УДК 001.89

О.М. Боровська, Є.С. Родін, І.П. Сініцин

ДОСЛІДЖЕННЯ ТА АНАЛІЗ МІЖНАРОДНОГО ТА НАЦІОНАЛЬНОГО ПІДХОДІВ ПОБУДОВИ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В ГРІД

Проаналізовано технічні та організаційні вимоги до ресурсів Українського національного гріду та обґрунтовано нагальну потребу у підтримці цими ресурсами певних напрямків інформаційної безпеки. На основі ретельного аналізу міжнародного досвіду впровадження інтегрованої інформаційної безпеки в грід-сайті та національного підходу до створення систем захисту інформації, з'ясовані певні протиріччя та єдиний можливий шлях до створення комплексної системи захисту інформації в Національній грід-інфраструктурі.

.

Вступ

Український національний грід (УНГ) є спілкою потужних національних наукових кластерів. Завдяки розгортанню проміжного програмного забезпечення (ППЗ), грід сервісів та наявності потужних телекомунікаційних мереж, кластери перетворюються в грід-сайти та створюють єдиний комплекс обчислювальних потужностей, а саме – УНГ. Наукові кластери, як учасники УНГ, передають у спільне користування певну частку своїх ресурсів. Доступ до спільних ресурсів УНГ регламентується та, за умови проходження сертифікації, пропонується членам українських та закордонних наукових організацій і проектів.

На даний час ресурси УНГ використовуються десятками національних та міжнародних проектів. Деякі національні кластери отримали статуси грід-сайтів міжнародного рівня та увійшли в європейську грід спільноту. Величезний обсяг інформації, що обробляється в УНГ, потребує відповідності грід-сайтів УНГ багатьом технічним та організаційним вимогам. Такі вимоги висуваються до:

– апаратних потужностей (для досягнення необхідної швидкості обробки інформації, для збереження великого обсягу інформації);

– програмного забезпечення (для коректної роботи необхідних грід служб і сервісів, що забезпечують взаємодію між сховищами кластерів);

– телекомунікаційних мереж (для досягнення потрібної швидкості передачі даних);

– кваліфікації технічного персоналу;

– регламентних процедур використання ресурсів УНГ.

Одним з головних аспектів, що вносить свої корективи в технічні та організаційні вимоги, є захист інформації. Участь у міжнародних проектах вимагає, з одного боку, відповідності УНГ міжнародним вимогам інформаційної безпеки, а, з іншого боку, УНГ має відповідати національним вимогам з безпеки інформації, що базуються на нормативних документах.

Дана робота покликана поєднати національний та міжнародний досвід у єдину стратегію побудови системи захисту інформації. Використання такої стратегії дозволить УНГ наблизитись до виконання міжнародних та національних вимог до безпеки інформації у гріді.

Характеристика УНГ

УНГ є неоднорідною багатоскладовою інтегрованою інформаційно-телекомунікаційною системою (ІТС). Виходячи з функціонального розподілення, виділяють такі організаційні структурні одиниці УНГ:

– базовий координаційний грід-центр національного рівня – виконує координаційну роботу УНГ на національному рівні, розробляє технічні вимоги функціонування УНГ у цілому та взаємодії його

елементів на національному та міжнародному рівнях, формує та випробовує типові інсталяційні пакети системного, проміжного та прикладного програмного забезпечення для грід-сайтів; забезпечує технічну підтримку функціонування елементів структури УНГ; розробляє та проводить освітні програми для персоналу УНГ; надає власні обчислювальні ресурси зареєстрованим віртуальним організаціям; здійснює центральний моніторинг роботи УНГ;

– регіональні координаційні грід-центри – виконують функції базового координаційного грід-центру на регіональному рівні;

– ресурсні центри національного рівня - надають власні обчислювальні ресурси зареєстрованим віртуальним організаціям; забезпечують сумісність програмного забезпечення грід; забезпечують технічну підтримку користувачів грід; забезпечують інформаційну підтримку користувачів грід і широкого загалу;

– центр сертифікації з регіональними філіями – надає послуги з видачі, підтримки та верифікації сертифікатів користувачів УНГ; надає послуги видачі, підтримки та верифікації сертифікатів вузлів грід-сайта та сервісів грід-сайта в УНГ; забезпечує надійну безвідмовну роботу інформаційної системи; забезпечує дотримання вимог інформаційної безпеки; забезпечує збереження від сторонніх осіб приватної інформації, що надана користувачем під час реєстрації; надає центру сертифікації віртуальних організацій інформацію щодо анульованих та тимчасово припинених сертифікатів користувачів для підтримки актуальності бази користувачів віртуальної організації. Virtual Organization Membership Service (VOMS); створює філії центру сертифікації користувачів національної грід-інфраструктури в регіональних та інших центрах;

– центр сертифікації грід-сайтів – забезпечує перевірку відповідності інфраструктури грід-сайта технічним вимогам УНГ, надає послуги видачі, підтримки та верифікації сертифікатів грід-сайтам;

