УДК 004.732.056(075.8); 621.391

В.Г. Кононович, канд. техн. наук (ОНАЗ, Україна)

ЕВОЛЮЦІЯ ПАРАДИГМИ ІНФОРМАЦІЙНОЇ, СОЦІАЛЬНО-ПСИХОЛОГІЧНОЇ ТА КІБЕРБЕЗПЕКИ

Розглядається еволюція парадигми інформаційної та кібербезпеки, пояснюються особливості нової соціально центричної парадигми кібербезпеки державного, суспільного та приватного інформаційного виробництва. Пропонується нова система соціально-психологічного захисту інформації, представляються її задачі, політика, засоби та організація.

Темпи розвитку інформаційних технологій дещо знизились, але залишаються високими. Слідом за ними і за новими загрозами стрімко розвиваються системи інформаційної безпеки.

Поняття парадигми розглядають як сукупність цінностей, методів, підходів, технічних навиків і засобів, способів рішення задач, прийнятих в науковому співтоваристві фахівців (інформаційної безпеки) в рамках наукової традиції, що склалася в певний період часу. Парадигма зазнає зміни залежно від накопиченого досвіду і результатів наукових досліджень. Історично парадигми інформаційної безпеки послідовно змінювали одна одну, зберігаючи, доповнюючи і удосконалюючи попередні: класична парадигма захисту інформації, що заснована на контролі доступів; парадигма ешелонованої багаторівневої системи інформаційної безпеки інформаційних ресурсів і технологій (система кругової оборони); мережецентрична парадигма інформаційної безпеки інформаційних ресурсів; парадигма кібербезпеки підприємств, як розвиток мережецентичної парадигми. На черзі знаходиться майбутня розробка нової социальноцентричної парадигми інформаційної безпеки державного, суспільного і приватного інформаційного виробництва.

Класична парадигма захисту інформації, заснована на контролі доступів, була застосована до автоматизованої системи класу 1 - одно - машинного одно - користувацького комплексу, який обробляє інформацію однієї або декількох категорій конфіденційності і прикладом якої служить автономна персональна електронна обчислювальна машина (ПЕОМ). Класична парадигма полягає в забезпеченні збереження заданих властивостей інформації і автоматизованої системи, а саме: конфіденційності і цілісності інформації, доступності ресурсу системи, цілісності і спостережності автоматизованої системи. Концепція захисту передбачала, як головні, задачі обмеження кола користувачів і створення системи розмежування доступу користувачів до інформації за категоріями. Теоретичною базою систем захисту стала теорія гарантовано захищених систем. Захист здійснюється комплексною системою захисту інформації (КСЗІ), яка складається з правового, організаційно-методичного, технічного, програмного, інформаційного і математичного забезпечень, які запобігають реалізаціям загроз або істотно утрудняють реалізацію атак.

Парадигма ешелонованого багаторівневого захисту інформаційних ресурсів розвинулася з розширенням сфери вживання інформаційних технологій, глобальним розповсюдженням Інтернет, активним упровадженням доступу до розподілених баз даних за технологією клієнт - сервер. Характерною особливістю цієї парадигми є перехід від концепцій захисту інформації до концепції інформаційної безпеки технологій і інформаційних ресурсів. Додатково до головної мети системи інформаційної безпеки додається забезпечення стійкого функціонування ІТС, захист законних інтересів підприємств від протиправних посягань, недопущення крадіжки фінансових коштів, підвищення якості наданих послуг і гарантій безпеки майнових прав і інтересів абонентів. Концептуальна технічна модель ешелонованої багаторівневої системи інформаційної безпеки представлена міжнародним стандартом ISO/IEC 15408, який визначає технологію розробки профілів захисту і проектів безпеки. Модель включає набір послуг безпеки (і механізмів безпеки, що реалізовують ці послуги), які забезпечують функції моніторингу, захисту і вживання інформаційних ресурсів з метою поетапного запобігання

можливості проникнення порушником, виявлення факту проникнення, локалізації об'єкту вторгнення і нападу, нейтралізації і видворення порушника, відновлення втрачених функцій системи. Новим в концептуальній моделі є широке вживання фільтрів, міжмережевих екранів, які забезпечують захист периметра.

