МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Київський національний університет будівництва і архітектури

Ю.І. Хлапонін

КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Конспект лекцій
для студентів спеціальності
125 «Кібербезпека»

Київ 2022

УДК 004.056(075.8)
Х-55

Рецензенти: В.О. Темніков, д-р. техн. наук, професор;
А.М. Котенко, канд. техн. наук, доцент

Затверджено на засіданні кафедри кібербезпеки та комп'ютерної інженерії протокол № 9 від 03 травня 2022 р.

Хлапонін Ю.І.

Х-55 Комплексні системи захисту інформації: конспект лекцій / Ю.І. Хлапонін. - Київ: КНУБА, 2022. – 84 с.

Розглянуто основні питання, що належать до галузі інформаційної безпеки; висвітлені основи організації захисту інформації, методи оцінювання захищеності та основні положення побудови комплексних систем захисту інформації.

Призначено для студентів спеціальності 125 «Кібербезпека».

УДК 004.056(075.8)

ЗМІСТ

ВСТУП

Науково-технічна революція останнім часом прийняла грандіозні масштаби в сфері інформатизації суспільства на базі сучасних засобів обчислювальної техніки, зв'язку, а також сучасних методів автоматизованої обробки інформації. Застосування цих засобів і методів прийняло загальний характер, а створювані при цьому інформаційно-обчислювальні системи і мережі стають глобальними як в сенсі територіального розподілення, так і в сенсі широти охоплення в рамках єдиних технологій процесів збирання, передачі, накопичення, зберігання, пошуку, переробки інформації і видачі її для використання. Іншими словами, людство почало реалізацію завдання створення і використання цілої індустрії переробки інформації.

У сучасному світі інформаційний ресурс став одним з найбільш потужних важелів економічного розвитку. Володіння інформацією необхідної якості в потрібний час і в потрібному місці є запорукою успіху в будь-якій сфері господарської діяльності. Монопольне володіння певною інформацією виявляється найчастіше вирішальною перевагою в конкурентній боротьбі і зумовлює, тим самим, високу ціну «інформаційного чинника».

Широке впровадження персональних ЕОМ вивело рівень «інформатизації» ділового життя на якісно новий щабель. Нині важко уявити собі фірму або підприємство (навіть найдрібніші), що не були б озброєні сучасними засобами обробки і передачі інформації. У ЕОМ на носіях даних накопичуються значні обсяги інформації, яка часто має конфіденційний характер або становить велику цінність для її власника. В даний час характерними і типовими стають такі особливості використання обчислювальної техніки:

- зростаюча питома вага автоматизованих процедур в загальному обсязі процесів обробки даних;
- наростаюча важливість і відповідальність рішень, прийнятих в автоматизованому режимі і на основі автоматизованої обробки інформації;
- збільшення концентрації в автоматизованих системах (АС) обробки даних інформаційно-обчислювальних ресурсів;
- велике територіальне розподілення компонентів АС;
- ускладнення режимів функціонування технічних засобів АС;
- накопичення на технічних носіях величезних обсягів інформації, причому для багатьох видів інформації стає все більш важким (і навіть неможливим) виготовлення немашинних аналогів (дублікатів).
- інтеграція в єдиних базах даних інформації різного призначення і різної належності;

- довготривале зберігання великих масивів інформації на машинних носіях;
- безпосередній і одночасний доступ до ресурсів (в тому числі і до інформації) АС великого числа користувачів різних категорій та різних установ;
- інтенсивна циркуляція інформації між компонентами АС, у тому числі і розташованих на великих відстанях один від одного;
- зростаюча вартість ресурсів АС.

Проте створення індустрії переробки інформації, даючи об'єктивні передумови для грандіозного підвищення ефективності життєдіяльності людства, породжує цілий ряд складних і великомасштабних проблем. Однією з таких проблем є надійне забезпечення збереження встановленого статусу використання інформації, що циркулює і обробляється в інформаційно-обчислювальних установках, центрах, системах і мережах, або коротко – в автоматизованих системах обробки даних. Дана проблема увійшла в побут під назвою проблеми захисту інформації або забезпечення безпеки інформації.

Означення 1. Інформаційною безпекою називають заходи захисту інформації від несанкціонованого доступу, руйнування, модифікації, розкриття і затримок у доступі.