– центр реєстрації віртуальних організацій – публікує в Інтернеті список зареєстрованих віртуальних організацій УНГ з посиланнями на їх Інтернет-сторінки та правила вступу до них; надає віртуальним організаціям послуги з ведення та підтримки бази користувачів віртуальної організації (VOMS); забезпечує надійну безвідмовну роботу інформаційної системи; забезпечує дотримання вимог інформаційної безпеки;

– центр моніторингу грід-інфраструктури і реєстрації грід-сайтів – відповідає за моніторинг стану елементів УНГ з метою виявлення фактів порушення правил використання ресурсів, загроз безпеки УНГ, аналізу завантаженості елементів УНГ, проводить реєстрацію грід-сайтів, перевірку їх дієвості, вносить відповідні записи до інформаційної системи після успішного тестування грід-сайта;

– центр віртуальних організацій – реєструє віртуальну організацію у центрі реєстрації віртуальних організацій УНГ, визначає адміністратора віртуальної організації; організовує реєстрацію користувачів віртуальної організації з числа зареєстрованих користувачів УНГ у центрі реєстрації віртуальних організацій; забезпечує дотримання правил користування грід і вимог інформаційної безпеки користувачами віртуальної організації; забезпечує сумісність програмного забезпечення грід у рамках віртуальної організації;

– вузли українського національного грід (грід-сайти) – потужні кластери з організаційною структурою персоналу, що отримали сертифікат грід-сайта та надають власні обчислювальні ресурси користувачам віртуальних організацій.

Базовий, регіональні та ресурсні центри національного рівня разом з центром сертифікації, центром реєстрації віртуальних організацій та центром моніторингу грід-інфраструктури і реєстрації грід-сайтів є постійними елементами УНГ.

Центри віртуальних організацій і решта вузлів УНГ можуть бути як постійними, так і тимчасовими складовими УНГ.

Регіональні координаційні центри розміщуються в установах, що розташовані в обласних центрах, мають досить потужний обчислювальний кластер та досвід застосування грід-технологій.

Ресурсні центри національного рівня розгорнуті в Національному технічному університеті України «Київський політехнічний інститут» та в Інституті кібернетики ім. В.М. Глушкова НАН України.

Функції моніторінгу можуть передаватися за домовленістю та за певним розкладом грід-сайтам або іншім структурним одиницям, які мають вільний ресурс. [1].

Всі вищезазначені одиниці організаційної структури УНГ, крім центрів віртуальних організацій та центру сертифікації, у своїй основі мають кластер та, перш за все, представляють собою грід-сайт. Таким чином, грід-сайти є головними складовими технічної структури УНГ.

Отже, технічна структура УНГ – це сукупність грід-сайтів, пов’язаних мережею передачі даних. Саме інформаційна безпека кожного грід-сайта за умови безпеки мережі в сукупності забезпечать захист інформації в УНГ у цілому. Тому в даній роботі пропонується розглянути підходи захисту інформації у грід-сайті.

Характеристика грід-сайта УНГ

Грід-сайт – певна сукупність об’єднаних ресурсів, що надається організацією (власником грід-сайта) для колективного використання. Ресурси грід-сайта включають обчислювальні ресурси, програмне забезпечення, ресурси збереження даних і мережеву інфраструктуру [1].

Технічну основу грід-сайта складає один або декілька кластерів. В УНГ більшість кластерів, на яких базуються всі грід-сайти, побудовані на основі концепції Beowulf , що базується на таких основних положеннях:

1) як сервери для виконання обчислень використовуються сервери зі стандартною архітектурою PC, розподіленою оперативною пам'яттю та зі стандартним мережевим обладнанням;

2) для об'єднання серверів як мережеве обладнання використовуються мережеві технології Gigabit Ethernet та InfiniBand;

3) як програмне забезпечення (операційна система й система керування завданнями) використовується вільно розповсюджуване програмне забезпечення (Linux, Torque) [2].

Інсталяція проміжного програмного забезпечення дозволяє кластеру пропонувати сервіси грід та перетворює кластер на учасника УНГ.

Кластер у ролі грід-сайта складається з таких базових елементів та сервісів:

– обчислювальний елемент Computing Element (CE), що є точкою входу завдань на грід-сайт;

– робочі вузли Working Nodes (WN) – певна кількість серверів (вузлів кластера), що використовуються грід-сайтом для обчислення завдань користувачів;

– елемент збереження даних Storage Element (SE), що є точкою доступу до відкритої для колективного використання в грід частині системи збереження даних;

– інтерфейс користувача User Interface (UI) [3].

Програмне забезпечення грід-сайта складається з:

– програмного забезпечення кластера (вищезгадуваного в складі кластера);

– проміжного програмного забезпечення (gLite або ARC – Advanced Resource Conector), що забезпечує роботу сервісів гріда [4];

– прикладного програмного забезпечення віртуальних організацій.

