь з перерахованих категорій. Так, наприклад, загроза розкрадання носіїв інформації може бути за певних умов віднесена до *всіх трьох категорій*.

Необхідно зазначити, що проблеми глобальної *інформаційної безпеки* посідають особливе місце в міжнародній інформаційній політиці та відображаються у звітах авторитетних організацій (ООН, ОБСЄ, ЄС та інші). Відома Європейська агенція з питань мережевої та інформаційної безпеки (European Network and Information Security Agency – ENISA) була створена на початку 2004 року з метою вирішення проблем, що пов'язані з вирішенням важливих питань у галузі інформаційної безпеки. Основні функції агенції – підвищення здатності європейських електронних мереж щодо протистояння зовнішнім впливам та атакам, збір та аналіз даних щодо комп'ютерних порушень в Європі та розробка методів оцінки й управління ризиками підвищення здатності ЄС реагувати на загрози в галузі інформаційної

безпеки. Стандарти інформаційної безпеки («Європейські критерії»), що розроблені у країнах Європи (Франція, Німеччина, Нідерланди та Великобританія) розглядають такі завдання інформаційної безпеки[10]:

- захист інформації від несанкціонованого доступу з метою забезпечення конфіденційності;
- забезпечення цілісності інформації за допомогою захисту її від несанкціонованої модифікації або знищення;
- забезпечення працездатності систем за допомогою протидії загрозам відмови в обслуговуванні.

Для вирішення проблеми попередження загроз щодо ІС введене поняття гарантій засобів захисту. Такі гарантії охоплюють два аспекти:

- ефективність, що відображає відповідність засобів безпеки задачам, які вирішуються;
- коректність, що характеризує процес їх розроблення та функціонування.

У «Європейських критеріях» нараховується сім рівнів гарантій: від Е0 до Е6 (у порядку зменшення ймовірності виникнення загрози). Рівень Е0 означає мінімальні гарантії (аналог рівня D «Жовтогарячої книги»). При перевірці гарантій аналізується життєвий цикл інформаційної системи – від початкової фази проектування інформаційної системи до експлуатації та супроводження.

Рівні гарантій від Е1 до Е6 складені з наростанням вимог щодо ретельності та контролю. Так, на рівні Е1 аналізується тільки загальна архітектура інформаційної системи, а гарантії засобів захисту підтверджується функціональним тестуванням. На рівні Е3 до аналізу залучаються вихідні тексти програм і схеми апаратного забезпечення. На рівні Е6 потрібен формальний опис функцій безпеки, загальної архітектури, а також політики безпеки, що забезпечують мінімальні ризики від загроз.

Таким чином, у «Європейських критеріях» визначені три рівні інформаційної безпеки – базовий, середній і високий. Інформаційна безпека вважається базовою, якщо засоби захисту здатні протистояти окремим випадковим атакам. Інформаційна безпека вважається середньою, якщо засоби захисту здатні протистояти зловмисникам, що мають обмежені ресурси та можливості. Інформаційну безпеку можна вважати високою, якщо є впевненість, що засоби захисту можуть бути подолані тільки зловмисниками з високою кваліфікацією, набір можливостей і ресурсів яких досить високі.

2.3. Канали витоку інформації

Необхідність *захисту інформації* від внутрішніх загроз історично була більш важливою на всіх етапах розвитку засобів *інформаційної безпеки*. З часом, на внутрішні загрози, до яких відноситься *витік інформації*, стали звертати більше уваги.

В основі *витоку інформації* полягає процес перенесення або передачі енергії чи речовини, які служать лише носіями інформації.

За фізичною природою можливі такі шляхи перенесення інформації: світлові промені; звукові хвилі; електромагнітні хвилі; матеріали і речовини.

Будь-який переданий сигнал переноситься або енергією, або речовиною. Це – або акустична хвиля (звук), або електромагнітні випромінювання (світло, радіохвиля), або лист паперу (чи інший носій написаного тексту).

Використовуючи ті або інші фізичні поля, людина створює визначену систему передачі інформації, що передається один одному. Такі системи прийнято називати *системами зв'язку*. Будь-яка система зв'язку складається з джерела інформації, передавача, каналу передачі інформації та приймача (одержувача інформації). Ці системи широко використовуються відповідно до їх призначення і являють собою засоби передачі інформації.

Процес передачі інформації загалом відбувається таким чином (рис. 4). Джерело інформації являє собою суб'єкта, яким створено певне повідомлення, звукові коливання, текст тощо. У джерелі сигналу (або перетворювачі) ці повідомлення перетворяться в сигнали: електричні, звукові, світлові тощо. Такі сигнали мають форму, що підходить для їх передачі каналами зв'язку. Канал зв'язку переносить сигнали з одного місця в інше до одержувача інформації.

Витік інформації у розрізі розглянутого процесу передачі інформації розглядається як неправомірний вихід відомостей за межі системи передачі інформації. Витік інформації також може здійснюватись за допомогою певного кола осіб, котрим деякі відомості були довірені.

За своєю сутністю *витік інформації* означає протиправне (усвідомлене або випадкове, таємне або явне) оволодіння інформацією, що не має бути поширена, незалежно від того, яким шляхом її отримано.

Несанкціоноване зняття інформації з технічних каналів являє собою поширене явище. Такі *канали витоку* являють собою сукупність: небезпечних фізичних сигналів; середовищ розповсюдження та зберігання фізичних сигналів; об'єктів технічної розвідки; різні способи та засоби технічної розвідки. За результатами аналізу наукових робіт існує узагальнена схема можливих каналів витоку і несанкціонованого доступу до інформації, що обробляється в типовому одноповерховому офісі[11].

Класифікація *каналів витоку інформації* також поділяється на:

- акустичні канали витоку інформації, куди входять також канали з акустично-електричними перетвореннями;
- радіотехнічні канали витоку інформації, до яких відносяться відкриті канали радіотехнічного зв'язку та канали, що утворюються шляхом паразитних випромінювань та наведення;
- оптичні канали витоку інформації;
- речові канали витоку інформації, який визначається людським фактором.

Таким чином, правильне визначення каналів витоку інформації та загроз безпеці в системах е-урядування дає можливість побудувати ефективні методи протидії цим загрозам, які будуть розглянуті в наступному розділі.

Висновки

1. Під час побудови сучасних систем з електронного урядування необхідно враховувати досвід різних країн світу з впровадження подібних систем в галузі основних принципів, підходів та методів створення корпоративних інформаційних структур.

До основних причин, що призводять до виникнення проблем безпечного функціонування систем електронного урядування, можуть бути віднесені: складність і різнорідність програмного та апаратного забезпечення, що використовується в системах електронного урядування; велика кількість вузлів у системах електронного урядування; наявність зовнішнього доступу до системи електронного урядування; функціонування груп технічного обслуговування та інформаційної безпеки.

2. До загроз інформаційній безпеці відносять сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам суспільства, держави та особистості. Загроза інформаційній безпеці системи розглядається як можливість реалізації впливу на інформацію, що призводить до порушення конфіденційності, цілісності або доступності даних, а також можливість впливів на компоненти системи, які можуть призводити до втрати або знищення інформації чи збою функціонування інформаційної системи.

3. Класифікація загроз інформаційній безпеці може бути здійснена за багатьма ознакам, що дозволяє добирати та застосовувати ефективні методи та засоби захисту інформації в системах е-урядування.

4. Використання стандартів інформаційної безпеки «Європейські критерії», що розроблені у провідних країнах Європи (Франція, Німеччина, Нідерланди та Великобританія), передбачає реалізацію таких основних завдань: захист інформації від несанкціонованого доступу з метою забезпечення конфіденційності; забезпечення цілісності інформації за допомогою захисту її від несанкціонованої модифікації або знищення; забезпечення працездатності систем за допомогою протидії загрозам відмови в обслуговуванні.

5. Витік інформації означає протиправне (усвідомлене або випадкове, таємне або явне) оволодіння інформацією, що не має бути поширена, незалежно від того, яким шляхом її отримано. Правильне визначення каналів витоку інформації та загроз безпеці в системах е-урядування дає можливість побудувати ефективні методи протидії цим загрозам.

Запитання для самоконтролю

1. Які є проблеми безпечного функціонування систем електронного урядування? Надайте характеристику кожної з проблем.
2. Що розуміється під загрозою інформаційній безпеці?
3. Які є загрози інформаційній безпеці? Як можна ці загрози класифікувати? Надайте приклади таких загроз.
4. З якою метою була створена Європейська агенція з питань мережевої та інформаційної безпеки?
5. Які завдання в галузі інформаційної безпеки передбачені у «Європейських критеріях»?

6. Скільки рівнів інформаційної безпеки передбачено у «Європейських критеріях»? Надайте характеристику кожного з них.
7. У чому полягає процес витоку інформації? Надайте приклади несанкціонованого витоку інформації з інформаційних систем органів публічного управління.
8. Які є канали витоку інформації за відомою класифікацією? Наведіть приклади каналів витоку інформації з практики органів публічного управління.

Рекомендована література

1. Остапов С.Е. Технології захисту інформації: навч. посіб. / С.Е. Остапов, С.П. Євсеєв, О.Г. Король. – Х.: ХНЕУ, 2013. – 476 с.
2. Кобозева А.А. Аналіз захищеності інформаційних систем: підручник / А.А. Кобозева, І.О. Мачалін, В.О. Хорошко. – К.: ДУІКТ, 2010. – 316 с.
3. Андрєєв В.І. Основи інформаційної безпеки: підручник / В.І. Андрєєв, В.О. Хорошко, В.С. Чередніченко [та ін.] – К.: ДУІКТ, 2009. – 292 с.
4. Ляшенко І.О. Європейські критерії безпеки інформаційних технологій / І.О. Ляшенко // Сучасні інформаційні технології у сфері безпеки та оборони. – 2012. – № 1 (13). – С. 84–86.

3. ВИЗНАЧЕННЯ РІВНІВ ПРОТИДІЇ ЗАГРОЗАМ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ В СИСТЕМАХ ЕЛЕКТРОННОГО УРЯДУВАННЯ

3.1. Законодавчий рівень забезпечення протидії загрозам інформаційній безпеці

Законодавчий рівень протидії загрозам є найважливішим для забезпечення інформаційної безпеки. Розробка та прийняття законодавчих актів покликані створити умови для безпечного використання інформаційно-комунікаційних технологій, доступу до інформації, захисту інформації від несанкціонованого доступу та витоку технічними каналами. Також на законодавчому рівні має бути вирішено питання захисту громадян, суспільства і держави від неправдивої інформації, реалізації технічних та інших складових інформаційної безпеки.

Нормативно-правове поле у сфері протидії загрозам інформаційної безпеки складають міжнародні, національні, галузеві нормативні документи та відповідні нормативні документи окремих органів публічного управління.

Актуальний список нормативних документів важливих законодавчих актів, нормативно-правових актів (НПА) та нормативних актів щодо інформаційної безпеки в Україні з актуальними змінами можна знайти на сайті Державної служби спеціального зв'язку та захисту інформації України[12] у розділі нормативно-правової бази.