Інформаційна безпека містить в собі заходи захисту процесів створення даних, їх введення, обробки і виведення. Метою інформаційної безпеки є убезпечення цінності системи, захист і гарантування точності та цілісності інформації, мінімізація руйнування, що може мати місце, якщо інформація буде модифікована або зруйнована. Інформаційна безпека вимагає врахування всіх подій, в ході яких інформація створюється, модифікується, до неї забезпечується доступ або вона поширюється.

Інформаційна безпека дає гарантію того, що досягаються такі цілі:

- конфіденційність критичної інформації;
- цілісність інформації та пов'язаних з нею процесів (створення, введення, обробки і виведення);
- доступність інформації, коли вона потрібна;
- облік всіх процесів, пов'язаних з інформацією.

У 60-х і частково в 70-х роках XX ст. проблема захисту інформації вирішувалася досить ефективно застосуванням, в основному, організаційних заходів. До них належали передусім, режимні заходи, охорона, сигналізація і найпростіші програмні засоби захисту інформації. Ефективність використання зазначених заходів досягалася за рахунок концентрації інформації на

обчислювальних центрах, як правило, автономних, що сприяло забезпеченню захисту відносно малими засобами.

«Розподілення» інформації за місцями її зберігання і обробки, чому значною мірою сприяла поява у величезних кількостях дешевих персональних комп'ютерів і побудованих на їх основі локальних і глобальних національних і транснаціональних мереж ЕОМ, що використовують супутникові канали зв'язку, створення високоефективних систем розвідки і здобування інформації загострило ситуацію з захистом інформації.

Проблема забезпечення необхідного рівня захисту інформації виявилася (і це предметно підтверджено як теоретичними дослідженнями, так і досвідом практичного вирішення) досить складною, що вимагає для свого вирішення не просто здійснення деякої сукупності наукових, науково-технічних і організаційних заходів та застосування специфічних засобів і методів, а створення цілісної системи організаційних заходів та застосування специфічних засобів і методів захисту інформації.

Координація робіт стосовно захисту інформації в державному масштабі традиційно здійснювалася і здійснюється Адміністрацією Держспецзв’язку України, яка створювалася як головна організація з протидії іноземним технічним розвідкам. У зв'язку з викладеними вище об'єктивними причинами до теперішнього часу відбулося переосмислення функцій Адміністрації Держспецзв’язку України.

Роботи з захисту інформації у нас у країні ведуться досить інтенсивно і вже тривалий час. Накопичено певний досвід. Його аналіз показав, що весь період робіт із захисту інформації в АС досить чітко ділиться на три етапи, кожен з яких характеризується своїми особливостями в принципових підходах до захисту інформації.

Перший етап характеризувався спрощеним підходом до самої проблеми, породженим переконанням, що вже сам факт подання інформації в ЕОМ у закодованому вигляді та обробки її за специфічними алгоритмами є серйозним захисним засобом, а тому цілком достатньо ввести до складу АС деякі технічні і програмні засоби та здійснити ряд організаційних заходів, і цього буде достатньо для забезпечення захисту інформації. Надії ці не виправдалися, фахівці дійшли висновку, що для захисту інформації потрібна деяка цілком організована система зі своїм керівним елементом. Такий елемент отримав назву ядра захисту або ядра безпеки. Проте все ще зберігалася надія, що система захисту з ядром надалі буде забезпечувати надійний захист протягом всього часу функціонування АС, хоча істотно підвищилася увага до організаційних заходів.

Викладений підхід був характерним і для другого етапу. Однак порушення безпеки інформації неухильно зростали, що викликало серйозну стурбованість, оскільки могло стати серйозною завадою на шляху впровадження обчислювальної техніки. Посилені пошуки виходу з такої майже кризової ситуації привели до висновку, що захист інформації в сучасних АС не є одноразова акція, а безперервний процес, цілеспрямовано здійснюваний протягом всього часу створення і функціонування систем з комплексним застосуванням всіх наявних засобів, методів і заходів. Формування цього висновку і знаменувало початок третього етапу розвитку підходів до захисту інформації, який здійснюється і на даний час. Так у найзагальніших рисах може бути охарактеризована суть зарубіжного та вітчизняного досвіду захисту інформації в АС.

На основі сказаного, теоретичних досліджень і практичних робіт в галузі захисту інформації сформульований так званий системно-концептуальний підхід до захисту інформації в АСОД.

Під системністю як складовою частиною системно-концептуального підходу розуміються нижченаведені положення.

По-перше, системність цільова, тобто захищеність інформації розглядається як складова частина загального поняття якості інформації.

