ТЕМА 5
СПЕЦІАЛІЗОВАНІ МІЖНАРОДНІ ОРГАНІЗАЦІЇ ТА ОБ'ЄДНАННЯ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

5.1 Вступ

Спеціалізовані організації, що мають глобальний вплив на управління інформаційною безпекою на різних рівнях і загальний стан інформаційної безпеки, як правило, можуть функціонувати на базі:

- приватних компаній, що займаються дослідженнями, розробками та консультаціями у сфері інформаційної безпеки;
- великих навчальних закладів, що спеціалізуються на інформаційних технологіях, а також володіють значним авторитетом та фінансовими ресурсами;
- урядових установ, відповідальних за забезпечення інформаційної безпеки в певних сферах.

Основним напрямком організаційної роботи, що здійснюється в такій формі, стає формування та підтримка баз даних, що містять інформацію про вразливості різних програмних і апаратних засобів, що стали відомими, а також інші форми та напрями інформаційної, консультативної та методичної роботи в даній сфері.

Важливими чинниками успішності функціонування таких організацій є об'єднання інформації з якомога більшої кількості джерел (зокрема, від якомога більшої кількості фахівців і компаній, що займаються проблемами інформаційної безпеки) і якомога більш ефективне поширення відомостей (знань) в співтоваристві користувачів інформаційних систем.

Зважаючи на те, що така форма організаційної роботи заснована на приватних компаніях і відносно невеликих установах, підходи до організації та управління зазвичай не підпорядковуються будь-яким загальним правилам. Також склад таких організацій може з часом змінюватися: на зміну одним дослідницьким центрам можуть приходити інші – більш успішні та ефективні – з тими ж функціями. В даний час можна виділити наступні найбільш значущі організації, що займають цю нішу:

- CERT Coordination Center – Координаційний центр CERT;
- Дослідницька група X-Force компанії IBM.

5.2 CERT Coordination Center (CERT/CC) – Координаційний центр CERT

CERT/CC, що виникла в 1988 році як Computer security incident response team (Група реагування на інциденти, пов'язані з комп'ютерною безпекою), функціонує на базі Інституту розробки програмного забезпечення при Університеті Карнегі-Мелон (Software Engineering Institute, Carnegie Mellon University) і фінансується Міністерством оборони та Міністерством національної безпеки США. Поряд з проведенням незалежних досліджень та вирішенням різних завдань по забезпеченню безпеки глобальної інформаційної інфраструктури, ця організація забезпечує централізований збір відомостей про всі вразливості в різних інформаційних системах і підтримка актуальної бази знань про уразливість в інформаційних системах. Відомості про знову виявлені вразливості, шкідливі програми і способи порушення інформаційної безпеки розсилаються по електронній пошті: передплатниками цього бюлетеня є більш 161000 фахівців у всьому світі.

В рамках цієї діяльності *CERT*/CC здійснює постійну дослідницьку роботу:

- визначення характеру можливих наслідків використання виявлених вразливостей і вірусів;
- аналіз наявних засобів використання вразливостей;
- аналіз того, наскільки активно використовуються уразливості і наскільки широко поширені віруси;
- взаємодія з постачальниками інформаційних систем з метою більш глибокого аналізу виявлених вразливостей.

На основі проведеного аналізу CERT/CC розробляє заходи щодо усунення вразливостей і рекомендації щодо зменшення негативних наслідків. За результатами цієї роботи всім передплатникам розсилається інформація про загрози інформаційної безпеки та можливі способи їх усунення. Також на основі цих даних формується спеціальна довідкова та технічна документація, проводиться подальша дослідницька та методична робота. Зокрема, CERT/CC підтримує програму безпечної розробки ПЗ («secure coding»), що ґрунтується на тому, що більша частина вразливостей виникає внаслідок відносно невеликого числа помилок у програмному коді інформаційних систем. Таким чином, CERT/CC на основі накопичених результатів аналізу

вразливостей веде цілеспрямовану роботу по виявленню типових програмних помилок, вироблення стандартів безпечного програмування та поширенню цієї інформації серед розробників ПЗ.