Безпекова складова стосується чи не кожного з основних напрямів державної інформаційної політики України, що визначені Законом України «Про інформацію»[13]:

- забезпечення доступу кожного до інформації;
- забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації;

- створення умов для формування в Україні інформаційного суспільства;
- забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень;
- створення інформаційних систем і мереж інформації, розвиток електронного урядування;
- постійне оновлення, збагачення та зберігання національних інформаційних ресурсів;
- забезпечення інформаційної безпеки України;
- сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору.

Найбільш практичним з точки зору використання технології інформаційної безпеки в системах е-урядування є Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»[14], який регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. У цьому законі визначено об'єкти захисту в системі та суб'єкти відносин, порядок доступу до інформації в системі, відносини між володільцем інформації, власником інформаційно-телекомунікаційної системи та користувачами, умови обробки та забезпечення захисту інформації в системі, повноваження державних органів та відповідальність за порушення законодавства, міжнародні договори та прикінцеві положення.

Ще один важливий Закон України «Про телекомунікації»[15] розкриває сутність правової основи діяльності у сфері телекомунікацій та визначає:

- повноваження держави щодо управління та регулювання зазначеної діяльності;
- права, обов'язки та засади відповідальності фізичних і юридичних осіб, які беруть участь у даній діяльності;
- права, обов'язки та засади відповідальності фізичних і юридичних осіб, які користуються телекомунікаційними послугами.

Основною метою Закону України «Про телекомунікації» є забезпечення повсюдного надання телекомунікаційних послуг достатніх асортименту, обсягу та якості шляхом обмеженого регулювання ринкових відносин для сприяння ефективному функціонуванню відкри-

того і справедливого конкурентного ринку. Цей Закон визначає засади захисту прав споживачів та контролю за ринком телекомунікацій з боку держави.

Закон України «Про Національну програму інформатизації»[16] визначає загальні засади формування, виконання та коригування Національної програми інформатизації, що також має включати безпекові аспекти.

Завданням законодавства про Національну програму інформатизації є створення правових, організаційних, науково-технічних, економічних, фінансових, методичних та гуманітарних засад регулювання процесу формування та виконання цієї Програми та окремих її завдань (проектів).

Національна програма інформатизації визначає стратегію розв'язання проблеми забезпечення інформаційних потреб та інформаційної підтримки соціально-економічної, екологічної, науково-технічної, оборонної, національно-культурної та іншої діяльності у сферах загальнодержавного значення.

Національна програма інформатизації включає:

- Концепцію Національної програми інформатизації;
- сукупність державних програм з інформатизації;
- галузеві програми та проекти інформатизації;
- регіональні програми та проекти інформатизації;
- програми та проекти інформатизації органів місцевого самоврядування.

Національна програма інформатизації формується, виходячи з довгострокових пріоритетів соціально-економічного, науково-технічного, національно-культурного розвитку країни з урахуванням світових напрямів розвитку та досягнень у сфері інформатизації і спрямована на розв'язання найважливіших загальносуспільних проблем (забезпечення розвитку освіти, науки, культури, охорони довкілля та здоров'я людини, державного управління, національної безпеки та оборони держави та демократизації суспільства) та створення умов для інтеграції України у світовий інформаційний простір відповідно до сучасних тенденцій інформаційної геополітики.

Проблема забезпечення *інформаційної безпеки Європейського Союзу* (ЄС) особливо тісно розглядається поряд з іншими проблемами становлення інформаційного суспільства протягом останніх двадцяти

років. Проблеми забезпечення інформаційної безпеки, кібербезпеки та захисту інформації у ЄС відображені у відповідних нормативно-правових документах. Наприклад, існує Серія документів ISACA про впровадження *європейської кібербезпеки*[17], де подається загальний огляд впровадження передового досвіду в галузі кібербезпеки згідно з діючими законами, стандартами та іншими настановами. У цих документах зазначено, що виходячи з європейського досвіду, кібербезпека вимагає, щоб у всіх державах-членах та асоційованих країнах застосовувалися загальноприйняті визначення та основні положення.

Окрім того, в Серіях документів ISACA про впровадження *європейської кібербезпеки* визначено, що кібербезпека – це не тільки захист організації та її інформаційних ресурсів. У багатьох випадках реструктуризація певних частин чи всього *корпоративного середовища інформаційних технологій* у певній організації призводить до посилення кібербезпеки.

У багатьох країнах, що користуються європейськими стандартами на *корпоративне управління кібербезпекою* існують різні вимоги, наприклад:

- захист і конфіденційність інформації;
- фінансовий контроль та пов'язана з ними система внутрішнього управління, включаючи фінансову звітність;
- державні та місцеві постанови про секретну інформацію (наприклад, про службові таємниці);
- збереження та обробку інформації третіми сторонами тощо.

Організації Євросоюзу, які здійснюють *корпоративне управління кібербезпекою* згідно з національними та міжнародними механізмами, повинні відображати підхід, який застосовується у Європі та ґрунтується на таких напрямках[18]:

- визначення та категоризація критичних інфраструктур;
- план і заходи захисту критичних інфраструктур;
- «Цифровий порядок денний» для Європи та пов'язані з ним ініціативи, включаючи закони та регуляторні акти;
- підтримка Європейського центру боротьби з кіберзлочинністю та схожих національних установ.

Також, до найбільш відомих нормативно-правових актів та планів дій у сфері становлення інформаційного суспільства, що діють на цей час, відзначають Резолюцію 64/211 ООН «Створення глобальної

культури кібербезпеки щодо захисту найважливіших інформаційних інфраструктур» від 21 грудня 2009 року[19] та Резолюцію 64/25 ООН «Досягнення в сфері інформатизації та телекомунікацій в контексті міжнародної безпеки» від 2 грудня 2009 року[20]. З тих пір ще були щорічні доповіді Генерального секретаря Генеральної Асамблеї та звіти європейських країн (Німеччина, Нідерланди, Іспанія, Англія, Франція, Швеція та інші) в контексті міжнародної безпеки[21].

У цих звітах[22] відзначено, що чинні та потенційні загрози у сфері *інформаційної безпеки* належать до найбільш серйозних проблем XXI століття. Відомі загрози походять з широкого кола джерел і виявляються у підривній діяльності, спрямованій однаковою мірою проти фізичних та юридичних осіб, національної інфраструктури та урядів різних країн. Її наслідки пов'язані зі значним ризиком для громадської безпеки, безпеки країн і стабільності. Нові вразливі місця та можливості для здійснення підривних дій виникають у результаті зростання застосування інформаційних і комунікаційних технологій.

Пізніше, у 2015 році було ухвалено європейську «Директиву з мережевої та інформаційної безпеки» (Network and Information Security Directive)[23]. Документ встановлює зобов'язання в галузі забезпечення кібербезпеки підприємств критичної інфраструктури (особливо для транспортних, енергетичних, фінансових і медичних компаній). Щодо Інтернет-компаній встановили менш суворі правила: компанії на зразок Google і Amazon зобов'язані повідомляти про інциденти в галузі інформаційної безпеки відповідно призначеним органам влади. Приховування такої інформації обумовить застосування санкцій. Як заявив у зв'язку з цим віце-президент Єврокомісії Андрус Ансіп (Andrus Ansip), закон допоможе значно зміцнити довіру користувачів до міжнародних Інтернет-сервісів.

Приклад. ***Досвід вирішення питань національної безпеки та кібербезпеки у Фінляндії та Україні: стратегічний правовий рівень.***

Відповідно до урядової програми, Фінляндія прагне стати однією з провідних країн світу за рівнем розвитку кібербезпеки[24]. Проблемою щодо розвитку Кіберстратегії, яку визначив Президент Фінляндії Саулі Нійністьо (2012 рік) є те, що в цій галузі необхідно постійно розвивати не тільки системи *захисту інформації*, а й досліджувати *способи зламу даних*. У зв'язку з цим у березні 2012 року Фінляндія брала участь у координованих діях НАТО з військових навчань серед

20 країн альянсу на випадок виникнення кібервійни[25]. Така участь у військових кібернавчаннях є актуальною, через те, що за даними Відомства зв'язку у Фінляндії щорічно фіксується близько 250 000 різних порушень кібербезпеки.

У розробленій у 2012 році **Стратегії національної безпеки та оборони Фінляндії**[26] один з основних розділів присвячений сфері *інформаційної безпеки*. У документі було зазначено, що проблема використання кіберпростору набуває все більш великого значення. Руйнування, які відбуваються в кіберпросторі, являють собою критичну загрозу національній безпеці Фінляндії. До найбільш небезпечних причин виникнення кіберзагроз є вразливості, що знаходяться в *корпоративних мережах*. Наступною важливою причиною виникнення загроз є дії хакерів, які навмисно завдають шкоди або незаконно отримують інформацію (створюють витік інформації). Існує також досить суттєва частка виникнення випадкових збоїв у комп'ютерних мережах. У зв'язку з цим постає проблема розмежування кібер-атак і випадкових збоїв з метою визначення джерел загроз.

У *Стратегії національної безпеки та оборони Фінляндії* зазначено, що існують проблеми з різних питань у сфері кібербезпеки, що викликають конфлікт і розподіл думок в рамках міжнародного співтовариства. Їх основними причинами стають інтереси економіки та безпеки, різні думки з питань прав людини і ролі держави в забезпеченні індивідуальної свободи. Ці питання вирішуються у співпраці з ЄС, НАТО, ОБСЄ і ООН, а також серед різних груп країн. Також у Стратегії відзначено, що багато держав вдосконалюють свою здатність захищатися від кібер-атак і розробляють різні форми контрзаходів до зловмисників. Тому вирішення проблем виникнення та знешкодження кібератак є життєво важливими темами щодо національної та військової безпеки Фінляндії.

Стратегія кібербезпеки Фінляндії[27] складається з таких розділів як вступ, бачення кібербезпеки, керування кібербезпекою та національний підхід, стратегічні принципи кібербезпеки, додатки (терміни та визначення).

До бачення кібербезпеки Фінляндії належать такі положення:

- Фінляндія може забезпечити захист своїх життєво важливих функцій від кіберзагроз, що виникають у різних ситуаціях;
- громадяни, органи влади та бізнес-структури можуть ефективно використовувати безпечний кіберпростір і ком-

петентності, які випливають із заходів кібербезпеки, як на національному, так і на міжнародному рівнях;

- до 2016 року Фінляндія запланувала глобальне лідерство в галузі усунення кіберзагроз і в управлінні наслідками, що викликані цими погрозами.

До основних рекомендацій, що записані в Стратегії кібербезпеки Фінляндії відносять:

- створення ефективної моделі співпраці між органами влади та іншими суб'єктами з метою розвитку національної безпеки та кіберзахисту;
- поліпшення всебічного розуміння ситуації кібербезпеки серед ключових дійових осіб в суспільстві;
- підтримка і розвиток можливостей підприємств і організацій, що грають вирішальну роль для виявлення та усунення кіберзагроз;
- надання відповідним органам необхідних заходів для запобігання, розкриття і усунення кіберзлочинності;
- визначення неодмінних умов для здійснення ефективних дій у сфері кібербезпеки в рамках національного законодавства.

Стратегія національної безпеки України[28], затверджена у 2015 році, складається з таких основних розділів як: загальні положення, цілі Стратегії національної безпеки України, актуальні загрози національній безпеці України, основні напрями державної політики національної безпеки України, прикінцеві положення.