Структура персоналу грід-сайта виглядає наступним чином (у залежності від розмірів грід-сайта, функції тих чи інших спеціалістів об’єднуються):

1) апарат управління:
   – менеджер грід-сайта;
   – технічний директор;
   – головний адміністратор;
2) операційні адміністратори (або групи адміністраторів):
   – безпеки;
   – програмного забезпечення

проміжного шару;

– операційної системи та загального програмного забезпечення;

– технічного забезпечення;

– WEB інтерфейсу.

Основні функції персоналу грід-сайта:

– реєстрація грід-сайта у центрі сертифікації грід-сайтів;

– підтримка сумісності програмного забезпечення грід-сайта, а саме:

– встановлення системного програмного забезпечення, що запропоноване базовим чи регіональним координаційним центром;

– встановлення прикладного програмного забезпечення, що необхідне в роботі користувачам віртуальних організацій;

– забезпечення надійної та безвідмовної роботи обчислювальних кластерів та сховища даних;

– забезпечення та дотримання умов інформаційної безпеки.

Отже, з огляду на вищезазначене, грід-сайт складається з кластера, до якого входить:

– технічне забезпечення (обчислювальні потужності, сховища даних, мережа);– програмне забезпечення (операційна система, система керування завданнями, прикладне програмне забезпечення);

– проміжне програмне забезпечення, що перетворює кластер на грід-сайт;

– персонал.

Кожна з зазначених складових грід-сайта підтримує певні напрямки інформаційної безпеки (рис.1).

На рівні кластера побудова СЗІ складається з:

– планування архітектури мережі, виділення демілітаризованих зон, побудови фізичних та віртуальних мереж для розподілення трафіка за функціональними та конфіденційними ознаками;

– налаштування міжмережевих екранів відповідно до правил відкритості портів протоколів передачі даних;

– встановлення режимів доступу до обчислювальних ресурсів грід-сайта користувачів різних рівнів;

– вибору технічного та програмного забезпечення із захисту: вибір мережевого обладнання, програмного забезпечення моніторингу та виявлення атак [5].

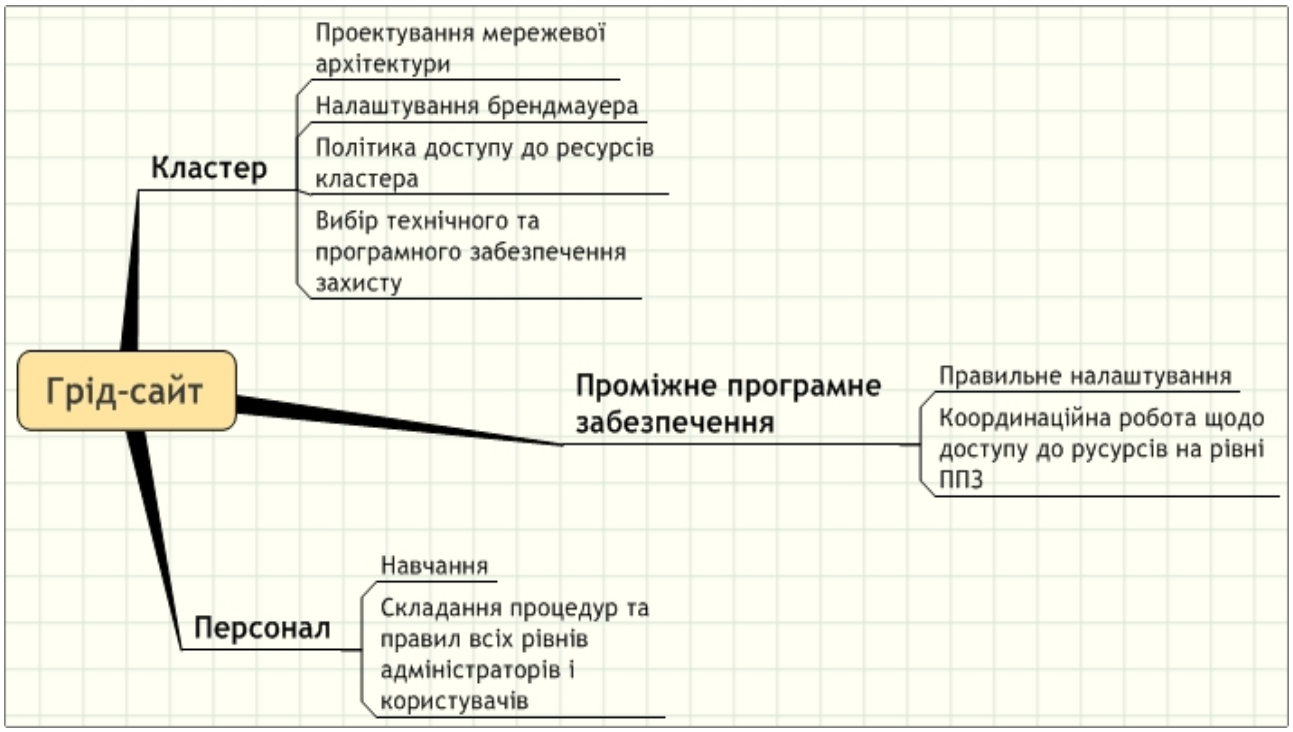

Рис. 1. Розподіл складових елементів грід-сайта за напрямками організації інформаційної безпеки

На рівні проміжного програмного забезпечення персонал кластера має коректно ввести в дію конфігураційні налаштування з безпеки, модулі, що відповідають за автентифікацію користувачів, моніторинг.