Мережецентричная парадигма інформаційної безпеки інформаційних ресурсів (сучасна парадигма інформаційної безпеки) витікає з сучасного досвіду і наукових досягнень, з факту бурхливого розвитку ІТС, з розвитку, складності і ролі мереж зв'язку, як критичного державного ресурсу. Ставляться вимоги забезпечення готовності і живучості, що передбачає підтримку таких властивостей як надійність функціонування телекомунікаційної системи, її сталість, доступність інформаційних ресурсів, цілісність та відновлюваність структури системи. Комплексний підхід означає необхідність створення мережної інфраструктури забезпечення інформаційної безпеки, оскільки уразливість якої-небудь ланки мережі може створити проблеми для всіх її учасників, як провайдерів і операторів, так і споживачів послуг. Інформаційна безпека повинна забезпечуватися не тільки від загроз кожному елементу або сервісу, а повинна бути забезпечена у взаємодії засобів і заходів безпеки в мультимедійному середовищі при повній комплексній реалізації безпеки передачі інформації з кінця в кінець.

Складність сучасних ІТС приводить до необхідності і корисності виділення окремо ІТС класу 4, - глобальний розподілений розрахований на багато користувачів, багатодоменний комплекс, який обробляє інформацію різних категорій конфіденційності і різних власників. Домен включає себе ІТС класу 3, яка належить одному власнику і має свою КСЗІ, що захищає домен по периметру, свою систему управління інформаційною безпекою, свою систему попередження, виявлення, обробки і ліквідації інцидентів з інформаційною безпекою, свою єдину для домена політику безпеки.

У ІТС забезпечення інформаційної безпеки переплітається з: управлінням якістю надання послуг зв'язку, де захищеність і готовність інформаційних ресурсів є складовою частиною оцінки якості; управлінням економічною ефективністю, де є взаємозв'язок між інформаційними і економічними ризиками; задачами технічної експлуатації в частині забезпечення вимог до збереження мінімального набору критично важливих функцій, до живучості інформаційних систем, до запасу стійкості при дії чинників зовнішнього середовища, що дестабілізують.

Парадигма кибербезпеки підприємств, як розвиток мережецентричної парадигми

Для підприємств ІТС актуальна концепція кібербезопеки. Кібербезпека – це набір засобів, стратегії, принципи забезпечення безпеки, гарантії безпеки, керівні принципи, підходи до управління ризиками, дії, професійна підготовка, практичний досвід, страхування і технології, які можуть бути застосовані для захисту кіберсередовища, ресурсів організацій і користувача. Ресурси організації або користувача включають приєднані комп'ютерні пристрої, персонал, інфраструктуру, застосування, послуги, системи зв'язку, і всю сукупність переданої и/или збереженої інформації у кіберсередовищі.

Кібербезпека полягає в спробі досягнення і збереження властивостей безпеки ресурсів організації або користувача, направлених проти відповідних загроз безпеки у кіберсередовищі. Загальні задачі забезпечення безпеки включають: доступність; цілісність, яка може включати автентичність і невідмовність; конфіденційність. «Кіберсередовище включає користувачів, мережі, пристрої, все програмне забезпечення, процеси, збережену або транзитну інформацію, додатку, послуги і системи, які можуть бути прямо або опосередковано сполучені з мережами.У сучасному діловому оточенні концепція периметра зникає. Межі між внутрішніми і зовнішніми мережами стають більш розмитими». Безпека забезпечується на всіх рівнях телекомунікаційних мереж, мережі доступу, мережному, транспортному рівнях, рівнях управлінні мережею і надання послуг.

