ТЕМА 3
ДІЯЛЬНІСТЬ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1. Загальні відомості

Серед міжнародних організацій, що діють у сфері інформаційної безпеки та роблять істотний вплив на функціонування глобальних інформаційних систем і діяльність всього інформаційного співтовариства, виділяються організації таких типів.

1. Великі міжнародні некомерційні та неурядові організації, що об'єднують фахівців у певних областях, що існують, як правило, вже протягом багатьох років і охоплюють безліч основних напрямків розвитку комп'ютерної інженерії, електроніки та телекомунікацій, включаючи в тому числі і певні питання забезпечення безпеки сучасних інформаційних технологій.
1. Окремі відносно невеликі організації, які спеціалізуються на більш-менш вузьких питаннях інформаційної безпеки, що мають глобальне значення для всього співтовариства користувачів інформаційних систем, і з'явилися на базі приватних компаній або дослідницьких структур протягом останнього десятиліття, коли проблеми інформаційної безпеки стали особливо актуальними.
2. Спільні структури (комітети, альянси і т.п.), створювані (іноді тимчасово) великими компаніями (іноді за участю великих дослідницьких центрів, навчальних закладів та урядових структур) для вирішення певних завдань у сфері інформаційних технологій та інформаційної безпеки.

Кожна з них, у свою чергу, має свої специфічні організаційні особливості, проте всі вони, як правило, вирішують завдання розробки, узгодження та подальшого поширення загальних для всього співтовариства користувачів інформаційних систем технічних і організаційних рішень, таких як:

- протоколи глобальних мереж;
- архітектури, алгоритми, протоколи загально доступних засобів шифрування даних;
- правила побудови глобальних мереж обміну даними та інших елементів

глобальної інфраструктури інформаційної безпеки.

Також важливими елементами організаційної роботи на рівні міжнародних структур є:

- організація обміну знаннями та актуальними новинами в середовищі фахівців з інформаційної безпеки в таких формах, як публікація спеціалізованих періодичних видань та збірників наукових праць, організація спеціалізованих науково-практичних конференцій, семінарів тощо;
- організація та підтримка в актуальному стані баз даних і баз знань, які містять відомості, необхідні користувачам інформаційних систем, адміністраторам, розробникам та іншим учасникам для забезпечення інформаційної безпеки. Прикладами таких баз даних є бази даних, що містять відомості про виявлені вразливості різних програмних і апаратних платформ інформаційних систем.

В цілому організаційна робота на рівні міжнародних структур не є універсальною, і в більшості випадків вони будують свою роботу самостійно. Однак можна виділити деякі основні організаційні принципи, характерні для діяльності багатьох з них:

- принцип добровільності участі в роботі таких структур і в окремих проектах або у всій роботі;
- принцип відкритості (доступності) результатів роботи (всіх або їх частини) для спільноти фахівців у сфері інформаційних технологій;
- принцип самофінансування.

3.2. Робота міжнародних професійних об'єднань

Робота великих міжнародних професійних (галузевих) організацій (об'єднань), як правило, має наступні особливості:

- вона, як правило, не спрямована тільки на вирішення завдань інформаційної безпеки – завдання інформаційної безпеки вирішуються в комплексі з безліччю інших проблем (розвитку інформаційних технологій, побудови телекомунікаційних систем тощо);

- вона певною мірою може спиратися на підтримку з боку різних державних структур;
- вона об'єднує велику кількість фахівців з різних дослідних, навчальних, комерційних організацій, але при цьому більшість учасників (членів) може не мати конкретних зобов'язань, що зобов'язують вносити вклад в роботу і досягати певних цілей.

Основними найбільш великими і відомими міжнародними професійними об'єднаннями, так чи інакше пов'язаними з питаннями інформаційної безпеки, є:

- ITU – International Telecommunication Union;
- IEEE – Institute of Electrical and Electronics Engineers;
- ACM – Association for Computing Machinery;
- W3 Consortium;
- ISSA – Information Systems Security Association;
- ISO – International Organization for Standardization;
- IETF – Internet Engineering Task Force;
- ICSA – International Computer Security Association;
- Information Systems Audit and Control Association (ISACA);
- Internet Security Alliance.