У свою чергу, персонал віртуальної організації повинен в тісній кооперації з адміністраторами грід-сайта визначити ролі для своїх членів таким чином, щоб права доступу кожній ролі члена віртуальної організації можна було співвіднести визначені права доступу на рівні кластера.

На рівні персоналу необхідно:

– визначити вимоги до кваліфікації персоналу;

– розробити правила та процедури поведінки користувачів всіх рівнів;

– проводити навчання персоналу та користувачів.

З точки зору характеру заходів СЗІ грід-сайта їх можна поділити на такі рівні:

1) технічний захист;

2) організаційний захист.

Технічний захист передбачає розробку вимог, планування та виконання заходів на рівні технічного, програмного, мережевого забезпечення.

Організаційний захист включає планування та проведення заходів навчання персоналу, розробку процедур та правил роботи персоналу і користувачів.

Вищезазначені напрямки інформаційної безпеки на сьогоднішній день певною мірою втілюються в життя в грід-сайтах УНГ. Розглянемо далі саме міжнародний та національний підходи до планування та втілення СЗІ.

Міжнародний досвід побудови системи захисту інформації у грід-сайті

Під час існування проекту Enabling Grids for E-sciencE (EGEE) Європейською Комісією заснований проект Інтегрованої системи безпеки грід-сайта Integrated Site Security for Grids (ISSeG). Головна мета проекту, який тривав 26 місяців, це систематизація досвіду з безпеки грід-сайтів та представлення його у формі методологій, рекомендацій, інструментів, тренінгів. Результати роботи проекту були викладені на окремому WEB-сайті http://isseg-training.web.cern.ch.

Група спеціалістів, яка сьогодні займається інформаційною безпекою у проекті EGI, будує свою роботу на досвіді проекту ISSeG. Згідно концепції ISSeG, захист грід-сайтів є запорукою захисту всієї грід-інфраструктури (рис. 2).

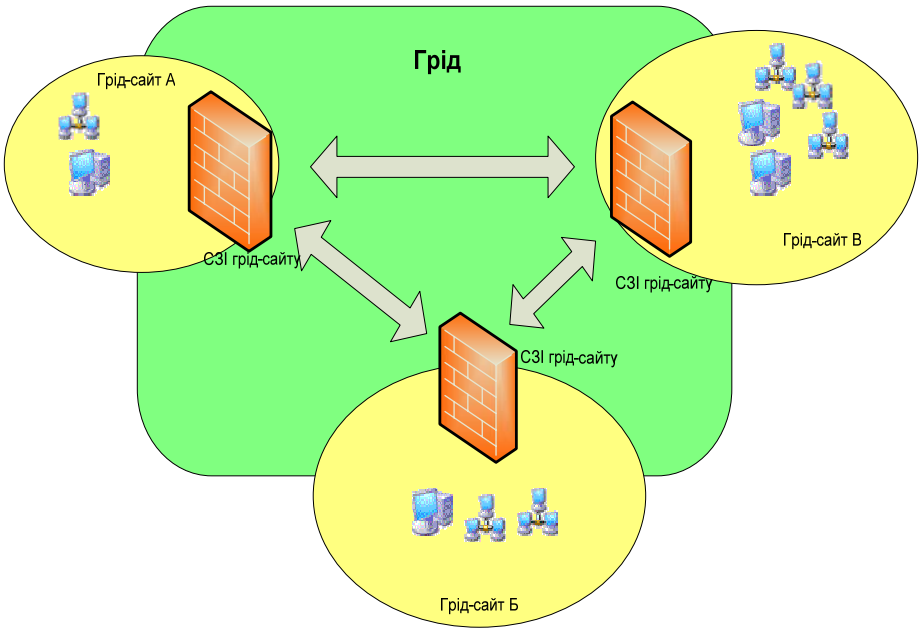

Рис. 2. Концепція ISSeG захисту грід-інфраструктури

В основі інтегрованої системи безпеки грід-сайта (рис. 3) покладені [9] принципи побудови стратегії інформаційної безпеки як безперервного процесу дій у наступних напрямках:

– технічний;

– адміністративний;

– освітній.