Основними цілями *Стратегії національної безпеки України* є:

- мінімізація загроз державному суверенітету та створення умов для відновлення територіальної цілісності України у межах міжнародно-визнаного державного кордону України, гарантування мирного майбутнього України як суверенної і незалежної, демократичної, соціальної, правової держави;
- утвердження прав і свобод людини і громадянина, забезпечення нової якості економічного, соціального і гуманітарного розвитку, забезпечення інтеграції України до Європейського Союзу та формування умов для вступу в НАТО.

Серед інших проблем щодо актуальних загроз національній безпеці України, які мають бути вирішені, у Стратегії також зазначені:

- загрози інформаційній безпеці;
- загрози кібербезпеці та безпеці інформаційних ресурсів.

Зокрема, до загроз у сфері кібербезпеки та безпеки інформаційних ресурсів відноситься:

- уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак;
- фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом;

До основних пріоритетів щодо вирішення проблем забезпечення кібербезпеки та безпеки інформаційних ресурсів віднесені:

- розвиток інформаційної інфраструктури держави;
- створення системи кібербезпеки, у тому числі координації діяльності у цій сфері, розвиток мережі реагування на комп'ютерні надзвичайні події (CERT);
- моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації;
- розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів;
- забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, відмова від програмного забезпечення, зокрема антивірусного, розробленого у Російській Федерації;
- реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації з урахуванням практики держав-членів НАТО та ЄС;
- створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектора безпеки і оборони;
- розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО, зокрема в межах Трастового фонду НАТО для посилення спроможностей України у сфері кібербезпеки.

У 2016 році Рада національної безпеки і оборони України схвалила проект **Стратегії кібербезпеки України**[29], де розкрито загальні положення, загрози кібербезпеці, національну систему кібербезпеки,

пріоритети та напрями забезпечення кібербезпеки України, прикінцеві положення.

Метою Стратегії кібербезпеки України є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Особливу увагу у проекті зазначено на проблемах необхідності розвитку та безпеки кіберпростору, запровадження електронного урядування, гарантування безпеки й сталого функціонування електронних комунікацій та державних електронних інформаційних ресурсів.

До основних пріоритетів та напрямів забезпечення кібербезпеки України у Стратегії кібербезпеки України належать:

- розвиток безпечного, стабільного і надійного кіберпростору;
- кіберзахист державних електронних інформаційних ресурсів та інформаційної інфраструктури та критичної інфраструктури;
- розвиток потенціалу сектору безпеки та оборони у сфері забезпечення кібербезпеки;
- боротьба з кіберзлочинністю.

3.2. Адміністративний та процедурний рівні забезпечення протидії загрозам інформаційній безпеці

Призначення *адміністративного рівня протидії загрозам інформаційній безпеці* має зводитися до таких основних трьох практичних кроків:

1. Визначення керівних документів і стандартів, що використовуються в ІБ. Такі основні положення включають:

- управління доступом до засобів ІС, програм і даних;
- антивірусний захист програм;
- питання резервного копіювання даних;
- проведення ремонтних та відновлювальних робіт;
- інформування про інциденти щодо ІБ.

2. Визначення підходів до управління ризиками ІБ. У цьому випадку може ставитися запитання: чи є достатнім базовий рівень захищеності або ж потрібно проводити повний варіант аналізу ризиків?

3. Порядок сертифікації на відповідність стандартам ІБ. У цьому випадку необхідно визначити періодичність проведення нарад за тематикою ІБ на рівні керівництва. До нарад доцільно включати періодичний перегляд положень політики ІБ, порядок навчання наявних категорій користувачів ІС з питань ІБ та основи функціонування КСЗІ.

Для побудови КСЗІ необхідно визначити межі системи, для якої повинен бути забезпечений режим ІБ за таким планом:

1. Структура органу публічного управління (ОПУ). Опис чинної структури і змін, які передбачається внести у зв'язку з розробкою або модернізацією ІС.

2. Розміщення коштів на підтримку ІС та інфраструктури. Модель ієрархії програмних та апаратних засобів ІС.

3. Ресурси ІС, що підлягають захисту. Рекомендується розглянути основні ресурси ІС: програмно-апаратні складові техніки. Такі інформаційні ресурси являють цінність з точки зору роботи організації. Для їх оцінки повинна бути обрана система критеріїв і методологія оцінок за цими критеріями.

4. Технологія обробки інформації та оцінка потреб. Для вирішення таких завдань повинні бути побудовані моделі обробки даних ІС в термінах інформаційних ресурсів.

У результаті опису меж дії КСЗІ може бути складений документ, в якому:

- зафіксовані межі і структура ІС;
- перераховані ресурси, які підлягають захисту ІС;
- показана система оцінки цінності критеріїв.

Мінімальним вимогам режиму ІБ відповідає базовий рівень. Звичайною областю використання цього рівня є типові проектні рішення.

Основою заходів адміністративного рівня загрозам безпеки ІС, тобто заходів, що вживаються керівництвом організації, є *політика безпеки.*

Існує ряд стандартів і специфікацій, в яких розглядається мінімальний (типовий) набір найбільш ймовірних загроз, таких як віруси, збої устаткування, несанкціонований доступ тощо. Для подолання цих загроз обов'язково повинні бути прийняті контрзаходи незалежно від ймовірності здійснення загроз і вразливості ІР.

У разі, коли порушення ІБ має важкі наслідки, базовий рівень

вимог щодо цього режиму є недостатнім. Для того, щоб сформулювати додаткові вимоги, необхідно:

- визначити цінність ІР;
- додати до стандартного набору найбільш імовірних загроз список нових записів загроз, що є актуальними для ІС;
- оцінити ймовірності виникнення нових загроз;
- визначити рівень уразливості ІР.

Адміністративний рівень протидії загрозам безпеки будується на основі аналізу ризиків, які визнаються реальними для ІС ОДУ. Коли ризики проаналізовані та стратегія ЗІ є визначеною, тоді складається програма, реалізація якої повинна забезпечити ІБ. Під цю програму виділяються ІР, призначаються відповідальні особи, визначається порядок контролю виконання завдань тощо.

Оцінка ризиків реалізації загроз.

Існують різні підходи щодо оцінки ризиків. Вибір підходу залежить від рівня вимог, що висуваються в організації до режиму ІБ. У цьому випадку розглядаються загрози або спектри дій загроз та ефективність потенційних контрзаходів. Процес оцінки ризиків містить кілька етапів (рис. 5).

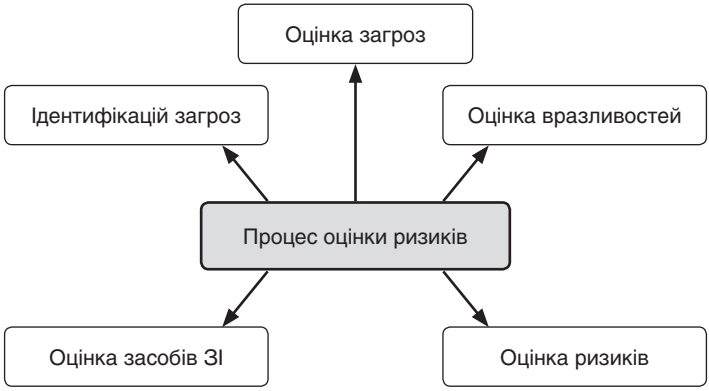


Рис. 5. Процес оцінки ризиків реалізації загроз інформаційній безпеці

Етап 1. Ідентифікація ІР та оцінка його кількісних показників (визначення негативного впливу).

Етап 2. Оцінка загроз.

Етап 3. Оцінка вразливих сфер.

Етап 4. Оцінка чинних і прогнозованих засобів ЗІ.

Етап 5. Оцінка ризиків.

На підставі оцінки ризиків обираються засоби, що забезпечують ефективний режим ІБ. ІР, що є важливими для нормальної роботи організації і мають певну ступінь уразливості, вважаються схильними до ризику, якщо стосовно них існує будь-яка загроза. Під час оцінки ризиків враховуються потенційні негативні впливи від небажаних загроз, показники значущості розглянутих вразливих сфер та загрози для конкретних ІР.

Загалом *ризик* характеризує небезпеку, якій може піддаватися ІС на рівні певної організації або у системі публічного управління. *Ризик* залежить від показників цінності ІР, ймовірності реалізації загроз і ступеня уразливості. Визначення ризику може бути використано при чинних або запланованих засобах забезпечення ІБ.

Мета оцінки ризиків полягає у визначенні їх характеристик для ІС та їх ІР. На основі таких даних можуть бути обрані необхідні засоби управління ІБ.

Під час оцінки ризиків враховується:

- цінність ІР;
- оцінка вагомих загроз;
- ефективність чинних і прогнозованих засобів ЗІ.

Потенційний негативний вплив на діяльність ОПУ можна визначати кількома способами:

- кількісними (наприклад, вартісні);
- якісними (наприклад, поняття помірний або надзвичайно небезпечний);
- їх комбінацією.

Для того, щоб конкретизувати визначення ймовірності реалізації загрози, розглядається певний відрізок часу, протягом якого передбачається захистити ресурс. Ймовірність того, що загроза з успіхом реалізується, визначається наступними факторами:

- привабливість ІР при розгляді загрози від навмисного впливу з боку людини;
- можливість використання ІР для отримання доходу під час розгляду загрози від навмисного впливу з боку людини;

- технічні можливості загрози, які використовуються під час навмисного впливу з боку людини;
- ймовірність того, що загроза реалізується;
- ступінь, з якою вразливість може бути використана.

До процедурного рівня протидії загрозам відносяться організаційні заходи ІБ, що виконуються людиною.

Можна виділити такі групи організаційних (процедурних) заходів:

- управління персоналом на рівні певної організації або в системі публічного управління;
- фізичний захист ІС;
- підтримка працездатності ІС на рівні певної організації або в системі публічного управління;
- реагування на порушення режиму безпеки на рівні певної організації або в системі публічного управління;
- планування відновлювальних робіт на організаційному рівні певної організації або в системі публічного управління.

Надійним засобом підвищення ефективності заходів *інформаційної безпеки* є навчання та інструктаж персоналу щодо організаційно-технічних заходів захисту, які застосовуються на рівні певної організації, системи публічного управління.

Таким чином, питання про те, як провести межу між допустимими і неприпустимими ризиками, вирішується фахівцями. Професійний розгляд адміністративного рівня вимагає врахування специфіки систем е-урядування для конкретних ОДУ.

На підставі розробки адміністративного рівня будується програма інформаційної безпеки, яка реалізується на процедурному і програмно-технічному рівнях.

<u>Приклад.</u> Протидія загрозам інформаційній безпеці, що можуть виникати внаслідок атаки на Wi-Fi мережу органу публічного управління.

Останнім часом в органах публічного управління практикують встановлення Wi-Fi мереж з метою забезпечення доступу до Інтернет як громадян, що відвідують ці органи влади, так і персоналу. Але при цьому слід враховувати, що найчастіше загрози, які являють собою проникнення у Wi-Fi мережу, відбуваються з метою зміни налаштувань DNS сервера у системах електронного урядування. Загалом DNS

сервер призначений для переведення назв доменних імен (наприклад, назв сайтів) до IP адрес.