3.3. International Telecommunication Union (ITU) – Міжнародний союз електрозв’язку

ITU є найстарішою міжнародною організацією, пов’язаною з інформаційними технологіями. Вона була заснована в 1885 році як Міжнародний телеграфний союз і отримала свою нову назву в 1934 році. В даний час ITU об'єднує близько 180 держав. Як зрозуміло з назви, основним її завданням спочатку було управління та координація діяльності у сфері передачі інформації і, зокрема, в радіозв'язку та телеграфного зв'язку. Однак у міру розвитку глобальних комп'ютерних мереж та інтеграції комп'ютерних і телекомунікаційних систем, сфера діяльності ITU була значно розширена і в даний час включає в себе безліч питань, пов'язаних з побудовою комп'ютерних мереж, передачею цифрових даних, обробкою інформації тощо.

Членами ITU-T є:

- державні органи влади (міністерства і відомства зв'язку окремих країн);
- наукові організації і компанії – виробники телекомунікаційного обладнання;
- регіональні та міжнародні телекомунікаційні організації.

Функціональними органами ITU-T є:

- Всесвітня асамблея з стандартизації телекомунікацій (World Telecommunication Standardization Assembly), що проводиться кожні чотири роки, – основний керівний орган сектора стандартизації;
- Бюро з стандартизації телекомунікацій (Telecommunication Standardization Bureau) – виконавчий підрозділ сектора стандартизації;
- Дослідницькі групи (всього їх 14);
- Консультативна група з стандартизації телекомунікацій (Telecommunication Standardization Advisory Group) – допоміжний підрозділ, що здійснює координаційну роботу.

Вищим органом влади Союзу є Повноважна Конференція (Plenipotentiary Conference), збори делегацій держав – членів Союзу, що проходить раз на чотири роки. Основні виконавчі органи – Рада і Генеральний секретаріат ITU. Основні робочі підрозділи розділені на три сектори:

- сектор стандартизації зв'язку, ITU-T;
- сектор радіозв'язку, ITU-R;
- сектор розвитку електрозв'язку ITU-D.

ITU-R і ITU-D виконують окремі дослідницькі, координаційні та технічні функції (такі як, наприклад, реєстрація радіочастот або координація роботи космічних телекомунікаційних супутників), тоді як Сектор стандартизації зв'язку – ITU-T більшою мірою відповідає за вирішення стратегічних завдань розвитку інформаційних технологій та інфраструктури і, зокрема, за розробку методик і стандартів, необхідних для всієї світової спільноти.

Основною метою роботи ITU-T є розробка універсальних рекомендацій та міжнародних стандартів, що відносяться до різних сфер телекомунікаційних технологій та управління телекомунікаціями. Розроблювані рекомендації

забезпечують основу для розвитку ринку послуг зв'язку, створення сумісних технічних та організаційних систем тощо. З точки зору забезпечення інформаційної безпеки найбільш значущими стали рекомендації, що відносяться до серії «X – Мережі передачі даних і зв'язок відкритих систем» і, зокрема, до серії «X.8xx – Безпека».

Відповідно до Резолюції 1 Всесвітньої асамблеї зі стандартизації телекомунікацій 2000-го року, була введена практика призначення Провідних дослідницьких груп (Lead Study Groups, LSGs) з певних питань, що вимагають одночасної координації зусиль кількох дослідницьких груп, які працюють в різних областях. Починаючи з вересня 2001 року функціонує «Дослідницька група 17: Мережі передачі даних та телекомунікаційне програмне забезпечення» («StudyGroup 17: Data Networks and Telecommunication Software»), утворена на основі існуючих до цього «Дослідницької групи 7» і «Дослідницької групи 10». З моменту свого утворення вона є Провідною дослідницькою групою з питань безпеки комунікаційних систем (Communication Systems Security, CSS) і, відповідно, не тільки працює над забезпеченням безпеки технологій, що безпосередньо належать до її компетенції, а й контролює питання забезпечення безпеки різних комунікаційних технологій, що розробляються іншими дослідницькими групами.

Однією з найбільш значущих розробок цієї групи в сфері інформаційної безпеки вважається Стандарт X.509, що заклав основи розвитку інфраструктури відкритих ключів. Найбільш актуальними проблемами, над якими нині працює Провідна дослідницька група з питань безпеки комунікаційних систем, є:

- управління безпекою;
- безпека мобільних систем;
- безпека систем зв'язку служб реагування на надзвичайні ситуації;
- телебіометрія.