Безумовно, ці напрямки перетинаються та створюють інтегровану систему захисту. Будь-який захід технічного напрямку має супроводжуватися відповідними заходами адміністративного та освітнього напрямків. Так, наприклад, перетин адміністративного та технічного аспекту полягає у тому, що робота адміністратора має включати ретельний аналіз технічних та програмних заходів щодо автентифікації користувачів. Адміністратор має знати та правильно використовувати існуючі бібліотеки проміжного програмного забезпечення.

Про зміни в налаштуваннях адміністратор має попередити користувачів та, за потребою, провести пояснювальні заняття. Отже, маємо перетин технічного, адміністративного та освітнього напрямків.

Технічний напрямок інтегрованої системи безпеки має регулювати такі процеси:

– контроль доступу до технічних засобів (ТЗ); централізоване керування конфігурацією (patch management);

– керування антивірусним захистом;

– керування розповсюдженням програмного забезпечення ПЗ;

– керування конфігурацією;

– керування мережевими комунікаціями;

– керування мережевими екранами;

– встановлення систем моніторингумережевих атак (intrusion detecting system);

– керування системою автентифікацій, авторизації;

– керування резервним копіюванням. Адміністративний напрямок інтегрованої системи безпеки регулює процеси:

– оцінки роботи існуючої або створення нової СЗІ, а саме: визначення загроз, оцінка ризику за загрозами;

– оцінки роботи (або створення нової) команди реагування на інциденти, розробка плану дій роботи команди;

– розробки політики безпеки; підтримки циклічного процесу безпеки: захистити-розпізнати-відреагувати;

– інвентаризації програмного та технічного забезпечення;

– регулювання політики використання головних операційних процедур.

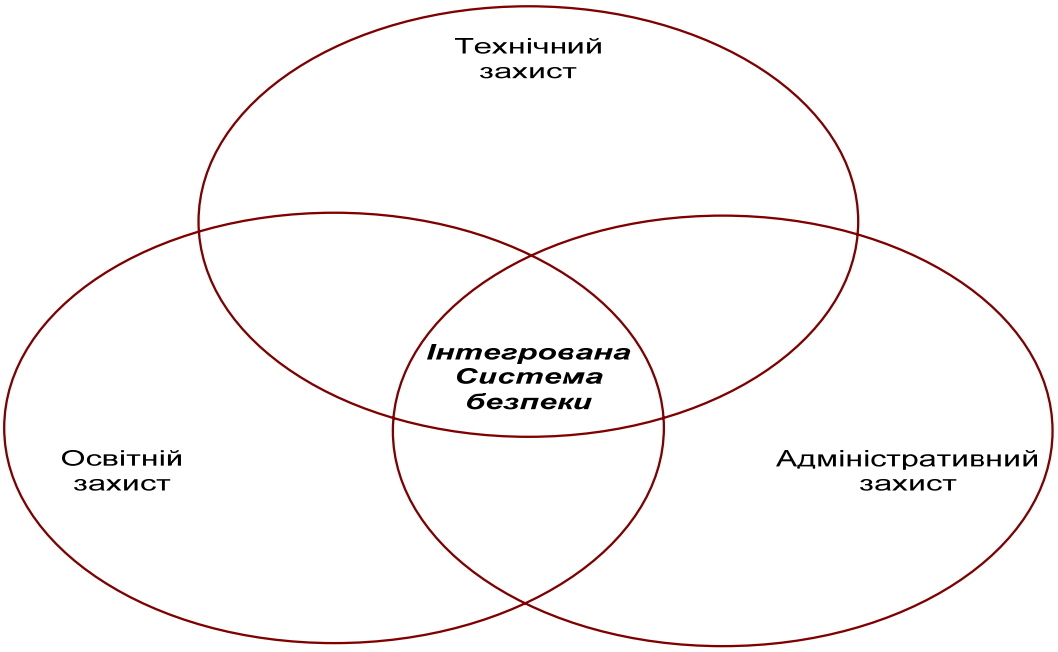

Рис. 3. Інтегрована система безпеки грід-сайта

Освітні аспекти інтегрованої системи безпеки повинні регулювати процеси розробки та проведення тренінгів безпеки для користувачів, адміністраторів та розробників.

Як вже зазначалося, робота в перелічених напрямках побудови інтегрованої системи безпеки грід-сайта полягає у циклічному виконані послідовних процесів: ідентифікація, аналіз, імплементація, моніторинг (рис. 4). Перший етап – «Ідентифікація ресурсів». Передбачає визначення, класифікацію ресурсів, які підлягають захисту за ступенем важливості. Результатом цього етапу є структурований перелік ресурсів.

Другий етап – «Аналіз загроз та ризиків». Визначає ступінь захищеності грід-сайта, визначає загрози та рівень ризику загроз. Результатом етапу є визначений список загроз, поділений за ступенем ризику.

Виконання першого і другого етапу супроводжується використанням інструменту запитальника. Методологія полягає у вже запропонованому переліку загроз, притаманних грід-сайтам. Кожна загроза описується певною кількістю запитань. Відповіді на ці запитання мають чисельне значення, певний коефіцієнт.