Крім основної інформаційної роботи з вразливостями CERT також займається супутніми видами діяльності:

- організація навчальних курсів з різними напрямами (мережева безпека, управління інформаційними ризиками, організація роботи груп реагування);
- сертифікація спеціалістів з реагування на інциденти у сфері інформаційної безпеки;
- підтримка фундаментальних наукових досліджень у різних галузях інформаційної безпеки, таких як методи розробки безпечних додатків, виявлення вразливостей, аналіз шпигунського ПЗ, вирішення питань безпеки як складової частини процесу розробки і т.п.;
- сприяння розвитку локальних (національних і корпоративних) груп реагування на інциденти.

5.3 X-Force security intelligence team – Дослідницька група X-Force

Діяльність цієї групи є одним з напрямків бізнесу компанії Internet Security Systems (ISS) – найбільш авторитетного постачальника комплексних рішень у сфері інформаційної безпеки, клієнтами якого є всі без винятку найбільші компанії США, а також урядові організації. В кінці 2006 року ISS була куплена компанією IBM і інтегрована до неї в якості самостійного підрозділу. Одним із завдань групи X-Force є підтримка в актуальному стані бази даних відомих вразливостей різних програмних і апаратних платформ. База даних, підтримувана цією групою, доступна по мережі Інтернет і постійно поповнюється відомостями про нові вразливості (нині їх налічується понад 40000).

Основні причини, за якими дана організація є провідною у цій галузі, такі:

- велика кількість крупних компаній-клієнтів, від яких постійно надходить інформація про атаки, вразливості і т.п.;
- наявність власної науково-дослідної бази, на основі якої постійно здійснюється виявлення нових вразливостей і узагальнення відомостей про

вразливості, отриманих з різних джерел;

- використання спеціально розроблених універсальних класифікацій (зокрема, загального словника найменувань вразливостей – Common Vulnerabilities and Exposures, CVE) для зберігання і обробки інформації в базах даних відомих вразливостей.

Також одним з напрямків довідково-інформаційної діяльності цієї дослідницької групи є надання послуг по індивідуальному аналізу загроз і інформуванню (X-Force Threat Analysis Service (XFTAS)). Даний комплекс послуг дозволяє замовникам щодня отримувати адаптовану актуальну інформацію про загрози і вразливості з урахуванням особливостей побудови їх інформаційних систем (платформ, додатків, сфери ведення бізнесу, географічного положення) і включає в себе:

- інформацію про загрози;
- експертний аналіз загроз;
- опис поточного і прогнозного стану загроз;
- рекомендовані способи усунення загроз;
- кількісний аналіз атак за останні 30 днів.

Ще одним із завдань групи є випуск періодичних (щоквартальних, щорічних) інформаційних бюлетенів з оглядами найбільш значущих подій у сфері інформаційної безпеки.

5.4 Альянси великих технологічних компаній

Спільні альянси (асоціації, коаліції, групи) великих (іноді середніх) технологічних і консультаційно-дослідницьких компаній являють собою тимчасові (укладаються на короткострокову або середньострокову перспективу) або довгострокові угоди між декількома фірмами, спрямовані на спільне, скоординоване, цілеспрямоване рішення визначених масштабних і ресурсоємних завдань розвитку технології, формування ринкового попиту на певні продукти та організації інфраструктури інформаційної безпеки. Висока значимість такої форми організаційної роботи у сфері інформаційної безпеки, як формування альянсів великими і середніми компаніями, що спеціалізуються на інформаційних технологіях,

обумовлена тим, що:

- такі альянси здатні здійснити найбільш великі інвестиції в розробку нових технологій і проведення досліджень, які можуть вплинути на весь розвиток інформаційних технологій і стан справ у сфері інформаційної безпеки;
- компанії, що входять в такі альянси, займають значну частку ринку і тому визначають загальний напрям розвитку інформаційних технологій взагалі та засобів захисту інформації зокрема;
- такі альянси компаній здатні створити комплексні технології, продукти і рішення, що охоплюють різні аспекти функціонування інформаційних систем і засобів захисту інформації, і таким чином досягти нового рівня захищеності інформації, що практично неможливо при роботі компаній (навіть найбільших) окремо.