По-друге, системність просторова, передбачає взаємопов'язані рішення всіх питань захисту в усіх компонентах окремо взятої АС, у всіх АС установи (закладу, відомства), розташованих на певній території.

По-третє, системність тимчасова, що означає безперервність робіт із захисту інформації, здійснюваних за взаємопов'язаним планом.

По-четверте, системність організаційна, що означає єдність організації всіх робіт із захисту інформації та управління їх здійсненням. Вона зумовлює об'єктивну необхідність створення в загальнодержавному масштабі чіткої системи органів, професійно орієнтованих на захист інформації, несе повну відповідальність за оптимальну організацію надійного захисту інформації в усіх АС і має для цього необхідні повноваження. Головною метою зазначеної системи органів має бути реалізація у загальнодержавному масштабі принципів системно-концептуального підходу до захисту інформації як державного, так і комерційного характеру.

Концептуальність підходу передбачає розробку єдиної концепції як повної сукупності науково обґрунтованих поглядів, положень і рішень, необхідних і достатніх для оптимальної організації та забезпечення надійності захисту інформації, а також для цілеспрямованої організації всіх робіт із захисту

інформації. Розробка такої концепції в даний час знаходиться на стадії завершення а її зміст охоплює всі напрями забезпечення надійного захисту інформації.

Враховуючи різноманіття потенційних загроз інформації в АС, складність їх структури і функцій, а також участь людини в технологічному процесі обробки інформації, цілі захисту інформації можуть бути досягнуті тільки шляхом створення системи захисту інформації на основі комплексного підходу.

Комплексна система захисту інформації (КСЗІ) є сукупністю методів і засобів, об'єднаних єдиним цільовим призначенням, які забезпечують необхідну ефективність захисту інформації в АС. Комплексність системи захисту інформації досягається охопленням всіх можливих загроз і узгодженням між собою різнорідних методів і засобів, що забезпечують захист всіх елементів АС [1].

ЛЕКЦІЯ №1. НД ТЗІ 3.7-003-2005 «ПОРЯДОК ПРОВЕДЕННЯ РОБІТ ІЗ СТВОРЕННЯ КСЗІ В ІТС»

НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення КСЗІ в ІТС» визначає 6 етапів створення КСЗІ та її документації:

1. Формування вимог до КСЗІ в ІТС

1.1. Обґрунтування необхідності створення КСЗІ і призначення СЗІ:

- наказ про порядок проведення робіт зі створення КСЗІ
- наказ про створення СЗІ
- положення про СЗІ
- перелік інформації, що підлягає обробленню в ІТС та потребує захисту

1.2. Категоріювання ІТС:

- наказ про призначення комісії з категоріювання
- акт категоріювання

1.3. Обстеження середовищ функціонування ІТС:

- наказ про призначення комісії з обстеження
- акт обстеження
- формуляр ІТС

1.4. Опис моделі порушника політики безпеки інформації: модель порушника

1.5. Опис моделі загроз для інформації: модель загроз

1.6. Формування завдання на створення КСЗІ: звіт за результатами проведення аналізу ризиків та формування завдань на створення КСЗІ

2. Розробка політики безпеки інформації в ІТС

2.1. Вибір варіанту КСЗІ

2.2. Складання політики безпеки

2.3. Складання плану захисту

2.4. Складання календарного плану робіт із захисту інформації

3. Розробка Технічного завдання на створення КСЗІ:

- складання технічного завдання та погодження його з органами Держспецзв'язку

4. Розробка проекту КСЗІ:

- складання документів ескізного проекту КСЗІ
- складання документів технічного проекту КСЗІ
- складання документів робочого проекту КСЗІ

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

5.1. Підготовка КСЗІ до введення в дію:

- інструкція про порядок введення в експлуатацію КСЗІ

5.2. Навчання користувачів:

- інструкція адміністратора безпеки в ІТС
- інструкція системного адміністратора ІТС
- інструкція користувача ІТС
- правила управління паролями в ІТС
- правила видачі, вилучення та обміну персональних ідентифікаторів, інших атрибутів розмежування доступу в ІТС

5.3. Комплектування КСЗІ

5.4. Будівельно-монтажні роботи:

- наказ про призначення комісії з приймання робіт
- акт приймання робіт

5.5. Пусконалагоджувальні роботи:

- акт інсталяції та налагоджування АВПЗ і КЗЗ від НСД
- акт завершення пусконалагоджувальних робіт