Тому зловмисник може змінити публічний DNS-сервер на свій власний для налаштування на іншу IP адресу. Наприклад, у браузері користувача при введенні назви сайту google.com.ua може бути здійснений перехід на особисту IP-адресу зловмисника. Внаслідок цього буде відбуватись перехоплення веб-трафіку або виконуватись зараження персонального комп'ютера публічного службовця.

Наступне, що може здійснити зловмисник – це перехоплення особистої інформації службовця за допомогою механізму атаки «людина посередині» (men-in-the-middle). За допомогою такої атаки весь вебтрафік, який за замовчуванням відправляється до Wi-Fi роутера службовця, буде відправлено спочатку зловмиснику, а потім до роутера.

Така атака дозволяє зловмиснику викрадати особисті дані (логіни, паролі) та переглядати мережеві потоки даних.

Слід також зазначити, що зловмисник, який перебуває у Wi-Fi мережі системи електронного урядування може здійснювати інші хакерські атаки: зломи сайтів, DDOS-атаки, додавання різних пристроїв захопленої мережі до інших бот-мереж, завантажувати небезпечну інформацію (віруси, трояни тощо). Ці дії можуть виконуватись від імені зареєстрованих користувачів інформаційних систем та їх IP адрес.

Тому важливим є дотримання правил безпеки процедурного рівня в системах електронного урядування в роботі з Wi-Fi мережею, до яких належать:

- правильний підбір типу шифрування протоколу взаємодії з точкою доступу (роутером) Wi-Fi мережі;
- фільтрація пристроїв комп'ютерної мережі за MAC-адресою;
- відключення віддаленого доступ до адміністрування роутера або точки доступу з глобальної мережі Інтернет;
- стійкі паролі.

3.3. Програмно-технічний рівень протидії загрозам інформаційній безпеці та політика безпеки в системах е-урядування

Програмно-технічний рівень протидії загрозам ІБ передбачає

такі механізми безпеки: ідентифікація і аутентифікація користувачів; управління доступом; протоколювання і аудит; криптографія; екранування каналів зв'язку; забезпечення високої доступності тощо.

Важливо керувати ІС у цілому і механізмами безпеки особливо. Згадані заходи безпеки повинні спиратися на загальноприйняті стандарти, бути стійким до мережевих загроз, враховувати специфіку окремих сервісів.

Зупинимось на основних положеннях програмно-технічного рівня протидії загрозам (рис. 6).

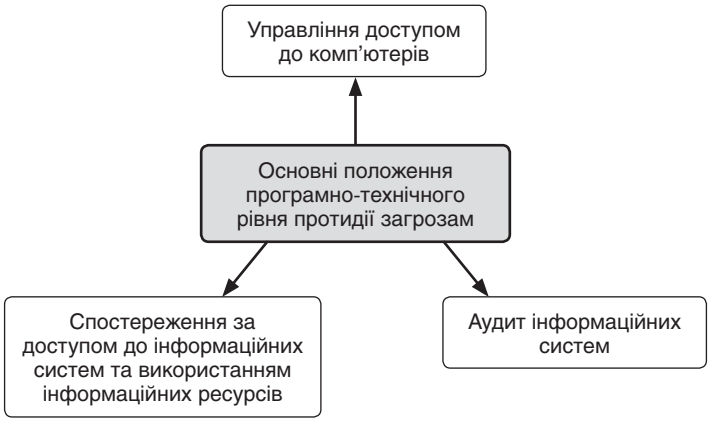


Рис. 6. Основні положення програмно-технічного рівня протидії загрозам інформаційній безпеці

Управління доступом до комп'ютерів. Доступ до ІС слід надавати тільки зареєстрованим користувачам. Комп'ютерні системи, що обслуговують багатьох користувачів, мають задовольняти такі вимоги: ідентифікувати і перевіряти відповідність особистості користувачів, а також за потребою – термінал або місцеперебування зареєстрованого користувача; фіксувати випадки успішного і безуспішного доступу до ІС; надати систему управління паролями, що забезпечує вибір надійних паролів; обмежити час підключення користувачів до ІС.

Доступ до ІС необхідно здійснювати за допомогою надійної процедури входу в систему. Процедура входу в комп'ютерну сис-

тему (login) повинна зводити ризик несанкціонованого доступу до мінімуму.

Процедура входу в систему повинна виконувати такі функції: не виводити на екран ідентифікатори системи або додатки доти, поки не завершиться процес входу в систему; виводити на екран загальне попередження про те, що тільки зареєстровані користувачі мають право доступу до комп'ютера; не надавати довідкову інформацію під час виконання процедури входу в систему; перевіряти точність реєстраційної інформації тільки після завершення введення всіх даних; при виникненні ситуації збою система не повинна вказувати, яка частина введених даних правильна чи неправильна; повинно бути обмеження кількості невдалих спроб входу в систему (рекомендується три спроби), перш ніж розірвати канал зв'язку з користувачем.

Спостереження за доступом до ІС та використанням ІР. Для забезпечення відповідності ПБ (управління доступом і стандартами) необхідно стежити за роботою ІС та використанням ІР. Це необхідно для того, щоб визначити ефективність вжитих заходів і забезпечити відповідність моделі ПБ. Усі надзвичайні ситуації і події, що пов'язані з порушенням режиму безпеки необхідно реєструвати в контрольному журналі. Записи в такому журналі варто зберігати протягом заданого проміжку часу для надання допомоги в майбутніх розслідуваннях і здійсненні контролю за доступом до ІС. Крім відкинутих спроб входу в систему, доцільно також реєструвати випадки успішного доступу до неї. Контрольний журнал повинний включати наступні дані: ідентифікатори користувачів; дата і час входу і виходу із системи; ідентифікаційний код робочої станції та за ким вона закріплена.

Необхідно також встановити процедури спостереження за використанням систем. Такі процедури вимагаються для забезпечення виконання користувачами тільки явно дозволених процесів. Рівень контролю, необхідний для окремих систем, варто визначити за допомогою незалежної оцінки ризиків. Усі дії, пов'язані зі спостереженням за системами, повинні бути формально дозволені керівництвом. Для забезпечення точності ведення контрольних журналів, що можуть знадобитися для розслідувань або як свідчення під час судових розглядів і при накладенні дисциплінарних стягнень, важливо правильно встановити системний годинник комп'ютерів. Неточні записи у контрольних журналах можуть перешкодити таким розслідуванням і підірвати довіру до такого свідчення.

Аудит ІС. Для зведення ризику виникнення збоїв у ІР до міні-

муму вимоги щодо аудиту і роботи, які пов'язані з перевіркою робочих станцій варто планувати і погодити. З цією метою пропонуються наступні рекомендації: вимоги до аудиту ІС повинні бути погоджені з відповідним керівництвом; масштаб перевірок необхідно погодити і контролювати; перевірки повинні бути обмежені доступом до даних і програм тільки на читання; інші типи доступу (відмінні від доступу тільки на читання) повинні бути дозволені для окремих копій системних даних, які необхідно стерти по завершенні процесу аудиту; необхідно явно ідентифікувати ІР для проведення перевірок і зробити їх доступними; необхідно визначити вимоги щодо спеціальної чи додаткової обробки даних і погодити їх з постачальниками послуг; усі випадки доступу необхідно відслідковувати і фіксувати в контрольному журналі для перевірок.

Ідентифікація і аутентифікація користувачів. Одним з найбільш поширених засобів ідентифікації та аутентифікації користувачів у системах електронного урядування є *електронний цифровий підпис (ЕЦП).* ЕЦП – це вид електронного підпису, що отриманий за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого (закритого, секретного) ключа та перевіряється за допомогою відкритого ключа.

ЕЦП призначений для використання фізичними або юридичними особами та використовується для:

- ідентифікації особи (підписувача);
- підтвердження цілісності даних в електронному документі (формі).

Вагомість ЕЦП полягає у наданні юридичної сили електронному документу. ЕЦП вважається інструментом забезпечення інформаційної безпеки держави. ЕЦП є ефективним засобом контролю походження та цілісності інформації на всіх рівнях інфраструктури суспільства: від персональної інформаційної безпеки людини до інформаційної безпеки держави.

Механізм формування ЕЦП полягає у тому, що відбувається накладання особистого ключа та перевірка результату дії за допомогою відкритого ключа. За правовим статусом така дія прирівнюється до власноручного підпису (печатки). Електронний підпис не може бути визнаний недійсним лише через те, що він має електронну

форму або не ґрунтується на посиленому сертифікаті ключа. За умови правильного зберігання власником особистого (закритого, секретного) ключа його підробка вважається неможливою. Електронний документ також не можливо підробити: будь-які зміни, не санкціоновано внесені в текст документу, будуть під час перевірки миттєво виявлені.

Особистий ключ ЕЦП формується на підставі генератора випадкових чисел. Друга частина ЕЦП – відкритий ключ обчислюється з особистого ключа таким чином, щоб одержати закритий ключ з відкритого було неможливо. Документ підписується ЕЦП тільки за допомогою особистого ключа, який існує у його власника.

Таким чином, *особистий ключ ЕЦП* є унікальною послідовністю символів довжиною 264 біта, що отримана випадковим чином та генерація якої з відкритого ключа є неможливою. Працює особистий ключ тільки в парі з відкритим ключем. Особистий ключ необхідно зберігати в таємниці, тому що будь-хто зможе підробити ЕЦП.

Також, є поняття *Сертифіката* (в якому міститься відкритий ключ), що підтверджує приналежність відкритого ключа певній особі. Крім самого відкритого ключа, Сертифікат містить в собі персональну інформацію про його власника (ім'я, реквізити), унікальний реєстраційний номер та термін дії Сертифіката. З метою забезпечення цілісності представлених у Сертифікаті даних він ще підписується особистим ключем Центру сертифікації ключів (ЦСК). *Сертифікат відкритого ключа* може публікуватися на сайті відповідного центру (ЦСК) відповідно до Договору про надання послуг ЕЦП.

В Україні існує Національна система електронного цифрового підпису, яка складається з:

- центрального засвідчувального органу;
- акредитованих центрів сертифікації ключів;
- центрів сертифікації ключів;
- контролюючого органу.

Послуги з надання ЕЦП в Україні впроваджуються акредитованими центрами сертифікації ключів.

Акредитованим центром сертифікації ключів є центр, де проходять сертифікацію ключі в установленому державою порядку. Акредитацію таких сертифікаційних центрів в Україні здійснює *Центральний засвідчувальний орган*. Актуальний (поточний) перелік

усіх акредитованих центрів сертифікації ключів публікується на сайті Центрального засвідчувального органу[30].

Відмінністю акредитованого центру від центрів сертифікації ключів є те, що він має право обслуговувати виключно посилені сертифікати ключів.

Акредитований центр сертифікації ключів (АЦСК) має виконувати усі зобов'язання та вимоги, встановлені законодавством для центру сертифікації ключів, та додатково зобов'язаний використовувати для надання послуг електронного цифрового підпису надійні засоби електронного цифрового підпису. АЦСК має право:

- надавати послуги електронного цифрового підпису та обслуговувати виключно посилені сертифікати ключів (згідно статті 9 Закону України «Про електронний цифровий підпис»);
- отримувати та перевіряти інформацію, що необхідна для реєстрації підписувача і формування посиленого сертифіката ключа, безпосередньо у юридичної або фізичної особи чи її представника.