Як правило, кожен такий альянс є унікальним, і учасники в кожному конкретному випадку визначають умови роботи в рамках такої організаційної форми. На конкретний підхід до організації альянсу можуть вплинути такі фактори, як:

- характер цілей і завдань, які ставляться перед альянсом;
- поточний стан справ в тій області, для роботи в якій створюється альянс;
- склад учасників альянсу, їх роль і місце на ринку інформаційних технологій;
- наявність можливих конкурентів (наприклад, аналогічних альянсів паралельно створюваних іншими групами компаній);
- раніше сформовані взаємини між компаніями – учасниками альянсу
- та інші.

Завданнями формування альянсів можуть бути:

- розробка нових продуктів і послуг, а також базових технологій, протоколів, алгоритмів і угод, на основі яких такі продукти та послуги в майбутньому могли б розроблятися;
- формування нових ринків збуту та підтримка існуючих;
- вплив на державні та громадські організації, а також на співтовариство користувачів інформаційних систем з метою забезпечення розвитку та більш широкого використання інформаційних технологій і засобів інформаційної

безпеки;

- вплив на систему професійної підготовки фахівців з метою забезпечення якості їх навчання.

Основними типовими прийомами організаційної роботи на такому рівні є:

- скоординований вибір та уніфікація технічних рішень (апаратних пристроїв, програмних алгоритмів), що використовуються в системах передачі та обробки інформації та/або системах захисту інформації;
- інформаційна підтримка як виробників інформаційних систем і постачальників рішень (входять в альянс і не входять до нього), так і споживачів і користувачів (потенційних і справжніх);
- скоординоване розділення функцій по розробці окремих елементів інформаційної технології в рамках спільної узгодженої стратегії розвитку;
- скоординована маркетингова і інформаційна політика, спрямована на забезпечення використання (підтримки, сумісності) створюваних рішень (технологій, протоколів тощо) якомога більшою кількістю споживачів і незалежних виробників, а також її визнання урядовими структурами;
- спільний вплив на органи державної влади (лобіювання) з метою забезпечення державної підтримки певних продуктів, проектів, технологій та архітектур інформаційних систем і систем захисту інформації.

5.5 Smart Card Alliance (SCA) – Альянс за смарт-картками

SCA займається питаннями розвитку технології смарт-карт – однієї з ключових технологій у сфері інформаційної безпеки, використовуваної для ідентифікації користувачів різних сервісів і інформаційних систем (таких як мобільні телефонні мережі, банківські «електронні гаманці» тощо). Цей довгостроковий (стратегічний) альянс був утворений на початку 2001 року шляхом злиття двох організацій: Smart Card Industry Association і Smart Card Forum. До складу альянсу входять близько сотні різних компаній і урядових організацій. При цьому у складі учасників альянсу виділяються кілька груп:

- Керівна Рада (Leadership Council) – провідні компанії, що визначають

основну політику Альянсу: Visa USA, Bank of America, IBM, Lockheed Martin, Intel, Mastercard International і деякі інші (всього більше двадцяти компаній);

- основна група членів Альянсу – різні фірми, так чи інакше пов'язані з питаннями інформаційної безпеки, постачанням відповідних продуктів і послуг (такі як Texas Instruments Incorporated, Sun Microsystems та інші) – всього близько 70 компаній;
- члени – урядові організації. У цю групу входять як федеральні урядові установи США (Державний департамент, Міністерство національної безпеки та інші), так і місцеві органи влади (Портова адміністрація Нью-Йорка, Транспортна адміністрація Вашингтона та інші) – всього близько 30 членів.

Також до складу Альянсу входить один університет і кілька асоційованих членів.