В цілому ж робота цієї дослідницької групи охоплює наступні основні сфери:

- безпека управління мережами (включає в себе роботу над наступними рекомендаціями: M.3010 – Принципи мереж управління телекомунікаціями, M.3016 – Огляд безпеки мереж управління телекомунікаціями і деякі інші);

- автентифікація і служби каталогів (X.500 – Огляд концептуальних моделей і сервісів, X.509 – Основи технології відкритих ключів і сертифікатів і деякі інші);
- управління системами (X.733 – Функція звіту про подію, X.740 – Функція проведення аудиту безпеки та деякі інші);
- основи архітектури безпеки (X.800 – Архітектура безпеки інфраструктури відкритих систем для додатків ITU; X.802 – Модель безпеки нижніх рівнів, X.803 – Модель безпеки верхніх рівнів і деякі інші);
- факсимільний зв’язок (T.36 – Можливості забезпечення безпеки при використанні факсимільних апаратів третьої групи; T.563 – Характеристики терміналів для використання з факсимільними апаратами четвертої групи і деякі інші);
- телевізійні та кабельні системи (J.170 – Специфікація безпеки IPCabelcom і деякі інші);
- техніка забезпечення безпеки (X.841 – Об'єкти інформаційної безпеки для контролю доступу та деякі інші);
- мультимедійні комунікації (H.233 – Система забезпечення конфіденційності для аудіовізуальних сервісів, H.234 – Управління ключами шифрування і системою аутентифікації в аудіовізуальних сервісах і деякі інші).

Крім розробки рекомендацій і стандартів, одним з важливих напрямків роботи ITU також стало забезпечення інформаційного обміну в різних формах: поширення методичних матеріалів, що стосуються забезпечення інформаційної безпеки, проведення семінарів і конференцій. Одним з найбільш масштабних таких заходів є Всесвітній саміт з інформаційного суспільства (WSIS: The World Summit On The Information Society).

3.4. Institute of Electrical and Electronics Engineers (IEEE) – Інститут інженерів з електроніки та електротехніки

IEEE є однією з найбільш відомих професійних організацій, існує з 1884 року і в даний час налічує близько 380 тисяч членів із 150 країн світу. У сферу її інтересів входить безліч питань, пов’язаних з електротехнікою, радіоелектронікою,

обчислювальною технікою, інформатикою, а також деякими розділами фізики і математики.

Основні напрямки роботи цієї організації:

- проведення спеціалізованих професійних конференцій;
- публікація спеціалізованих видань;
- підтримка освітньої діяльності;
- підтримка інноваційних технічних та методичних розробок у різних сферах;
- розробка та поширення технічних стандартів.

До складу IEEE входять 10 регіональних відділень, 38 професійних товариств, 4 ради і 1450 студентських відділень. Поточне управління діяльністю на верхньому рівні здійснюється Радою директорів і Виконавчим комітетом, роботу яких очолюють Президент та Виконавчий директор.

Одним з основних підрозділів IEEE, що спеціалізуються на питаннях інформаційної безпеки, є Технічний комітет з безпеки і захисту приватної інформації – «IEEE Computer Society Technical Committee on Security and Privacy» (http://www.ieee-security.org/). У його складі функціонують три підкомітети:

- підкомітет з стандартів (Subcommittee on Standards);
- підкомітет з академічної роботи (Subcommittee on Academic Affairs);
- підкомітет з спеціалізованих конференцій (Subcommittee on Security Conferences).

Основними заходами, які проводить цей комітет, є :

- щорічний симпозіум з безпеки і захисту приватної інформації (IEEE CS Symposium on Security and Privacy);
- щорічний семінар з основ інформаційної безпеки (Computer Security Foundations Workshop).

Також комітет веде роботу зі збору та узагальненню актуальної інформації про події в співтоваристві фахівців з інформаційної безпеки: оголошення про заплановані конференції, звіти про минулі конференції і семінари, огляди літератури та періодики, посилання на ресурси в мережі Інтернет і т.п. Спеціальний інформаційний бюлетень з цією інформацією – «Cipher» – розсилається передплатникам в середньому один раз в два місяці.

3.5. Association for Computing Machinery (ACM) – Асоціація обчислювальної техніки

ACM є однією з найстаріших організацій, пов'язаних з інформаційними технологіями, – вона була заснована в 1947 році, на зорі розвитку комп'ютерної техніки. Основні завдання ACM – підтримка освітніх проектів у сфері інформаційних технологій, організація науково-практичних конференцій, симпозіумів та семінарів, суспільно-політична робота, пов'язана з інформаційними технологіями, публікація періодичних видань та збірників наукових праць, присвячених проблемам сучасних інформаційних технологій, підтримка електронного архіву таких публікацій, а також інша подібна діяльність. Основним керуючим органом цієї організації є Рада ACM, до якої входить 16 осіб, у тому числі президент і віце-президент. Управління поточними справами Асоціації здійснюють чотири профільних комітети. Штаб-квартира ACM, в якій працюють основні виконавчі органи, розташовується в Нью-Йорку, починаючи з 1960 року.