5.6. Попередні випробування КСЗІ:

- наказ про створення комісії з проведення випробувань
- програма та методика попередніх випробувань
- протокол про проведення попередніх випробувань
- акт завершення попередніх випробувань

5.7. Дослідна експлуатація КСЗІ:

- наказ про введення ІТС в дослідну експлуатацію
- акт завершення дослідної експлуатації
- акт завершення робіт зі створення КСЗІ

5.8. Державна експертиза КСЗІ:

- заявка на проведення державної експертиза КСЗІ
- експертний висновок щодо відповідності КСЗІ вимогам НД ТЗІ
- атестат відповідності КСЗІ вимогам НД ТЗІ
- наказ про дозвіл на обробку в ІТС інформації, яка підлягає захисту

6. Супровід КСЗІ:

- наказ про порядок забезпечення захисту інформації в ІТС
- інструкція щодо забезпечення правил обробки ІзОД в ІТС
- інструкція з антивірусного захисту інформації в ІТС
- інструкція про порядок використання засобів КЗІ в ІТС
- інструкція про порядок обліку та використання машинних носіїв інформації
- інструкція з правил управління паролями в ІТС

- інструкція про порядок створення і зберігання резервних копій інформаційних ресурсів ІТС
- інструкція про порядок проведення контролю режиму обробки та захисту інформації в ІТС
- інструкція про порядок супроводу та модернізації КСЗІ в ІТС
- інструкція про порядок відновлювальних та ремонтних робіт ІТС
- інші інструкції.

Формування вимог до КСЗІ в ІТС

Після прийняття рішення про необхідність створення КСЗІ відповідальний за ТЗІ організації-власника (розпорядника) ІТС готує для керівника організації 3 накази:

1) про створення **Служби захисту інформації в ІТС** (далі - СЗІ), порядок створення, завдання, функції, структура та повноваження якої визначено в НД 1.4-001-2000 «Типове положення про СЗІ в АС»;

2) про призначення **комісії з категоріювання ІТС**, завдання та повноваження якої визначено в НД ТЗІ 1.6-005-2013 «Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці»;

3) про призначення **комісії з обстеження середовищ функціонування ІТС**, завдання та повноваження якої визначено в ДСТУ 3396.1-96 «Технічний захист інформації. Порядок проведення робіт».

Після призначення СЗІ складає «**Положення про СЗІ в ІТС**», що має бути оформлене у вигляді окремого документа згідно рекомендацій НД ТЗІ 1.4-001-2000 та затверджене керівником організації-власника (розпорядника) ІТС.

Положення повинно складатись з таких розділів:

- загальні положення;
- завдання СЗІ;
- функції СЗІ;
- повноваження та відповідальність СЗІ;
- взаємодія СЗІ з іншими підрозділами організації та зовнішніми підприємствами, установами, організаціями;
- штатний розклад та структура СЗІ;
- організація та фінансування робіт СЗІ.

Категоріювання ІТС

Комісія з категоріювання визначає ступень обмеження доступу до інформації, яка оброблятиметься в ІТС, та з урахуванням цього ступеня

встановлює категорію ІТС. Встановлена категорія зазначається в Акті категоріювання ІТС, який складається комісією за результатами її роботи. Акт категоріювання є чинним протягом 5 років з моменту проведення категоріювання, якщо не змінилась ознака, за якою була встановлена категорія об'єкта.

В акті зазначається:

1. Підстава для категоріювання (рішення про створення КСЗІ, закінчення терміну дії акта категоріювання, зміна ознаки, за якою була встановлена категорія, та реквізити наказу про призначення комісії з категоріювання.

2. Вид категоріювання: первинне, чергове, позачергове (у разі чергового або позачергового категоріювання вказується категорія, що була встановлена до цього категоріювання, та реквізити акту, яким було встановлено цю категорію).

3. В ІТС здійснюється обробка ІзОД.

4. Ступінь обмеження доступу до ІзОД, що обробляється в ІТС (передбачена законом таємниця; службова інформація; конфіденційна інформація, яка перебуває у володінні розпорядників інформації, інша конфіденційна інформація, вимога щодо захисту якої встановлена законом).

5. Встановлена комісією категорія.

Обстеження середовищ функціонування ІТС

За результатами обстеження інформаційного середовища складається «**Перелік інформації, що підлягає автоматизованому обробленню в ІТС і потребує захисту**», який оформлюється як окремий документ, затверджений керівником організації-власника (розпорядника) відповідної інформації, або як розділ у інших документах (Політика безпеки, План захисту, Технічне завдання на створення КСЗІ тощо).