Порядок акредитації та вимоги, яким повинен відповідати акредитований центр сертифікації ключів, встановлюються Кабінетом Міністрів України.

Центр сертифікації – це компонент глобальної служби каталогів, що відповідає за управління криптографічними ключами користувачів. Центр сертифікації ключів має право:

- надавати послуги за посвідченням сертифікатів електронного цифрового підпису (згідно статті 8 Закону України «Про електронний цифровий підпис»[31]);
- обслуговувати сертифікати відкритих ключів;
- отримувати та перевіряти інформацію, необхідну для створення відповідності інформації зазначеної у сертифікаті ключа і пред'явленими документами.

Перелік міжнародних та європейських стандартів, інших актів технічного регулювання для гармонізації з метою реформування, розвитку та забезпечення інтероперабельності системи електронного цифрового підпису визначений наказом Міністерства юстиції України та Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 05.12.2013 р. № 2563/5/645 (у редакції наказу від 25.12.2014 р. № 2170/5/703)[32].

Основні нормативні акти, що регламентують використання в України ЕЦП, зокрема, Закон України «Про електронний цифровий підпис» та Закон України «Про електронні документи та електронний документообіг»[33] були прийняті ще у 2003 році, однак поширене застосування даної технології спостерігається переважно у сфері податкової звітності та у банківській діяльності. Це відбувається внаслідок складності адміністративних процедур, дотримання яких вимагається для створення та розвитку суб'єктів інфраструктури, яка необхідна для поширення сфери використання ЕЦП. За статтею 3 Закону України «Про електронний цифровий підпис», «Електронний цифровий підпис за правовим статусом прирівнюється до власноручного підпису (печатки) у разі, якщо:

- електронний цифровий підпис підтверджено з використанням посиленого сертифіката ключа за допомогою надійних засобів цифрового підпису;
- під час перевірки використовувався посилений сертифікат ключа, чинний на момент накладення електронного цифрового підпису;
- особистий ключ підписувача відповідає відкритому ключу, зазначеному у сертифікаті».

Таким чином, ЕЦП ефективно використовується як спосіб ідентифікації підписувача електронного документа та дозволяє однозначно визначати походження цифрових даних (джерело інформації), що містяться у файлах користувачів.

<u>Приклад.</u> Порівняння підходів щодо діяльності центрів сертифікації ключів електронного цифрового підпису в Україні та країнах Європейського Союзу.

В Європейському Союзі питання вимог щодо учасників ринку у наданні послуг в галузі електронного цифрового підпису регламентується Директивою ЄС «Про порядок використання електронних підписів в Європейському Співтоваристві» 1999/93/ЕС[34], де встановлені вимоги щодо технічного та криптографічного захисту інформації щодо осіб, які забезпечують обіг посилених сертифікатів ключів.

Слід також зазначити, що вимоги українського законодавства щодо створення та діяльності центрів сертифікації ключів є занадто надмірними у порівнянні з ЄС. Чинна в Україні нормативно-правова база суттєво стримує розвиток відповідних суспільних відносин у цій галузі[35]. Вирішенням цього питання може бути узгодження національ-

ного законодавства України із Директивою ЄС «Про порядок використання електронних підписів в Європейському Співтоваристві» 1999/93/ЕС з метою суттєвого спрощення відповідних адміністративних процедур (наприклад, питання визнання сертифікатів ключів електронного цифрового підпису, виданих в інших країнах).

Важливою частиною побудови *процедурного та програмно-технічного рівнів* протидії загрозам інформаційної безпеки є розробка *політики безпеки*.

Політика безпеки (ПБ) – це сукупність принципів, правил, процедур і практичних рішень у галузі інформаційної безпеки, які регулюють керування, захист та розподіл інформації, що захищається. *ПБ* визначає загальну стратегію організації в області інформаційної безпеки, а також ту міру уваги і кількість ресурсів, яку керівництво організації вважає за доцільне виділити для забезпечення ЗІ.

ПБ залежить від багатьох чинників, а саме від: рівня секретності та властивостей інформації, яка підлягає захисту; конкретної технології обробки інформації; технічних та програмних засобів, що використовуються організацією; інших чинників, які уточнюються на етапі розробки ПБ.

ПБ щодо системи е-урядування має враховувати сучасний стан та найближчі перспективи розвитку інформаційних технологій, мету, завдання, правові основи експлуатації ІС, режими функціонування об'єктів, містити аналіз загроз безпеки та способи їх реалізації. Основні положення таких документів повинні розповсюджуватися на структурні підрозділи ОПУ, а також на інші організації, які взаємодіють як постачальники або споживачі ІР.

Нормативно-правовою основою ПБ служать Конституція України, Цивільний та Кримінальний кодекси, закони, укази, постанови, акти Держспецзв'язку.

ПБ є методологічною основою для формування та впровадження єдиної політики в галузі захисту інформації в ОДУ; прийняття важливих рішень та розробки спільних практичних заходів, спрямованих на виявлення, знешкодження та ліквідацію наслідків реалізації різних типів загроз БІ; координацію діяльності структурних підрозділів організації під час виконання робіт зі створення, розвитку та експлуатації ІР з дотриманням вимог щодо забезпечення ІБ; розробки пропозицій щодо вдосконалення правового, нормативного, технічного та організаційного забезпечення ІБ в ОПУ.

Таким чином, конкретні заходи програмно-технічного рівня протидії загрозам інформаційної безпеки мають бути визначені в ОПУ окремими завданнями.

<u>Приклад.</u> Інформаційні ресурси підтримки програмно-технічного рівня протидії загрозам інформаційної безпеки в системах електронного урядування: досвід Фінляндії та України.

Інформаційні ресурси Фінляндії. Інформаційні ресурси, що знаходяться в *Національному центрі з кібербезпеки Фінляндії*[36] є найбільш відомі в країні в галузі захисту інформації та розкривають питання інформаційної безпеки, особливості уразливих ділянок автоматизованих систем, рекомендації щодо забезпечення інформаційної безпеки різних організацій, права і обов'язки операторів телекомунікаційних вузлів. Серед важливих розділів сайту: попередження, відомі уразливості, безпечне використання послуг в галузі електронних комунікацій, безпечне використання пристроїв (ADSL-модемів, WLAN-пристроїв, міжмережевих екранів), електронні ідентифікаційні (цифрові підписи та сертифікати), інформація про інспекцію органів безпеки, права та обов'язки операторів зв'язку, права та обов'язки корпоративних абонентів зв'язку, статистика та звіти.

Ще один важливий інформаційний ресурс: *Національний акредитаційний орган Фінляндії* (FINAS)[37] є національним органом з акредитації в Фінляндії. FINAS акредитує лабораторії, органи з сертифікації, інспектуючих державних органів, фахівців є професійного тестування і перевірки параметрів навколишнього середовища та викидів парникових газів. Серед важливих розділів сайту є новини, цікаві статті, відомі курси, різні послуги, інформація про акредитації тощо.

Міністерство фінансів Фінляндії також приділяє велику увагу питанням кіберзахисту наявних інформаційних ресурсів держави. У матеріалах, розміщених на сайті Міністерства фінансів Фінляндії[38] зазначено, що існують загальні відправні точки, які включають в себе відповідальність кожної організації в галузі інформаційної безпеки під час здійснення своїх власних операцій, зобов'язання з інформаційної безпеки, передбачені нормативно-правовими актами, Постановами Уряду про підвищення інформаційної безпеки Фінляндії, Стратегією кібербезпеки Фінляндії, а також інструкціями з інформаційної безпеки, виданими Міністерством Фінансів Фінляндії.

У лютому 2016 року з'явився документ з *електронного урядування в Фінляндії* (редакція 18)[39], де було зазначено, що основним

напрямом програми реалізації кібербезпеки на державному рівні країни є подальший розвиток:

- Центру з кібербезпеки;
- центрального урядового оперативного органу з інформаційної безпеки з режимом роботи 24/7;
- мережі безпеки для управління та обміном зашифрованими даними.

Таким чином, актуальним у цій країні буде залишатися розв'язання таких важливих питань як: надання поліції певних можливостей реагування на кіберзлочини; створення ефективної моделі співпраці між органами влади та іншими суб'єктами держави з метою впровадження механізмів національної кібербезпеки; зміцнення національної кібербезпеки шляхом активної участі в діяльності міжнародних організацій і спільних форумів в галузі інформаційної безпеки; закріплення передумов для здійснення ефективних заходів в області кібербезпеки в рамках національного законодавства; розробка стандартів управління інформаційною безпекою; проведення наукових досліджень та освітніх програм, що направлені на поліпшення знань та обізнаності в галузі кіберзлочинності.

Інформаційні ресурси України. Інформаційні ресурси *Державної служби спеціального зв'язку та захисту інформації України*[40] складаються з новин та тематичних розділів. Звертає на себе увагу розділ зі стандартизації, оцінки відповідності (сертифікація) та метрології, де вказані важливі законодавчі та нормативні акти, укази, постанови. Серед важливих документів на сайті знаходиться інформація про: захист державних інформаційних ресурсів в інформаційно-телекомунікаційних мережах, криптографічний захист інформації, технічний захист інформації, національну систему конфіденційного зв'язку тощо.

Інформаційні ресурси *Міжвідомчої комісії з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України*[41] представлені новинами, планами заходів, послугами, форумом.

Звертає на себе увагу *інформаційний ресурс CERT-UA*[42], де змістовно розповідається про мету та основні функціональні напрями діяльності CERT-UA, види кіберзагроз та правова основа діяльності CERT-UA. До важливих сервісів цього сайту відносяться: перевірка вразливості в OpenSSL, система накопичення і обробки інформації про скомпрометовані IP-адреси IP Guard та розподілена система активного моніторингу мережевих загроз IP Guard AMS 1.0. Також на

сайті є можливість повідомлення про інцидент за допомогою інтерактивної форми. Розміщено й рекомендації щодо роботи різних сервісів мережі Інтернет, описи шкідливого програмного забезпечення, відомі вразливості різних протоколів тощо.

3.4. Рівні системи електронного урядування з точки зору протидії загрозам інформаційній безпеці

Завдання із захисту інформаційних ресурсів ускладнюється тим, що системи електронного урядування використовують як публічні службовці, так і різні категорії населення, які здійснюють такі дії:

- операції, пов'язані з функціональними обов'язками публічних службовців і комунікацією з громадянами та бізнесом;
- збереження та обробка даних (документів, програмного забезпечення, баз даних і т.п.);
- виконання доступу до зовнішніх інформаційних ресурсів;
- виконання доступу до внутрішніх інформаційних ресурсів за запитами із зовнішніх небезпечних ділянок мережі Інтернет.

З точки зору *інформаційної безпеки* існують певні програмно-технічні архітектури, що охоплюють чотири рівні протидії загрозам інформаційній безпеці (рис. 7).

Рівень прикладного програмного забезпечення
Рівень системи управління базами даних
Рівень операційної системи
Транспортний рівень корпоративної мережі

Рис. 7. Рівні системи електронного урядування з точки зору протидії загрозам інформаційної безпеки

Рівень прикладного програмного забезпечення, яке використовують публічні службовці або користувачі – споживачі сервісів електронного урядування. Прикладом елементів систем електронного урядування, що працюють на цьому рівні, є офісні програми: текстовий редактор Word, редактор електронних таблиць Excel, поштова програма Outlook, стандартні програми обміну повідомленнями (icq, skype), браузери, антивірусні програми тощо.