Однією з основ організації роботи ACM є поділ всієї спільноти членів асоціації на так звані групи спеціальних інтересів *(Special Interests Group – SIG)* – підрозділи, що спеціалізуються на окремих відносно вузьких проблемах розвитку інформаційних технологій. Всього ACM об'єднує 34 групи, що спеціалізуються на різних питаннях розробки та використання програмного забезпечення, апаратних засобів і телекомунікацій. Кожна з груп самостійно визначає для себе межі своєї діяльності, а їхня політика та фінансові питання координуються одним з комітетів.

Одна з цих груп – **Special Interest Group on Security, Audit and Control** (SIGSAC, Група спеціальних інтересів з питань безпеки, аудиту та контролю, http://www.acm.org/sigs/sigsac/) – спеціалізується на питаннях інформаційної безпеки.

Основним завданням цієї групи є організація роботи спеціалізованих науково-практичних конференцій, таких як:

- Симпозіум з технологій і моделей управління доступом (SACMAT: ACM Symposium on Access Control Models and Technologies), що проводиться щорічно починаючи з 1995 року;
- Конференція з безпеки комп'ютерів і комунікацій(CCS:ACM Conference on Computer and Communications Security), проводиться щорічно починаючи з

1993 року.

Крім того, питання інформаційної безпеки прямо або побічно зачіпаються в роботі інших спеціалізованих груп Асоціації, таких як, наприклад, Special Interest Group on Electronic Commerce (Група з проблем електронної комерції).

3.6. World Wide Web Consortium (W3C) – Консорціум Всесвітньої Павутини

Створення W3C було ініційовано в 1989 році з метою розробки єдиних, узгоджених стандартів обміну інформацією в глобальних мережах передачі даних, а офіційно створення консорціуму було оформлено в 1994р. Його основними завданнями є:

- забезпечення можливості доступу до мережі Інтернет для якомога більшого числа людей незалежно від знання іноземних мов, культурної приналежності, географічного положення і доступних їм технічних засобів і технічної інфраструктури;
- забезпечення можливості підключення до Інтернет різних технічних пристроїв;
- забезпечення можливості структурування та формалізації інформації, доступної через Інтернет, з метою зробити її якомога більш придатною для автоматизованої обробки;
- забезпечення надійності та безпеки обміну інформацією, а також можливості брати участь в інформаційному обміні з тим рівнем захищеності, який окремі користувачі вважають для себе за потрібний.

До теперішнього часу консорціум об’єднує більше чотирьохсот провідних технологічних і телекомунікаційних компаній, урядових організацій, дослідницьких центрів, інститутів і університетів по всьому світу. Крім того, в штаті консорціуму знаходяться близько 70 незалежних технічних експертів, які забезпечують його роботу. Фінансування діяльності здійснюється за рахунок членських внесків, а основні адміністративні функції і повсякденна діяльність виконуються на базі трьох організацій:

- Массачусетський технологічний інститут (США);
- Європейський консорціум з досліджень в галузі інформатики та математики (Франція);

- Університет Кейо (Японія).

Крім формування стандартів («рекомендацій»), ця організація також займається освітньою діяльністю та надає можливості для обговорення різних питань, пов'язаних з функціонуванням мережі Інтернет.

Діяльність консорціуму організована у вигляді груп: Робочі групи (займаються опрацюванням технічних питань), Групи спеціальних інтересів і Координаційні групи (забезпечують взаємодію між іншими групами). У кожну групу входять представники організацій-учасників консорціуму і запрошені експерти. Сфери роботи консорціуму («домени», Domain), розділені на напрями (Activities). Робота по двадцяти чотирьох напрямках виконується в цілому шістдесятьма групами.

Питаннями інформаційної безпеки займається сфера «Технологія і суспільство» (Technology and Society Domain) в рамках спеціального напряму «Безпека» (W3C Security Activity), що складається з двох робочих груп. Також до 2006 року в складі Консорціуму функціонувало напрям «Захист приватної інформації» (Privacy).