Сума показників відповідей на запитання, що описують певну загрозу, є показник ризику за даною загрозою. ISSeG пропонує діапазон показників для надання рекомендацій чи варто звертати увагу на дану загрозу, чи реагувати негайно. Третій етап – «Імплементація заходів, спланованих за результатами аналізу, проведеному на етапі 2». Передбачає створення плану заходів мінімізації ступеня ризику, оцінку цих заходів, вибір найефективніших заходів та введення їх у дію. Виконання третього етапу супроводжується використанням переліку з 62 рекомендацій. Кожна з цих рекомендацій посилається на одне або декілька запитань з запитальника, кожна рекомендація відповідає на запитання: «що треба зробити?», «чому саме такий захід?», «як саме втілити захід (перелік конкретних дій)?», «на які загрози впливає втілення рекомендації"?». Рекомендація має свою категорію з трьох: технічна, адміністративна, освітня.

Також рекомендації щодо конкретних дій розділені за групами відповідно наступним ролям учасників у роботі грід-сайта: користувач, системний адміністратор,розробник, менеджер. Кожна з рекомендацій має посилання на інші залежні від неї рекомендації.

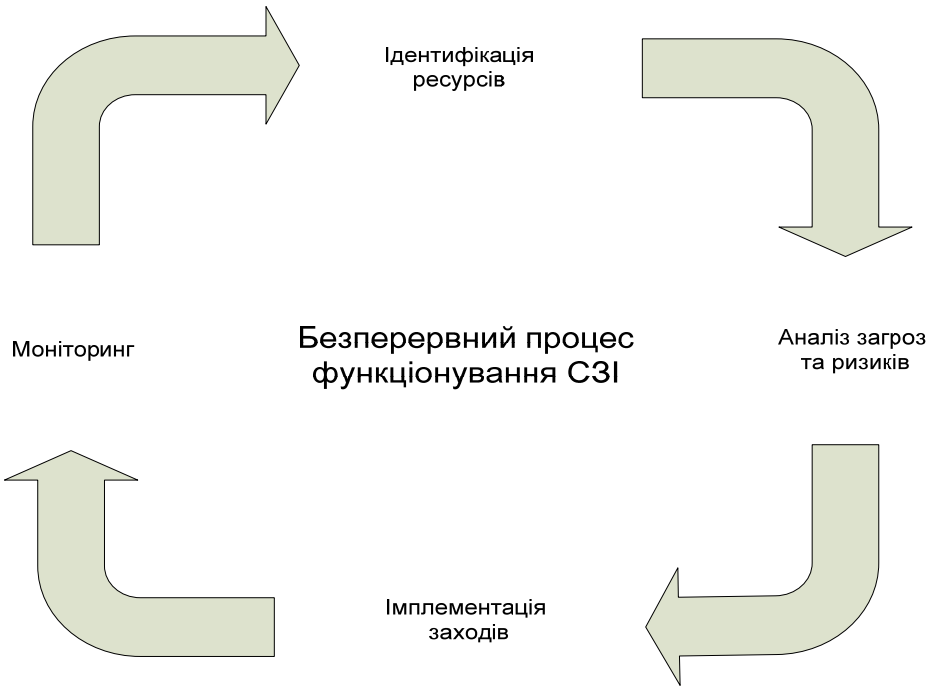

Рис. 4. Циклічність впровадження інтегрованої системи безпеки грід-сайта

Четвертий етап – «Моніторинг та перегляд виконання планових заходів з захисту». Передбачає ведення статистики подій, оцінку ефективності прийнятих заходів та внесення відповідних змін у план заходів захисту. Головною рекомендацію втілення в дію цього етапу є налагодження системи реагування на інциденти, ретельний запис та опис інцидентів, розгортання системи запису активності користувачів, періодичний перегляд вже втілених у дію заходів з безпеки, та оцінка їх ефективності за допомогою запитальника.

Слід зазначити, що досвід проекту ISSeG базується на становленні та розвитку існуючих грід-сайтів, тому перелік запитань запитальника відповідає саме специфіці грід-інфраструктури. Кожна загроза, яка розкривається запитальником, наділена списком конкретних рекомендацій щодо її усунення. Загальна ж методологія послідовності та циклічності дій по забезпеченню інформаційної безпеки схожі з загально прийнятими стандартами безпеки ІТС.

Національний підхід до створення системи захисту інформації у грід-сайті

Чому саме захист інформації в УНГ має враховувати державну нормативну базу?

Серед інших видів інформації, що циркулюватиме в УНГ, присутня інформація, яка є власністю держави, та інформація, вимога щодо захисту якої встановлена законом, і яка підлягає захисту згідно нормативно-законодавчих документів [6].

Побудова системи захисту інформації, що є власністю держави, регулюється такими основними нормативними документами, що в свою чергу мають посилання на інші необхідні нормативи:

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».