У переліку має бути наведено перелік інформаційних ресурсів (видів інформації), що підлягають обробленню в ІТС, класифікований за такими ознаками:

- назва відповідного інформаційного ресурсу, який визначається цільовим призначенням відповідної інформації;
- характеристики інформації відповідно до встановленого законодавством правового режиму та режиму доступу (ІДТ, КІВД, КІ, ВІВД, ВІ);
- вищий ступінь обмеження доступу (для ІДТ) до інформації (ступінь секретності) відповідно до вимог Зводу відомостей, що становлять державну таємницю;
- критичні властивості інформації з погляду забезпечення її захищеності, визначені з урахуванням вимог Правил 373 і вимог власника (розпорядника)

інформації;

- вимоги (за наявності) щодо обмеження доступу до інформації користувачів ІТС різних категорій, визначені з урахуванням, наприклад, вимог «Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в АС» або «Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію».

За результатами обстеження середовищ функціонування ІТС складається «**Формуляр ІТС**», який оформлюється як окремий документ і складається з таких розділів:

- загальні відомості про ІТС;
- склад технічних засобів ІТС;
- склад програмного забезпечення;
- відомості про програмно-апаратний КЗЗ від НСД;
- відомості про впровадження, випробування та приймання в експлуатацію;
- посадові особи, відповідальні за технічне обслуговування;
- посадові особи, відповідальні за забезпечення захисту інформації;
- реєстрація проведених робіт (технічне обслуговування, ремонт, модернізація тощо);
- відмітки про проведення перевірок КСЗІ;
- перелік технічних та експлуатаційних документів КСЗІ.

У разі обробки в ІТС таємної інформації здійснюється також обстеження фізичного середовища, під час якого аналізується взаємне розміщення засобів обробки інформації ІТС на ОІД, комунікацій, систем життєзабезпечення і зв'язку, а також режим функціонування цих об'єктів.

Порядок проведення обстеження повинен відповідати ДСТУ 3396.1-96 «Технічний захист інформації. Порядок проведення робіт», а в частині, що стосується захисту інформації від витоку технічними каналами, - НД ТЗІ 3.1-001-07 «Створення комплексу технічного захисту інформації. Передпроектні роботи».

За результатами комісія складає «**Акт обстеження середовищ функціонування ІТС**», який затверджується керівником організації-власника (розпорядника) ІТС і складається з таких розділів:

- клас і склад обчислювальної системи,
- перелік і характеристики інформаційних ресурсів,
- перелік і повноваження користувачів,

- опис фізичного середовища (до акту додаються генеральний і ситуаційний плани, схеми систем життєзабезпечення та заземлення).

Останній крок 1-го етапу складається з таких робіт:

1. Формування завдання на створення КСЗІ в ІТС.
2. Аналіз ризиків реалізації загроз для інформації в ІТС.
3. Вибір варіанту побудови та складу КСЗІ в ІТС.
4. Оформлення звіту за результатами проведеної роботи.

Етап завершується оформленням «**Звіту за результатами проведення аналізу ризиків та формування завдань на створення КСЗІ**», який затверджується керівником організації-власника (розпорядника) ІТС.

Звіт повинен містити 2 розділи:

- формалізований або неформалізований опис результатів аналізу ризиків, пов'язаних з реалізацією загроз для інформації в ІТС;
- формулювання, з урахуванням результатів виконаного аналізу ризиків, завдань на створення КСЗІ в ІТС.

Забезпечення послуг безпеки (функцій захищеності)

З точки зору забезпечення безпеки інформації ІТС або КЗЗ можна розглядати як набір функціональних послуг. Кожна послуга являє собою набір функцій, що дозволяють протистояти деякій множині загроз.

Існує певний перелік послуг, які на підставі практичного досвіду визнані «корисними» для забезпечення безпеки інформації. Вимоги до реалізації даних послуг наведені в **НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в КС від НСД»**.

Кожна послуга може включати декілька рівнів. Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз. Рівні послуг мають ієрархію за повнотою захисту, проте не обов'язково являють собою точну підмножину один одного. Рівні починаються з першого (1) і зростають до значення *n*, де *n* - унікальне для кожного виду послуг.