До робіт консорціуму у сфері інформаційної безпеки відносяться:

- розробка стандарту цифрових підписів для інформаційних ресурсів (PICS Signed Labels 1.0 Specification);
- розробка системи електронного підпису для документів XML;
- розробка стандартів передачі зашифрованих даних з використанням мови XML.

3.7. NIST

NIST – Національний інститут стандартів і технологій, США (The National Institute of Standards and Technology) – заснований в 1901 році і до 1988 року відомий як Національне бюро стандартів (National Bureau of Standards (NBS)). Інститут є підрозділом Управління по технологіям США, одного з агентств Департаменту торгівлі США.

Основні завдання: сприяння підвищенню інноваційної та індустріальної конкурентоспроможності США шляхом розвитку наук щодо вимірювання, стандартизації і технології з метою підвищення економічної безпеки і поліпшення якості життя.

Інститут реалізує свою місію в чотирьох спільних програмах:

- NIST Laboratories – лабораторії NIST – проводять дослідження в галузі розвитку технологічної інфраструктури промисловості США для постійного поліпшення вироблених товарів і послуг%
- Baldrige National Quality Program – національна програма контролю якості ім. Балдріджа – забезпечує перевірку якості діяльності виробничих і сервісних підприємств, освітніх і медичних установ, некомерційних організацій; організовує програми підтримки організаціям і проводить щорічне вручення Національної премії якості імені Малкома Балдріджа за досягнення високих результатів діяльності і високу якість;
- Hollings Manufacturing Extension Partnership – мережа локальних центрів, що пропонують технічну і підприємницьку допомогу невеликим підприємствам;
- Technology Innovation Program – програма підтримки інноваційних технологій – пропонує часткову компенсацію досліджень перспективних технологій для задоволення державних і соціальних потреб суспільства.

Національний інститут стандартів і технології (NIST), разом з Американським національним інститутом стандартів (ANSI) бере участь в розробці стандартів і специфікацій до програмних рішень, що застосовуються як в державному секторі США, так і має комерційне застосування. З більш детальною інформацією щодо діяльності Інституту можна ознайомитись за посиланням: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf

3.8. International Organization for Standardization (ISO) – Міжнародна організація по стандартизації

ISO в нинішньому вигляді була заснована в 1946р. І являє собою неурядове об’єднання національних організацій з стандартизації, націлене на уніфікацію стандартів (головним чином, технічних) в різних областях виробничої діяльності та надання послуг.

Крім основних членів (близько 150 країн), які безпосередньо беруть участь у роботі, в ISO також входять члени-кореспонденти (Correspondent member) – країни, що не мають повноцінних органів стандартизації, а також члени-передплатники

(Subscriber member) – країни з невеликими економіками, які отримують необхідну довідкову інформацію на пільгових умовах.

Головним органом управління ISO є щорічна Генеральна Асамблея, яка приймає стратегічні рішення, що стосуються розвитку всієї організації. Підготовкою матеріалів для прийняття таких рішень займається Рада ISO, збори якої проходять два рази на рік. Безпосередньою розробкою стандартів займаються технічні комітети і підкомітети, в роботі яких беруть участь представники зацікавлених країн. За розробку кожного документа в підкомітеті відповідає спеціально створювана для цього робоча група. Проекти міжнародних стандартів, прийняті технічними комітетами, розсилаються в національні організації для голосування; документ набуває статусу міжнародного стандарту, якщо за нього проголосувало не менше 75% членів, які брали участь у голосуванні.

Основним підрозділом ISO, який займається питаннями інформаційної безпеки, є Об'єднаний технічний комітет JTC 1 «Інформаційні технології», до складу якого входить підкомітет SC 27 «Засоби безпеки в інформаційних технологіях «(IT Security techniques). За час своєї роботи цей підкомітет розробив понад 60 міжнародних стандартів, що відносяться до інформаційної безпеки.

З питаннями інформаційної безпеки також пов'язана робота підкомітету SC 37 «Біометрична ідентифікація» (Biometrics) та підкомітету SC 17 «Картки і персональна ідентифікація» (Cards and personal identification) .

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ:

1. Що є елементами організаційної роботи на рівні міжнародних структур?
2. Назвіть основні найбільш великі і відомі міжнародні об’єднання, пов’язані з питаннями інформаційної безпеки.
3. Назвіть основні завдання Консорціуму Всесвітньої Павутини.
4. Назвіть головні завдання Міжнародної організації по стандартизації.