2. Закон України «Про захист персональних даних».

3. Постанова Кабінету Міністрів України від 29 березня 2006 р. № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах».

4. Указ Президента України «Про Положення про технічний захист інформації в Україні».

5. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі НД ТЗІ 3.7-003-05.

6. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу НД ТЗІ 2.5-00.4-99.

Згідно нормативних документів, побудова СЗІ передбачає комплексний підхід, тому й система захисту інформації називається комплексною – КСЗІ. Такий підхід базується на принципі захисту периметрів всіх рівнів функціонування грід-сайта, включаючи різні середовища функціонування. Побудова КСЗІ має охоплювати весь комплекс можливих чинників безпеки інформації: зовнішнє середовище, будівлі, персонал, технічне та програмне забезпечення, комплекс всіх можливих загроз на всіх рівнях, моделі порушників, оцінка ризиків за всіма загрозами, відповідні заходи з безпеки, фінансові складові захисту [7].

Життєвий цикл створення та супроводження КСЗІ має більш лінійний характер подій. Важливим етапом створення КСЗІ є отримання позитивного результату державної експертизи створеної КСЗІ – Атестату відповідності. Слід зазначити, що етапи створення КСЗІ чітко визначені у доступній формі і передбачають сувору послідовність та ретельну документованість.

Для того, щоб модернізувати КСЗІ, в багатьох випадках необхідно пройти аналогічні етапи, що й при створенні нової системи захисту. Нажаль, у такий спосіб даний підхід зменшує мотивацію до по-

кращення існуючої КСЗІ. Також нормативні документи передбачають деякі відмінності та відповідні рекомендації при створенні КСЗІ в існуючій інформаційно-телекомунікаційній системі (ІТС), та в такій, що тільки планується до розробки.

Переглянемо основні етапи створення КСЗІ.

1. Формування загальних вимог до КСЗІ в ІТС за допомогою обстеження середовищ функціонування ІТС спрямовано на доведенні (чи спростуванні) необхідності створення КСЗІ.

Результатами даного етапу мають стати:

– документи із загального обстеження системи;

– визначення наявності у складі ІТС інформації, що підлягає автоматизованій обробці, таких її видів, що потребують обмеження доступу до неї, або забезпечення цілісності чи доступності відповідно до вимог нормативно-правових актів;

– документи аналізу ризиків (вивчення моделі загроз і моделі порушника, можливих наслідків від реалізації потенційних загроз, величини можливих збитків, перелік суттєвих загроз);

– оцінка можливих переваг (фінансово-економічних, соціальних тощо) експлуатації ІТС у разі створення КСЗІ.

2. Розробка політики безпеки інформації в ІТС.

Цей етап передбачає більш детальне вивчення об’єкта, на якому створюється КСЗІ, уточнюються моделі загроз, потенційного порушника та результати аналізу можливості керування ризиками. Також готуються альтернативні варіанти створення КСЗІ і планів їх реалізації з вибором основних рішень з протидії всім суттєвим загрозам, здійснюється оцінка переваг і недоліків кожного варіанта, вибір найбільш оптимального варіанта. Такий варіант оформлюється як документ з політики безпеки, що за своїм змістом є планом захисту.

3. Розробка технічного завдання (ТЗ) на створення КСЗІ.

Цей етап передбачає створення документу (ТЗ), який чітко формалізує вимоги до КСЗІ, порядок створення КСЗІ, порядок проведення всіх видів випробувань КСЗІ та введення її в експлуатацію у складі ІТС.

4. Розробка проекту КСЗІ.

На даному етапі на базі ТЗ, політики безпеки, опису ІТС формуються та описуються конкретні технічні, програмні, організаційні рішення (та організаційно-технічні заходи реалізації цих рішень), впровадження яких задовольняє вимогам інформаційної безпеки, визначених в ТЗ. Результатом даного етапу є технороботчий проект створення КСЗІ.

5. Введення КСЗІ в дію та оцінка захищеності інформації в ІТС.

Цей етап передбачає, по-перше, низку підготовчих заходів до введення КСЗІ в експлуатацію, а саме, за необхідністю, будівельно-монтажні роботи, комплектування та встановлення технічних та програмних засобів, навчання персоналу. Важливим кроком є випробування всіх компонентів КСЗІ, їх дослідна експлуатація, оцінка захищеності ІТС та проведення державної експертизи.

6. Етап супроводження КСЗІ передбачає роботи з організаційного забезпечення функціонування КСЗІ та керування засобами захисту інформації відповідно до плану (політики) захисту та експлуатаційної документації на компоненти КСЗІ [5].