Роботу альянсу очолюють Рада директорів на чолі з головою та Виконавчий директор. Діяльність альянсу розділена на членські ради (Member Council) з окремих сфер інтересів:

- Рада з безконтактних і мобільних платежів;
- Рада з охорони здоров'я (спеціалізується на питаннях використання смарт-карт у сфері охорони здоров'я);
- Рада з ідентифікації;
- Рада з систем контролю за фізичним допуском;
- Рада з транспорту (спеціалізується на питаннях просування та адаптації смарт-карт у транспортній сфері).

Кожна рада керується головою, віце-головами і керуючим комітетом.

Напрямки роботи Альянсу включають в себе:

- організацію спеціалізованих щорічних конференцій;
- організацію освітніх програм і системи сертифікації фахівців;
- видання різних інформаційних та довідкових матеріалів як технічного, так і управлінського характеру;

- ведення централізованої бази даних постачальників обладнання та послуг у сфері смарт-карт.

5.6 Internet Security Alliance (ISA) – Альянс з безпеки мережі Інтернет

ISA був створений в квітні 2001 року з ініціативи двох великих авторитетних організацій: *CERT*/CC Університету Карнегі-Меллон та Асоціації електронної промисловості (Electronic Industries Alliance, EIA). Вже до середини 2004 року в альянс входило близько тридцяти членів, в числі яких такі великі компанії, як Boeing, NEC, Mitsubishi, Federal Express, AIG, Sony, Symantec та інші.

Роботою Альянсу керує Рада директорів, до якої входять авторитетні представники найбільш відомих компаній-членів. Крім того, до складу альянсу входять близько тридцяти асоційованих членів. На початковому етапі створення альянсу його основним завданням було підвищення ефективності обміну інформацією про вразливості, поширюваної *CERT*/CC. Надалі коло завдань альянсу розширювалося, і тепер робота ведеться за наступними напрямками:

- створення ефективних механізмів обміну інформацією про уразливість в мережі Інтернет і знайдених рішеннях проблем безпеки;
- дослідження фундаментальних проблем безпеки;
- розвиток програм професійної підготовки та сертифікації фахівців з інформаційної безпеки;
- взаємодія з державними органами законодавчої і виконавчої влади.

5.7 The International Biometric Industry Association (IBIA) – Міжнародна асоціація компаній-виробників біометричного устаткування

Асоціація була створена в 1998 році з метою колективної підтримки інтересів компаній, пов’язаних з виробництвом біометричного устаткування. Основним завданням альянсу є взаємодія з потенційними замовниками їхньої продукції (як серед комерційних компаній, так і в громадському секторі) з метою просування засобів біометричної ідентифікації. Членами асоціації є близько 30 компаній і організацій, серед яких Hitachi, LG Electronics, Panasonic, NEC та інші.

Управління поточними справами здійснює Рада директорів у складі одинадцяти чоловік, а також виконавчий директор. Діяльність Асоціації розділена на шість робочих груп, серед яких:

- Робоча група зі стандартів та технологій. Її основна мета – захищати базові інтереси членів альянсу у сфері стандартизації біометричних технологій і систем, що використовують біометрію;
- Робоча група зі споживчих додатків. Займається орієнтацією ринку споживчих систем на більш широке використання біометричних технологій;
- Робоча група з міжнародних ринків. Здійснює контакти з іншими біометричними організаціями по всьому світу;
- Робоча група з освіти, маркетингу та інформування. Забезпечує інформаційну присутність компаній-членів асоціації в різних областях через реалізацію маркетингових заходів і освітніх програм;
- Робоча група з глобальної політики. Проводить інформаційну роботу з представниками урядових структур по всьому світу.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ:

1. Які існують альянси великих технологічних компаній, організації, що займаються дослідницькою та інформаційною роботою у сфері інформаційної безпеки.
2. Назвіть основні напрями організаційної роботи в сфері інформаційної безпеки Координаційного центру CERT.
3. Назвіть напрями діяльності Альянсу за смарт-картками.
4. Перерахуйте основні напрями діяльності Альянсу з безпеки мережі Інтернет.