Рівень системи управління базами даних, що відповідає за

зберігання і обробку даних системи електронного урядування. До елементів цього рівня можна віднести як потужні системи, що використовуються в системах електронного документообігу: MS SQL, MySQL, PostgreSQL, так і більш прості: MS Access.

Рівень операційної системи, що відповідає за обслуговування системи електронного урядування, інформаційних систем, баз даних і прикладного програмного забезпечення. До елементів, що працюють на цьому рівні, можна віднести мережеві серверні та клієнтські операційні системи Linux, FreeBSD, Sun Solaris, Microsoft Windows та інші.

Транспортний рівень корпоративної мережі, що відповідає за взаємодію окремих вузлів системи електронного урядування. До елементів, що працюють на цьому рівні, відносять стеки протоколів TCP/IP, IPS/SPX, SMB/NetBIOS, VPN та інші.

Такий поділ з точки зору протидії загрозам інформаційної безпеки (рис. 9) системи електронного уряду зручний для дослідження можливих атак та розробки захисних дій. Робота системи електронного уряду передбачає використання захисних механізмів до яких відносяться міжмережеві екрани та проксі-сервери, що забезпечують захист від більшості атак. Однак, у зловмисників в певних випадках залишається можливість у проведенні комп'ютерних атак, що можуть відноситись до вказаних рівнів (рис. 9).

Рівень прикладного програмного забезпечення. Проникнення до інформаційних ресурсів системи електронного уряду зі стандартних (Web, FTP) та прикладних (платіжні) електронних сервісів, інформаційних систем з обробки інформації. *Прикладами комп'ютерних атак* на прикладне програмне забезпечення є завантаження небезпечного змісту («троянський кінь», мобільний код Java та ActiveX, віруси) та несанкціонований доступ до пароля (вбудовування спеціальних програм-кейлогерів, підбір пароля).

Рівень системи управління базами даних. Проникнення до інформаційних ресурсів системи електронного уряду за допомогою SQL-запитів з Web ресурсів до баз даних. *Прикладом комп'ютерної атаки* на системи управління базами даних є використання SQL-ін'єкцій під час роботи з Web-інтерфейсом інформаційної системи.

Рівень операційної системи. Проникнення до інформаційних ресурсів системи електронного уряду з вищевказаних рівнів та крадіж паролів, важливих файлів (баз даних, документів). *Прикладами комп'ютерних атак* на операційну систему є несанкціоноване виконання команд у результаті вразливостей у прикладних програмах

або базах даних і порушення прав доступу внаслідок неправильної роботи міжмережевих екранів.

Транспортний рівень корпоративної мережі. Проникнення до інформаційних ресурсів системи електронного уряду для виконання моніторингу та перегляду вмісту мережевого трафіку. *Прикладами комп'ютерних атак* на корпоративну мережу є Dos або DDos («відмова в обслуговуванні», атака що ускладнює роботу з прикладними сервісами) та несанкціонований перегляд мережевого трафіку на предмет паролів або відомих вразливостей прикладних програмних засобів та баз даних.

<u>Приклад.</u> Досвід програмно-технічної підтримки інформаційних систем протидії кібератакам у Фінляндії.

У Фінляндії існує практика централізованого програмно-технічного обслуговування та підтримки інформаційної безпеки обчислювальних систем, що знаходяться у державних установах. З метою надання якісних послуг державним організаціям в галузі ІКТ у Фінляндії створено сервісний центр Valtori[43], що діє в рамках адміністративної компетенції Міністерства фінансів. Основною метою створення центру Valtori є представлення незалежних ефективній послуг у сфері ІКТ у співпраці з клієнтами в галузі підтримки діяльності органів державного управління. Valtori була створена шляхом об'єднання персоналу чинних урядових центрів з незалежними агентствами з послуг ІКТ. Поряд з іншими установами та організаціями Фінляндії Valtori надає послуги, які: виконуються в галузі захисту інформації та інформаційної безпеки; мають високу якість підтримки та високі технічні вимоги; є конкурентоспроможними стосовно інших суб'єктів ринку країни; враховують екологічно обґрунтовані вимоги клієнтів.

Також, необхідно зазначити, що й у Фінляндії, і в Україні існує певний досвід підтримки інформаційних систем протидії кібератакам, що охоплює:

- інформування широкого кола заінтересованих суб'єктів про знайдені найбільш поширені уразливості інформаційних систем;
- інформування широкого кола осіб про використання антивірусних та інших засобів протидії загрозам інформаційній безпеці;

- створення організаційних структур швидкого реагування на інциденти, що зустрічаються під час несанкціонованого втручання в інформаційні системи користувачів.

Висновки

1. Визначення протидії загрозам безпеки в інформаційних системах становить комплексну проблему, для вирішення якої необхідно поєднання заходів на законодавчому, адміністративному, процедурному і програмно-технічного рівнів ІБ.

2. Розробка та прийняття нормативно-правових актів у галузі захисту інформації покликані врегулювати безпечне використання інформаційно-комунікаційних технологій, доступу до інформації, захисту інформації від несанкціонованого доступу та витоку технічними каналами.

3. Призначення адміністративного рівня протидії загрозам інформаційної безпеки має зводитися до таких важливих практичних кроків як визначення керівних документів і стандартів, підходів до управління ризиками та сертифікація на відповідність стандартам інформаційної безпеки.

4. До процедурного рівня протидії загрозам відносяться організаційні заходи інформаційної безпеки. Важливою частиною побудови процедурного та програмно-технічного рівнів протидії загрозам інформаційної безпеки в системах е-урядування є розробка політики безпеки.

5. Політика безпеки (ПБ) в організаціях, підключених до систем е-урядування, являє собою сукупність принципів, правил, процедур і практичних рішень у галузі ІБ, які регулюють керування, захист та розподіл інформації, що захищається. ПБ залежить від багатьох чинників.

6. ПБ повинна враховувати сучасний стан та найближчі перспективи розвитку інформаційних технологій, мету, завдання, правові основи експлуатації ІС, режими функціонування об'єктів, містити аналіз загроз безпеки та способи їх реалізації.

7. Програмно-технічний рівень протидії загрозам ІБ передбачає такі механізми безпеки як ідентифікація і аутентифікація користува-

чів, управління доступом до ІС, протоколювання і аудит; криптографію, екранування каналів зв'язку, забезпечення високої доступності і т.п.

Запитання для самоконтролю

1. Які завдання вирішуються на законодавчому рівні забезпечення протидії загрозам інформаційної безпеки?
2. Які напрями державної інформаційної політики України мають безпекові складові? Наведіть приклади, що стосуються системи публічного управління.
3. Які Закони України врегульовують питання інформаційної безпеки в системах електронного урядування?
4. Що визначають адміністративний та процедурний рівні забезпечення протидії загрозам інформаційній безпеці?
5. Що передбачає оцінювання ризиків реалізації загроз інформаційній безпеці? У чому це виражається?
6. Що визначає програмно-технічний рівень забезпечення протидії загрозам інформаційній безпеці?
7. Які основні положення програмно-технічного рівня протидії загрозам?
8. Що розуміється під політикою безпеки інформаційних систем?

Рекомендована література

1. Кобозева А.А. Аналіз захищеності інформаційних систем: підручник / А.А. Кобозева, І.О. Мачалін, В.О. Хорошко. – К.: ДУІКТ, 2010. – 316 с.
2. Дубов Д.В. Основи електронного урядування: навч. посіб. / Д.В. Дубов, С.В. Дубова. – К.: Центр навч. літ., 2012. – 176 с.
3. Електронне урядування: опорний конспект лекцій /

С.В. Дзюба, І.Б. Жиляєв, С.К. Полумієнко [та ін.]; за ред. А.І. Семенченка. – К.: НАДУ, 2012. – 264 с.

4. Клімушин П.С. Електронне урядування в інформаційному суспільстві: монографія / П.С. Клімушин, А.О. Серенок. – Х.: Вид-во ХарРІ НАДУ «Магістр», 2010. – 312 с.

5. Бабаєв В.М. Електронне урядування: текст лекцій / В.М. Бабаєв, М.М. Новікова, С.О. Гайдученко. – Х.: ХНУМГ, 2014. – 127 с.

ЗАВДАННЯ ДО ПРАКТИЧНИХ ЗАНЯТЬ

Практична робота 1. Основні категорії інформації та правила інформаційної безпеки під час роботи з ресурсами Інтернет.

Метою практичної роботи є ознайомлення з основними категоріями інформації та підходами щодо забезпечення інформаційної безпеки. Під час виконання завдань практичної роботи необхідно використовувати літературу, що наведена у відповідному розділі та інформаційні ресурси мережі Інтернет.

Завдання 1. За допомогою даних літератури та пошуку в мережі Інтернет дайте визначення основним категоріям інформації та наведіть приклади класифікації інформації у відповідності до Закону України «Про інформацію»[44].

Завдання 2. За допомогою даних літератури та пошуку в мережі Інтернет надайте визначення інформації з обмеженим доступом, що зображено на рис. 8. Розгляньте різні категорії інформації з обмеженим доступом: конфіденційна, таємна та службова інформація. Наведіть приклади використання такої інформації в діяльності органів публічного управління та опишіть підходи щодо її захисту.

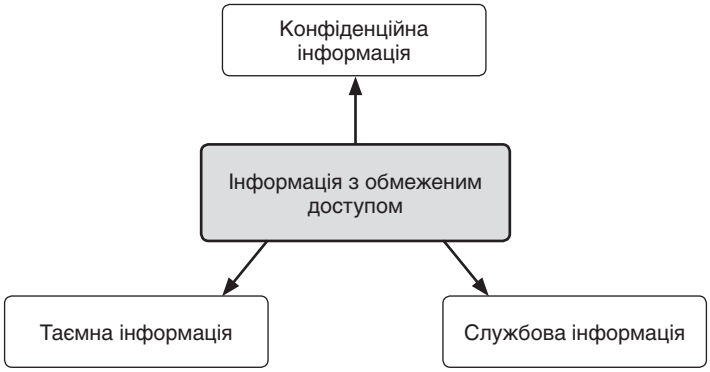


Рис. 8. Види інформації з обмеженим доступом за Законом України «Про інформацію» (стаття 21)

Завдання 3. За допомогою даних літератури та пошуку в мережі Інтернет виконайте аналіз відповідальності за порушення законодавства України про інформацію (рис. 9), наведіть приклади з практики діяльності органів публічного управління.