Функціональні послуги розбиті на 4 групи, кожна з яких описує вимоги до послуг, що забезпечують захист від загроз одного із 4-х основних типів: конфіденційність (К), цілісність (Ц), доступність (Д) і спостережність (Н).

1. **Реалізація послуг конфіденційності** дозволяє забезпечити захист інформації від несанкціонованого ознайомлення з нею (компрометації). Конфіденційність забезпечується такими послугами: довірча конфіденційність, адміністративна конфіденційність, повторне використання об'єктів, аналіз прихованих каналів, конфіденційність при обміні. Принципи, що лежать в основі реалізації послуг, визначаються політикою конфіденційності.

2. **Реалізація послуг цілісності** дозволяє забезпечити захист інформації від несанкціонованої модифікації (включаючи її знищення). Цілісність забезпечується такими послугами: довірча цілісність, адміністративна цілісність, відкат, цілісність при обміні. Принципи, що лежать в основі реалізації послуг, визначаються політикою цілісності.

3. **Реалізація послуг доступності** забезпечується в ІТС такими послугами: використання ресурсів, стійкість до відмов, гаряча заміна, відновлення після збоїв.

4. **Реалізація послуг спостережності** забезпечується в ІТС такими послугами: реєстрація (аудит), ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність КЗЗ, самотестування, ідентифікація і автентифікація при обміні, автентифікація відправника, автентифікація отримувача.

Всі послуги є більш-менш незалежними. Якщо ж така залежність виникає, тобто реалізація якої-небудь послуги неможлива без реалізації іншої, то цей факт відбивається як необхідні умови для даної послуги (або її рівня). За винятком послуги «аналіз прихованих каналів» залежність між функціональними послугами безпеки та гарантіями відсутня.

В межах кожного класу ІТС класифікуються на підставі вимог до забезпечення певних властивостей інформації.

З точки зору безпеки інформація характеризується трьома властивостями: конфіденційністю, цілісністю і доступністю. Виходячи з цього, кожний клас ІТС (х = 1, 2, 3) поділяється на підкласи, які визначають підвищені вимоги до забезпечення:

- конфіденційності оброблюваної інформації (підклас «х. К»);
- цілісності оброблюваної інформації (підклас «х.Ц»);
- доступності оброблюваної інформації (підклас «х.Д»);
- конфіденційності і цілісності оброблюваної інформації (підклас «х.КЦ»);
- конфіденційності і доступності оброблюваної інформації (підклас «х.КД»);
- цілісності і доступності оброблюваної інформації (підклас «х.ЦД»).
- конфіденційності, цілісності і доступності оброблюваної інформації (підклас «х.КЦД»).

НД ТЗІ 2.5-005-99 «Класифікація ІТС і стандартні функціональні профілі захищеності оброблюваної інформації від НСД» вводить таке поняття як «стандартний функціональний профіль захищеності» (далі - СФПЗ). Він являє собою перелік мінімально необхідних рівнів послуг, які повинен реалізовувати

КЗЗ обчислювальної системи ІТС, щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється в даній ІТС.

Для кожного з підкласів кожного класу вводиться деяка кількість ієрархічних стандартних функціональних профілів, яка може бути різною для кожного класу і підкласу ІТС. Профілі є ієрархічними в тому розумінні, що їх реалізація забезпечує наростаючу захищеність від загроз відповідного типу (К, Ц і Д). Зростання ступеня захищеності може досягатись як підсиленням певних послуг, тобто включенням до профілю більш високого рівня послуги, так і включенням до профілю нових послуг.

Згідно НД ТЗІ 2.5-005-99 кожний профіль має свій буквено-числовий ідентифікатор, який включає:

- номер класу ІТС (1 - ПЕОМ, 2 - ЛОМ, 3 - РОМ),
- букви, що характеризує види загроз, від яких забезпечується захист (К, Ц, Д),
- номер профілю.

Всі частини ідентифікатора відділяються один від одного крапкою.

Наприклад, СФПЗ ІТС класу «2» номер 1 з підвищеними вимогами до забезпечення конфіденційності інформації виглядає таким чином:

2.К.1 = {КД-2, НР-2, НИ-2, НК-1, НО-1, НЦ-1}

А СФПЗ ІТС класу «1» номер 2 з підвищеними вимогами до забезпечення конфіденційності, цілісності і доступності інформації виглядає таким чином:

1.КЦД.2 = {КА-1, КО-1, ЦА-1, ЦО-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1}

Версія може служити, зокрема, для вказівки на підсилення певної послуги всередині профілю. Наприклад, нарощування можливостей реєстрації приведе до появи нової версії. Тим не менше, при внесенні деяких істотних змін, особливо додання нових послуг, може або привести до появи нового профілю, або до того, що профіль буде відноситись до іншого класу чи підкласу ІТС.