Соціальноцентрична парадигма інформаційної безпеки державного, суспільного і приватного інформаційного виробництва. Перехід людства до інформаційного суспільства закономірно вимагає розробки нової соціальноцентрічної парадигми Розвинене і стабільне інформаційне суспільство характеризується прагненням і можливістю держави створювати

умови для вільного доступу своїх громадян до інформаційних продуктів, товарів і інших ресурсів, і умінням захищати національні інформаційні ресурси, інтереси особи, суспільства і держави в цілому від внутрішнього і зовнішнього негативного впливу. При цьому, у сфері захисту інформаційних ресурсів необхідно забезпечувати надійне, безпечне функціонування національної інформаційної інфраструктури, інформаційного виробництва і їх подальший ефективний розвиток. Цілі і задачі інформаційної безпеки переплітаються з метою і задачами соціально-економічної безпеки і розв'язуються, багато в чому, за допомогою однакових механізмів безпеки. Невід'ємною частиною комплексної безпеки інформаційного суспільства буде і безпека людського капіталу, як частина соціальної та національної безпеки.

Поняття про систему соціального захисту інформації. Законодавством визначені поняття криптографічного та технічного захисту інформації. У їх склад входять у різних пропорціях криптографічні, технічні та організаційні засоби захисту.

З міркувань симетричності, яка є одною із фундаментальних властивостей природи, та почуття естетичності функціональної повноти класів систем захисту інформації, яке по праву вважається критерієм правильності технічних рішень, а також потреб практичної діяльності має бути реалізований клас систем захисту інформації, в якому головну роль, поряд з технічним та криптографічним забезпеченням системи захисту, відігравали б соціально-психологічні організаційні засоби – робота з персоналом, користувачами, кадровим забезпеченням, тобто в якому головна увага приділялась би людському фактору. Є вагомі обґрунтування уведення цього поняття виду захисту – СЗІ. З численних статистичних даних випливає, що до 60% інцидентів з інформаційною безпекою пов’язані з людським фактором. Значний обсяг відкритої та закритої інформації, які підлягають захисту, вимагає застосування автоматизованих систем і засобів захисту. Зростає роль соціальної інформації в підтримці і забезпеченні національної безпеки, що посилює необхідність її захисту.

СЗІ забезпечують проведення організаційно-психологічних заходів для захисту соціальної інформації. Системи СЗІ мають функціонувати на об’єктах інформаційної діяльності органів державного управління та самоврядування, фірмах та підприємствах будь-якої форми власності, суспільних організаціях, об’єднаннях громадян тощо.

Споживачами послуг системи СЗІ є суб’єкти системи національної безпеки, органів державного управління, систем інформаційної безпеки комунікацій (транспорту, енергетичних мереж, паливо-проводів, зв’язку), систем забезпечення життєдіяльності, оборони, надзвичайних ситуацій, правопорядку, промислових об’єктів тощо.

Системи КЗІ, ТЗІ, СЗІ взаємопов’язані одна з одною. Вони можуть бути складовою частиною інших систем безпеки: економічної безпеки, екологічної безпеки, енергетичної, продовольчої безпеки тощо. Політика безпеки соціальної інформації має передбачати наступні задачі захисту: підтримка властивостей цілісності й доступності соціальної інформації; попередження негативних впливів інформації з точки зору інформаційного протиборства; інформаційне забезпечення процесів відтворення соціального капіталу в державі.

Соціальний захист інформації (СЦЗІ) – це вид захисту інформації, спрямований на забезпечення за допомогою організаційних та психологічних заходів, а за необхідності інженерно-технічних та криптографічних засобів, унеможливлення впливу на інформацію, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації. Спосіб реалізації СЦЗІ та його склад потребують подальшого уточнення.

СЦЗІ призначений забезпечити інформаційну безпеку людини, суспільства та держави. Інформаційна безпека суспільства – це стан захищеності інформаційного середовища суспільства, яке забезпечує його формування й усталений розвиток в інтересах громадян та держави. При цьому, під інформаційним середовищем розуміють сукупність інформаційної інфраструктури, інформаційних ресурсів, систему формування, зберігання, розповсюдження, використання й захисту інформації. Загроза інформаційні безпеці – це фактори або їх сукупність, які створюють небезпеку функціонуванню та розвитку інформаційного середовища суспільства, організації, підприємства. Подібно тому, як ТЗІ є необхідним при забезпеченні правил оброблення документів, які містять державну таємницю, так і СЦЗІ є необхідним при

забезпеченні правил обігу й оброблення соціальної й іншої відкритої інформації та організації роботи з персоналом та користувачами.