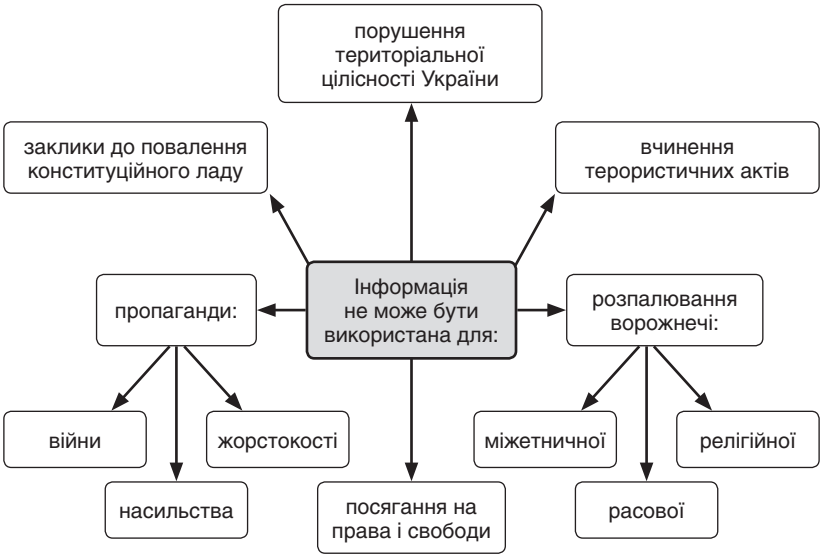


Рис. 9. Відповідальність за порушення законодавства про інформацію (за Законом України «Про інформацію», розділ IV)

Завдання 4. Знайдіть Інтернет-ресурси про правила безпеки по роботі з основними ресурсами Internet web, ftp, e-mail та з соціальними мережами. Зробіть висновки про культуру використання мережі Інтернет[45]. Знайдіть в мережі Інтернет відомі українські проекти: безпека дітей в Інтернеті, підготовку педагогів-тренерів з безпеки в Інтернеті. Поясніть на прикладах підходи щодо захисту дітей та молоді від негативних інформаційних впливів як один із напрямів державної політики України.

Практична робота 2. Визначення загроз інформаційної безпеки в системах електронного урядування.

Метою практичної роботи є аналіз загроз інформаційній безпеці, у тому числі внаслідок витоку інформації. Для виконання практичної роботи необхідно мати операційну систему Windows (7, 8 або 10) та програмні засоби, що забезпечують моніторинг з витоку інформації. Під час виконання завдань практичної роботи необхідно керуватися літературою, що наведена у відповідному розділі та інформаційними ресурсами мережі Інтернет.

Завдання 1. За допомогою даних літератури[46] та пошуку в мережі Інтернет зробіть висновки щодо можливих каналів витоку інформації, що зображені на рис. 10 та наведіть приклади, що можуть стосуватися органів публічного управління.

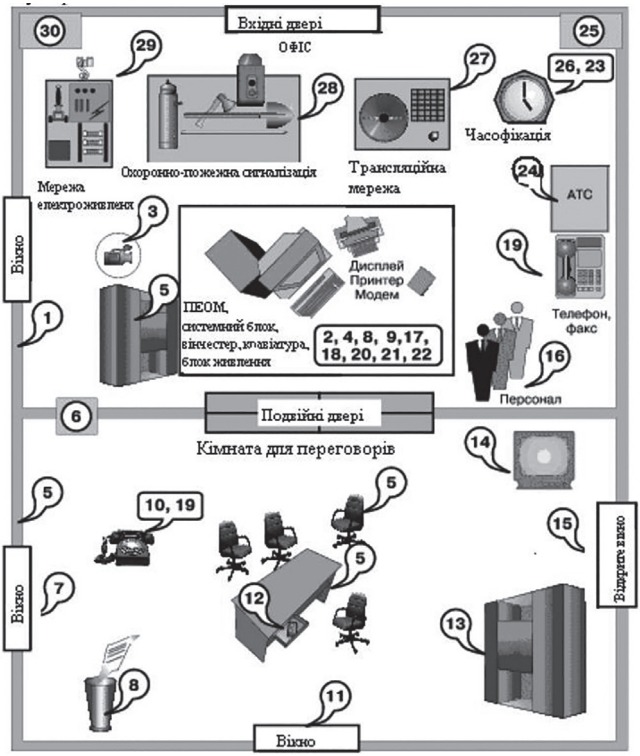


Рис. 10. Схема можливих каналів витоку і несанкціонованого доступу до інформації, що обробляється в типовому одноповерховому офісу

Завдання 2. За допомогою інформаційних ресурсів мережі Інтернет виконайте аналіз найбільш розповсюджених видів сучасних комп'ютерних загроз: несанкціонованого доступу до інформаційних ресурсів та інформаційно-телекомунікаційних систем; Інтернет-шахрайства та крадіжку коштів; роботу бот-мереж (botnet) та DDoS-атак (Distributed Denial of Service); «крадіжку особистості» (Identity Theft). Спрогнозуйте ступінь їх потенційного впливу на функціонування систем електронного урядування.

Завдання 3. Ознайомтесь з роботою та встановіть на робочі станції комп'ютерної лабораторії програмні засоби, що можуть забезпечувати моніторинг з витоку інформації: Mipko Employee Monitor, SmartWebCam, Actual Spy, Elite Keylogger, Spy And Control.

Практична робота 3. Протидія загрозам інформаційній безпеці в системах електронного урядування з використанням криптографічних програмних засобів в операційній системі Windows.

Метою практичної роботи є вивчення загального принципу дії криптографічних та стеганографічних програмних засобів методами шифрування (криптографія) та приховування (стеганографія) інформації та отримання практичного досвіду роботи з програмними засобами криптографії та стеганографії в операційній системі Windows. Для виконання практичної роботи необхідно мати операційну систему Windows (7, 8 або 10). Під час виконання завдань практичної роботи необхідно керуватися довідковою інформацією з мережі Інтернет.

Завдання 1. За допомогою пошуку в мережі Інтернет та даних літератури зробіть висновки щодо загального принципу дії криптографічних програмних засобів.

Завдання 2. За допомогою пошуку в мережі Інтернет та даних літератури зробіть висновки щодо загального принципу дії стеганографічних програмних засобів.

Завдання 3. Ознайомтесь з роботою та встановіть на робочі станції комп'ютерної лабораторії програмні криптографічні засоби із захисту інформації в операційній системі Windows: TrueCrypt, Kruptos 2 Professional, Dekart Private Disk Light, FET XP.

Завдання 4. Ознайомтесь з роботою та встановіть на робочі стан-

ції комп'ютерної лабораторії програмні засоби стеганографії в операційній системі Windows: Steganos LockNote, Steganos Privacy Suite.

Практична робота 4. Протидія загрозам інформаційної безпеки в системах електронного урядування з використанням антивірусних програмних засобів в операційній системі Windows

Метою практичної роботи є вивчення загального принципу дії вірусів та хробаків, методів боротьби та їх виявлення, видалення наслідків зараження та профілактику зараження. Робота передбачає ознайомлення з роботою: програмних засобів, що забезпечують антивірусний захист інформації; міжмережевих екранів (файєрволів). Для виконання практичної роботи необхідно мати операційні системи Windows (7, 8 або 10). Під час виконання завдань практичної роботи необхідно керуватися літературою, що наведена у відповідному розділі, та інформаційними ресурсами мережі Інтернет.

Завдання 1. За допомогою пошуку в мережі Інтернет та даних літератури зробіть висновки щодо загального принципу дії вірусів та хробаків, їх виявлення, методів боротьби з ними, видалення наслідків зараження та профілактики зараження, необхідних дій під час виявлення зараження вірусами.

Завдання 2. Ознайомтесь з роботою програмних засобів, що забезпечують антивірусний захист інформації. Розгляньте перелік антивірусного програмного забезпечення та антивірусних баз даних, що мають позитивний експертний висновок та рекомендовані[47] до роботи в органах публічного управління: Zillya! (дійсний до 20.10.2017), McAfee (дійсний до 29.12.2017), Kaspersky Internet Security (дійсний до 04.02.2018), ESET (дійсний до 22.07.2018), Symantec (дійсний до 22.07.2018).

Завдання 3. Ознайомтесь з роботою міжмережевих екранів (файєрволів), що забезпечують блокування потоків даних в корпоративних мережах та робочих станціях: Outpost Firewall Free, Ashampoo Firewall, Comodo Firewall, Windows 10 Firewall Control, Privatefirewall, SafeZone та інші.

Завдання 4. Встановіть на робочі станції комп'ютерної лабораторії антивірусні програмні засоби: avast, esset, McAfee.

Рекомендована література

1. Пам’ятка щодо дотримання вимог інформаційної безпеки при використанні систем дистанційного банківського обслуговування. – Режим доступу: https://www.otpbank.com.ua/pdf/big-corporate/pamyatka-dotrymannya-bezpeky.pdf – Назва з екрану.
2. Кочарян А. Б. Виховання культури користувача Інтернету. Безпека у всесвітній мережі: навч.-метод. посіб. / А. Б. Кочарян, Н. І. Гущина. – К., 2011. – 100 с.
4. Центр антивірусного захисту інформації Держспецзв’язку України. – Режим доступу: cazi.gov.ua – Назва з екрану.

ГЛОСАРІЙ

Атака – спроба реалізації загрози. Якщо атака є успішною, це називають проникненням. Наслідком успішної атаки є порушення безпеки інформації в системі, яке називають компрометацією.

Вади захисту – сукупність причин, умов і обставин, наявність яких може призвести до порушення нормального функціонування системи або політики безпеки інформації.

Витік інформації – неконтрольоване поширення інформації, яке призводить до її несанкціонованого отримання.

Загроза – будь-які обставини чи події, що можуть спричинити порушення політики безпеки інформації та нанесення збитку інформаційно-(теле)комунікаційній системі.

Закладний пристрій – потай встановлюваний технічний засіб, який створює загрозу для інформації.

Засіб технічного захисту інформації – пристрій та (чи) програмний засіб, основне призначення яких – захист інформації від загроз.

Захист інформації – це сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру.

Захищена комп'ютерна система – комп'ютерна система, що здатна забезпечувати захист інформації від визначених загроз.

Інформативний сигнал – фізичне поле та (чи) хімічна речовина, що містять інформацію.

Комплекс засобів захисту – сукупність програмно-апаратних засобів, що забезпечують реалізацію політики безпеки інформації.

Комплексна система захисту інформації – взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації.

Носій інформації – матеріальний об'єкт, що містить інформацію.

Побічне електромагнітне випромінення і наведення – електромагнітне випромінення і наведення, що є побічним результатом функціонування технічного засобу і може бути носієм інформації.

Приховування інформації (стеганографія) – спосіб технічного

захисту інформації, який полягає в унеможливленні або суттєвому утрудненні несанкціонованого отримання інформації.

Програмна закладка – потай упроваджена програма, яка створює загрозу для інформації, що міститься в комп'ютері.

Самочинний (технічний) канал витоку інформації – ненавмисний канал витоку інформації.

Система управління інформаційною безпекою – частина загальної системи управління організації, яка ґрунтується на підході, що враховує ризики інформаційної безпеки як бізнес-ризики, призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки.

Спеціальний вплив – вплив на технічні засоби, що призводить до здійснення загрози для інформації.