Контрольні питання:

1. Яку послідовність та назву мають етапи створення КСЗІ?
2. Що повинно бути визначено наказами керівника установи?
3. Які акти складаються під час першого етапу створення КСЗІ?
4. Які заходи здійснюються на першому етапі створення КСЗІ?
5. Які складові ІТС підлягають обстеженню?
6. У якому разі здійснюється обстеження фізичного середовища ІТС?
7. Який документ першого етапу є підсумковим?
8. Які є види функціональних послуг безпеки?
9. Які є послуги конфіденційності?
10. Які є послуги цілісності?
11. Які є послуги доступності?
12. Які є послуги спостережності?
13. На підставі чого класи ІТС поділяються на підкласи?
14. Запишіть умовні назви підкласів ІТС з підвищеними вимогами до забезпечення цілісності та доступності інформації.
15. Запишіть умовну назву СФПЗ ІТС класу «1» номер 3 з підвищеними вимогами до забезпечення конфіденційності та цілісності інформації.

ЛЕКЦІЯ № 2-3. РОЗРОБКА ПОЛІТИКИ БЕЗПЕКИ ІНФОРМАЦІЇ В ІТС

Опис політики безпеки інформації в ІТС здійснюється згідно вимог додатку «**Методичні вказівки щодо структури та змісту Плану захисту інформації в АС**» до НД ТЗІ 1.4-001-2000 «**Типове положення про СЗІ в АС**», затверджується керівником організації-власника (розпорядника) ІТС, та вноситься, за необхідності, до відповідних розділів Плану захисту та Технічного завдання на створення КСЗІ.

Виходячи з міжнародного досвіду та вимог міжнародних стандартів в області інформаційної безпеки розрізняють 3 типи політики безпеки.

1. Програмна політики безпеки є політикою вищої ланки управління в організації. Об'єктом є організація в цілому, за розробку і здійснення програмної політики несе відповідальність керівництво організації. Програмна політика визначає стратегічні напрямки забезпечення інформаційної безпеки.

2. Системно - орієнтована політика – це структура, склад, вимоги до окремих компонентів, процедур і функцій ІТС, етапу документування, які визначені вітчизняними нормативними документами.

3. Проблемно - орієнтована політика спрямована на вирішення окремих проблем або завдань в області забезпечення інформаційної безпеки. Існує ряд областей діяльності організації, для яких необхідно розробити окремі політики: фізичної безпеки, керування доступом, адміністрування, криптозахисту, антивірусного захисту, інтернет-доступу тощо.

Політика безпеки повинна містити набір вимог, правил, обмежень, рекомендацій тощо, які регламентують порядок оброблення в ІТС інформації, зазначеної у «Переліку інформації, що підлягає автоматизованому обробленню в ІТС і потребує захисту», та спрямовані на захист її критичних властивостей від загроз, притаманних умовам функціонування конкретної ІТС.

Політика (з урахуванням результатів обстеження середовищ функціонування ІТС) визначає інформаційні ресурси ІТС, що потребують захисту. Мають бути сформульовані основні загрози для інформації з різними характеристиками відповідно до встановленого законодавством правового режиму та режиму доступу, компонентів обчислювальної системи, персоналу та вимоги щодо захисту від цих загроз.

Перераховуються основні рішення з протидії всім суттєвим загрозам, правила, які регламентують використання захищених технологій обробки інформації в ІТС, окремих заходів і засобів захисту інформації, діяльність користувачів всіх категорій.

Як складові частини загальної політики повинні бути наведені політики забезпечення конфіденційності, цілісності та доступності оброблюваної інформації, а також політика забезпечення спостережності та керованості ІТС.

Під час розробки політики повинні бути враховані технологія обробки інформації, моделі порушників і загроз, особливості ОС, фізичного середовища та інші чинники. Як складові частини загальної політики мають існувати політики забезпечення конфіденційності, цілісності, доступності оброблюваної інформації та спостережності ІТС.

Політика має бути розроблена таким чином, що б вона не потребувала частої модифікації (потреба частої зміни вказує на надмірну конкретизацію, наприклад, не завжди доцільно вказувати конкретну назву чи версію програмного продукту).