СЗІ захищає соціальну інформацію при забезпеченні психологічної безпеки еліти, персоналу та населення України. Система СЦЗІ не є ні ідеологічною системою, ні політичним органом. Хоча одним із її побічних призначень є необхідність, хоча би частково, замістити вакуум, який утворився після краху соціалістичної ідеології та радянської політичної системи, у питаннях організаційно-психологічної роботи з персоналом, захисту соціальної інформації і підтримки соціального капіталу суспільства та забезпечення відтворення соціального капіталу в рамках інформаційної безпеки країни та її суб'єктів.

Система СЦЗІ не підміняє собою керування персоналом чи соціальний захист суб'єктів. Соціальний захист населення (СЗН), на відміну від СЦЗІ, – це система заходів й відповідних інститутів, призначених для захисту різних прошарків населення від економічної і соціальної деградації, пов'язаної з безробіттям, втратою або різким скороченням доходу, виробничою травмою або професійним захворюванням, хворобою, інвалідністю, старістю, втратою годувальника, народженням дитини і т. п. Система СЦЗІ відіграє не другорядну роль у веденні інформаційного протиборства і складає його невід'ємну частину. Інформаційне протиборство – це форма боротьби сторін, за якого використовуються спеціальні – політичні, економічні, дипломатичні, військові тощо – методи, способи й засоби для впливу на інформаційне середовище протилежної сторони та захисту власної в інтересах досягнення поставлених цілей.

Інакше кажучи, система СЦЗІ відіграє в інформаційному протиборстві приблизну ту ж роль, що громадянська оборона відіграє у військові сфері. При цьому в СЦЗІ є і самостійна роль – роль фактора забезпечення відтворення соціального капіталу й захисту соціальної інформації за нормального функціонування суспільства.

Інформаційно-психологічний вплив – це є ціле спрямоване виробництво та розповсюдження спеціальної інформації, яка спричиняє безпосередній позитивний чи негативний вплив на соціальний капітал, на функціонування та розвиток інформаційно-психологічного середовища суспільства, психіку та поведінку політичної еліти, персонал економічної й технічної інфраструктури та населення країни.

Завданням і цілями управління СЦЗІ є захист інформаційних ресурсів в інформаційній сфері від несанкціонованого доступу, зокрема, соціальної інформації, та забезпечення розумно достатнього рівня безпеки інформаційно-телекомунікаційних та електронних систем, де вона циркулює. Сфера СЦЗІ нормується державою, підконтрольна державі та суспільству і створюється для забезпечення національної безпеки, усталеного розвитку суспільства і людини в умовах інформаційних воєн та інформаційного впливу. Система СЦЗІ є складовою частиною безпеки національного інформаційного простору, соціального захисту суспільства, і суспільних об'єднань (соціального капіталу) та соціального захисту особи.

У класі СЦЗІ, крім технічних каналів впливу на інформаційні ресурси, розглядаються інформаційно-психологічні канали впливу на суб'єкти інформаційних відносин. Захисту підлягають інформаційний простір держави, інформаційне середовище суспільства та людини, а також інформаційні ресурси.

Засобом ефективності СЦЗІ можуть бути показники якості соціального капіталу та його відтворювання, результати аналізу соціальної інформації. СЦЗІ створюється на всіх рівнях: держави, суспільних організацій та спільнотах, підприємствах, організаціях, фірмах.

Висновки. Система соціального захисту інформації, формально замикає класи захисту інформації в симетричні та функціонально повні відносно розв'язуваних задач, класів систем захисту. Практично СЦЗІ забезпечує виконання завдань захисту соціальної та інших видів відкритої інформації на підприємствах і установах будь-якої форми власності, суспільних організаціях та держави в рамках системи національної безпеки і захисту інформаційного простору України.