Штучний (технічний) канал витоку інформації – навмисний канал витоку інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про електронні документи та електронний документообіг: Закон України від 22 трав. 2003 р. № 851-IV. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/851-15.
2. Про електронний цифровий підпис: Закон України від 22 трав. 2003 р. № 852-IV. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/852-15.
3. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII, із змінами. – Режим доступу: zakon2.rada.gov.ua/laws/show/2657-12 – Назва з екрану.
4. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР, зі змінами. – Режим доступу: zakon5.rada.gov.ua/laws/show/80/94-вр. – Назва з екрану.
5. Про телекомунікації: Закон України від 18.11.2003 р. № 1280-IV, зі змінами. – Режим доступу: zakon3.rada.gov.ua/laws/show/1280-15. – Назва з екрану.
6. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007 № 537-V – Режим доступу: zakon5.rada.gov.ua/laws/show/537-16 – Назва з екрану.
7. Про Національну програму інформатизації: Закон України від 04.02.1998 р. № 74/98-ВР, із змінами. – Режим доступу: zakon0.rada.gov.ua/laws/show/74/98-вр. – Назва з екрану.
8. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 27.01.2016 р. № 96/2016. – Режим доступу: http://www.president.gov.ua/documents/962016-19836. – Назва з екрану.
9. Про затвердження Концепції технічного захисту інформації в Україні: постанова Кабінету Міністрів України від 08.10.1997 р. № 1126, із змінами. – Режим доступу: zakon3.rada.gov.ua/laws/show/1126-97-п. – Назва з екрану.
10. Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформа-

ційних ресурсів та інформації, вимога щодо захисту якої встановлена законом (станом на 15 серпня 2016 року). – Режим доступу: www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=234237&cat_id=39181. – Назва з екрану.

11. Стратегія національної безпеки України: затверджена Указом Президента України «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» від 26 травня 2015 року № 287/2015. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/287/2015
12. Василюк В. Об'єкти захисту інформації. Методи та засоби захисту інформації / В. Василюк // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2006. – № 2 (13). – С. 88–102.
13. Електронне урядування: опорний конспект лекцій / С.В. Дзюба, І.Б. Жиляєв, С.К. Полумієнко [та ін.]; за ред. А.І. Семенченка. – К.: НАДУ, 2012. – 264 с.
14. Захист інформації // Вікіпедія. – Режим доступу: https://uk.wikipedia.org/wiki/. – Назва з екрану.
15. Ляшенко І.О. Європейські критерії безпеки інформаційних технологій / І.О. Ляшенко // Сучасні інформаційні технології у сфері безпеки та оборони. – 2012. – № 1 (13). – С. 84–86.
16. Остапов С.Е. Технології захисту інформації: навчальний посібник / С.Е. Остапов, С.П. Євсеєв, О.Г. Король. – Х.: ХНЕУ, 2013. – 476 с.
17. Офіційний веб-сайт Державної служби спеціального зв'язку та захисту інформації України: нормативно-правова база. – Режим доступу: www.dstszi.gov.ua/dstszi/control/uk/index – Назва з екрану.
18. Теоретические основы компьютерной безопасности / П.Н. Девянин, О.О. Михальский, Д.И. Правиков [и др.]. – М.: Радио и связь, 2000. – 192 с.
19. Хорошко В.О. Основи інформаційної безпеки: підручник / В.О. Хорошко, В.С. Чередниченко, М.Є. Шелест; за ред. В.О. Хорошка. – К.: ДУІКТ, 2008. – 186 с.
20. Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures:

Resolution adopted by the General Assembly on 21 December 2009. – Access mode: www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211. – Title from the screen.

21. Developments in the field of information and telecommunications in the context of international security: Resolution adopted by the General Assembly on 2 December 2009. – Access mode: www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/25. – Title from the screen.
22. Developments in the field of information and telecommunications in the context of international security: Report of the Secretary-General. – Access mode: www.un.org/ga/search/view_doc.asp?symbol=A/71/172. – Title from the screen.
23. Developments in the field of information and telecommunications in the context of international security: United Nations Office for Disarmament Affairs. – Access mode: www.un.org/disarmament/topics/informationsecurity. – Title from the screen.

ПРИМІТКИ

1 Про інформацію: Закон України від 02.10.1992 р. № 2657-XII, із змінами. URL: zakon2.rada.gov.ua/laws/show/2657-12.
2 Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007 р. № 537-V. URL: zakon5.rada.gov.ua/laws/show/537-16.
3 Захист інформації. Вікіпедія. URL: https://uk.wikipedia.org/wiki/.
4 Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94-вр, із змінами. URL: zakon5.rada.gov.ua/laws/show/80/94-вр.
5 Остапов С. Е. Технології захисту інформації: навч. посіб. Харків, 2013. 476 с.
6 Про затвердження Концепції технічного захисту інформації в Україні: постанова Кабінету Міністрів України від 08.10.1997 р. № 1126, із змінами. URL: zakon3.rada.gov.ua/laws/show/1126-97-п.
7 Остапов С. Е. Технології захисту інформації: навч. посіб. Харків, 2013. 476 с.
8 Електронне урядування: опорний конспект лекцій. К., 2012. 264 с.
9 Теоретические основы компьютерной безопасности. Москва, 2000. 192 с.
10 Ляшенко І. О. Європейські критерії безпеки інформаційних технологій. Сучасні інформаційні технології у сфері безпеки та оборони. 2012. № 1 (13). С. 84–86.
11 Василюк В. Об'єкти захисту інформації. Методи та засоби захисту інформації. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2006. № 2 (13). С. 88–102.
12 Офіційний веб-сайт Державної служби спеціального зв'язку та захисту інформації України: нормативно-правова база. URL: www.dstszi.gov.ua/dstszi/control/uk/index.
13 Про інформацію: Закон України від 02.10.1992 р. № 2657-XII, із змінами. URL: zakon2.rada.gov.ua/laws/show/2657-12.
14 Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР, зі змінами. URL: zakon5.rada.gov.ua/laws/show/80/94-вр.
15 Про телекомунікації: Закон України від 18.11.2003 р. № 1280-IV, зі змінами. URL: zakon3.rada.gov.ua/laws/show/1280-15.
16 Про Національну програму інформатизації: Закон України від 04.02.1998 р. № 74/98-ВР, із змінами. URL: zakon0.rada.gov.ua/laws/show/74/98-вр.
17 Впровадження європейської кібербезпеки: загальний огляд. URL: http://www.isaca.org/Knowledge-Center/Research/Documents/European-Cybersecurity-Implementation-Overview_res_Ukr_1215.pdf .
18 EU Cybersecurity Policy: A Model for Global Governance. URL: www.atlantic-community.org/-/eu-cybersecurity-policy-a-model-for-global-governance.
19 Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures: Resolution adopted by the General Assembly on 21 December 2009. URL: www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211.
20 Developments in the field of information and telecommunications in the context of international security: Resolution adopted by the General Assembly on 2 December 2009. URL: www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/25.
21 Developments in the field of information and telecommunications in the context of international security: Report of the Secretary-General. URL: www.un.org/ga/search/view_doc.asp?symbol=A/71/172.

22 Developments in the field of information and telecommunications in the context of international security: United Nations Office for Disarmament Affairs. URL: www.un.org/disarmament/topics/informationsecurity.
23 The Directive on security of network and information systems (NIS Directive). Digital Economy & Society. URL: ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.
24 Президент Ниинистё и министерская комиссия обсудили киберстратегию: UUTISET > Новости. URL: yle.fi/uutiset/prezident_niiniste_i_ministerskaya_ komissiya_obsudili_ kiberstrategiyu/6601382.
25 Финляндия участвует в военных учениях на случай кибервойны: UUTISET > Новости. URL: yle.fi/uutiset/finlyandiya_uchastvuet_v_voennykh_ucheniyakh_ na_sluchai_ kibervoiny/6601505.
26 Finnish Security and Defence Policy 2012: Government Report from 01.2013. URL: www.bbn.gov.pl/ftp/dok/07/FIN_Finnish_Security_Defence_Policy_2012_Government_ Report.pdf
27 Finland's Cyber security Strategy: Government Resolution from 01.2013. URL: www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf .
28 Стратегія національної безпеки України: затверджена Указом Президента України від 26 трав. 2015 р. № 287/2015. URL: http://zakon5.rada.gov.ua/laws/show/287/2015.
29 Про Стратегію кібербезпеки України: Рішення Ради національної безпеки і оборони України від 27 січня 2016 року. URL: www.president.gov.ua/documents/962016-19836.
30 Центральний засвідчувальний орган: Головна сторінка. URL: www.czo.gov.ua.
31 Про електронний цифровий підпис: Закон України від 22.05.2003 № 852-IV. URL: zakon5.rada.gov.ua/laws/show/852-15.
32 Про внесення змін до наказу Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 05 груд. 2013 р. № 2563/5/645: Наказ. URL: zakon4.rada.gov.ua/laws/show/v2170323-14.
33 Про електронні документи та електронний документообіг: Закон України від 22.05.2003 р. № 851-IV. URL: zakon3.rada.gov.ua/laws/show/851-15.
34 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures: Access to European Union law. URL: eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31999L0093.
35 Бойко Д. В. Вимоги до центрів сертифікації ключів. Право та інновації. 2014. № 3 (7). С. 43–48.
36 The National Cyber Security Centre Finland (NCSC-FI): The Finnish Communications Regulatory Authority (FICORA). URL: www.viestintavirasto.fi/en/ cybersecurity.html.
37 FINAS: Finnish Accreditation Service. URL: www.finas.fi/sites/en/Pages/ default.aspx.
38 Information security and cybersecurity: Ministry of Finance. URL: vm.fi/en/information-security-and-cybersecurity.
39 e-Government in Finland. European Commission. URL: joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernmnent%20in%20Finland% 20-%20February%202016%20-%2018_00%20-%20v2_00.pdf.
40 Державна служба спеціального зв'язку та захисту інформації України: Офіційний сайт. URL: www.dstszi.gov.ua/dstszi/control/uk/index.
41 Міжвідомча комісія з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України. Офіційний сайт. URL: www.vaibit.org.
42 CERT-UA, About US. Офіційний сайт. URL: cert.gov.ua/?page_id=207.

43 Valtori: Government ICT Centre. URL: www.valtori.fi/en-US/.
44 Про інформацію: Закон України від 02.10.1992 р. № 2657-XII, із змінами. URL: zakon2.rada.gov.ua/laws/show/2657-12.
45 Кочарян А. Б. Виховання культури користувача Інтернету. Безпека у всесвітній мережі: навч.-метод. посіб. Київ, 2011. 100 с.
46 Василюк В. Об'єкти захисту інформації. Методи та засоби захисту інформації. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2006. № 2 (13). С. 88–102.
47 Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом (станом на 15 серпня 2016 року. URL: www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=234237&cat_id=39181.

Навчальне видання

Олександр Мирославович Хошаба

Загальна редакція
Андрій Іванович Семенченко, Валерій Михайлович Дрешпак

ЕЛЕКТРОННЕ УРЯДУВАННЯ ТА ЕЛЕКТРОННА ДЕМОКРАТІЯ

Навчальний посібник у 15 частинах

Частина 13

ЗАХИСТ ІНФОРМАЦІЇ В СИСТЕМАХ ЕЛЕКТРОННОГО УРЯДУВАННЯ

Формат 60×90/16.
Папір офс. 80 г/м² . Гарн. Таймс. Друк офс.
Ум. друк. арк. 4,5. Авт. арк. 3,0.
Наклад 500 прим.

Видавець та друк: ФОП Москаленко О. М.,
print.ukr@gmail.com