Чіткий план дій створення КСЗІ із зазначеними необхідними результатами кожного етапу є суттєвою допомогою при створенні КСЗІ, проте, з практичної точки зору, нормативні документи не покликані й не дають інструментарію виконання завдань розробки КСЗІ, наприклад, таких як методологія оцінки варіантів системи захисту та визначення найкращого, методологія визначення списку найвагоміших загроз, методологія оцінки ефективності керування ризиками інформаційної безпеки. Крім того, нормативні документи, що регулюють створення КСЗІ, не мають серед своїх визначень та термінів таких, що ха-

рактеризують саме грід-сайт та визначають його особливості при побудові КСЗІ. Для відпрацювання зазначених питань необхідно використання проаналізованого вище міжнародного досвіду побудови системи захисту інформації у грід-сайті.

Висновки

Загальний висновок за двома підходами можна визначити так: основні етапи побудови СЗІ схожі в обох випадках, проте, якщо міжнародна методологія носить рекомендаційний характер, то національні вимоги – обов'язкові до виконання.

Міжнародний досвід дає більш практичні поради та інструменти при побудові СЗІ саме в грід-сайті, натомість, серед вітчизняних нормативів ще не існує таких рекомендацій, оскільки технологія грід є новою для нашої держави.

Також обидва підходи передбачають:

– комплексний (інтегрований) підхід до побудови СЗІ;

– однакову послідовність головних етапів створення СЗІ: обстеження середовищ, визначення ресурсів, визначення загроз і відповідно ризиків, оцінка варіантів захисту, планування, введення в дію, підтримка та моніторинг;

– необхідність створення документації (обстеження, політики безпеки, плану дій, моделі загроз, настанов, інструкцій, журналів реєстрації подій);

– захист апаратних та програмних ресурсів крім інформаційних ресурсів.

Здійснювати обробку інформації, якою володіє держава, згідно національним вимогам, можна тільки при отриманні Атестату відповідності, виданого за результатами державної експертизи, яка здійснює оцінку відповідності КСЗІ вимогам нормативних документів із захисту інформації; у випадку міжнародних рекомендацій аналіз якості захисту виконується власником грід-сайта.

Щодо модернізації СЗІ, то міжнародний досвід наполягає на постійному циклічному перегляді засобів захисту, в той час як при проведенні модернізації згідно українського законодавства, необхідно знову проводити державну експертизу, що демотивує власників ресурсів покращувати старі та вводити нові засоби захисту.

Єдиним шляхом розв'язання зазначеного протиріччя, на наш погляд, є створення такої СЗІ українського грід-сайта, яка б враховувала рекомендації міжнародного досвіду та, з іншого боку, не йшла в розріз з державними нормативними документами.

Саме такий підхід має бути використано при створенні комплексної системи захисту інформації в Національній грід-інфраструктурі [7].

1. *Свістунов С.Я.* Пропозиції щодо Положень про структурні складові УНГ та регламентацію їх взаємодії і про загальні грід-сервіси: матеріали конференції УНГ-2010. Інститут теоретичної фізики ім. М.М. Боголюбова НАН України, 1 – 2 листопада 2010 р.
2. *Бойко Ю.В., Зинов'єв М.Г., Свістунов С.Я., Судаков О.О.* Український академічний грід: досвід створення і перші результати експлуатації // Математичні машини і системи. – 2008. – № 1. – С. 67 – 84.
3. *GLITE* 3.1 User guide. EGEE-II Collaboration, 2006. http://www.eu-egee.org.
4. *The* NorduGrid/ ARC User Guide. "The NorduGrid Collaboration," http://www.nordugrid.org.
5. *The* NorduGrid/ ARC Information System. Technical Description and Reference Manual. NorduGrid project. http://www.nordugrid.org.
6. *Постанова* Кабінету Міністрів України від 29 березня 2006 р. № 373 "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах". Документ 373-2006-п, редакція від 01.01.2007 на підставі 1700-2006-п. http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=373-2006-%EF.
7. *Підходи* до створення комплексної системи захисту інформації в Національній грід-інфраструктурі / Боровська О.М., Родін Є.С., Свістунов С.Я., Сініцин І.П., Шилін В.П. – (Препринт / Інститут теоретичної фізики НАН України ім. Боголюбова М.М.; Київ, 2010-12). http:

//grid.nas.gov.ua/index.php?option=com_content&view=frontpage&Itemid=72
8. *Порядок* проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі НД ТЗІ 3.7-003-05. Державна служба спеціального зв'язку та захисту інформації України. http://dstszi.kmu.gov.ua.
9. *Integrated Site Security for Grids*. ISSeG Collaboration 2008. http: // isseg-training.web.cern.ch/ISSeG-training/.

Отримано 10.09.2011

Про авторів:

Боровська Олена Миколаївна,
головний програміст,

Родін Євген Сергійович,
аспірант,

Сініцин Ігор Петрович,
доктор технічних наук.

Місце роботи авторів:

Інститут програмних систем
НАН України,
03187, Київ-187,
проспект Академіка Глушкова, 40.
Тел.: (044) 526 1444
e-mail: e.borovskaya@ekotex.ua