Політика повинна стосуватись:

- інформації (рівня критичності ресурсів ІТС),
- взаємодії об'єктів (правил, відповідальності за захист інформації, гарантій захисту),
- області застосування (яких складових компонентів ІТС політика безпеки стосується, а яких - ні).

Політика повинна передбачати використання всіх заходів захисту інформації:

- правові та морально-етичні норми,
- організаційні (адміністративні),
- фізичні, технічні (апаратні і програмні) заходи,
- правила та порядок застосування в ІТС кожного заходу.

Політика безпеки повинна базуватися на наступних основних принципах:

- системності;
- комплексності;
- неперервності захисту;
- достатності механізмів і заходів захисту та їхньої адекватності загрозам;
- гнучкості керування системою захисту, простоти і зручності її використання;
- відкритості алгоритмів і механізмів захисту, якщо інше не передбачено окремо.

Політика безпеки повинна поширюватись на такі об'єкти захисту:

- відомості (незалежно від виду їхнього представлення), віднесені до інформації з обмеженим доступом (ІзОД) або інших видів інформації, що підлягають захисту, обробка яких здійснюється в ІТС і які можуть знаходитись на паперових, магнітних, оптичних та інших носіях;

- інформаційні масиви та бази даних, програмне забезпечення, інші інформаційні ресурси;

- обладнання ІТС та інші матеріальні ресурси, включаючи технічні засоби та системи, не задіяні в обробці ІзОД, але знаходяться у контрольованій зоні, носії інформації, процеси і технології її обробки. Технічні області, в яких необхідно захищати інформаційне та програмне забезпечення - робоча станція, комунікаційні канали (фізична мережа) та комутаційне обладнання, сервери, засоби друку та буферизації для утворення твердих копій, накопичувачі інформації;

- засоби та системи фізичної охорони матеріальних та інформаційних ресурсів, організаційні заходи захисту;

- користувачів (персонал) АС, власників інформації та АС, а також їхні права.

Політика повинна визначити вимоги до заходів, методів та засобів захисту, вихідними даними для чого є:

- завдання і функції ІТС;

- результати аналізу середовищ функціонування ІТС;

- модель загроз і модель порушників;

- результати аналізу ризиків.

На підставі цих даних визначаються компоненти ІТС (наприклад, окрема ЛОМ, спеціалізований АРМ, Інтернет-вузол тощо), для яких необхідно або доцільно розробляти свої власні політики безпеки, відмінні від загальної політики безпеки в ІТС.

Для кожного компонента та (або) ІТС в цілому формується перелік необхідних функціональних послуг захисту від НСД та вимог до рівнів реалізації кожної з них, визначається рівень гарантій реалізації послуг (згідно з НД ТЗІ 2.5-004-99 і 2.5-005-99). Визначені вимоги будуть складати ФПЗ ІТС або її компоненти.

Для кожного компонента та (або) ІТС в цілому у разі обробки таємної інформації визначаються загальні підходи та вимоги з захисту інформації від витоку технічними каналами.

На наступному кроці визначаються механізми безпеки, що реалізують функціональні послуги безпеки, здійснюється вибір технічних засобів захисту інформації від витоку технічними каналами.

Політика повинна доказово давати гарантії того, що:

- в ІТС забезпечується адекватність рівня захисту інформації рівню її критичності;

- реалізація заходів захисту інформації є рентабельною;

- в будь-якому середовищі функціонування ІТС забезпечується оцінюваність і перевіряємість захищеності інформації;

- забезпечується персоніфікація положень політики безпеки (стосовно суб'єктів ІТС), звітність (реєстрація, аудит) для всіх критичних з точки зору безпеки ресурсів, до яких здійснюється доступ в процесі функціонування ІТС;

- персонал і користувачі забезпечені достатньо повним комплектом документації стосовно порядку забезпечення захисту інформації;

- всі критичні з точки зору безпеки інформації технології (функції) ІТС мають відповідні плани забезпечення неперервної роботи та її поновлення у разі виникнення непередбачених ситуацій;

- враховані вимоги всіх документів, які регламентують порядок захисту інформації в ІТС, та забезпечується їхнє суворе дотримання.

Документальне оформлення політики безпеки

Результати робіт з розроблення політики безпеки оформлюються у вигляді окремих документів або розділів одного документа, в якому викладена політика безпеки інформації в ІТС. Структурно до політики безпеки (документів, що її складають) повинні входити такі розділи:

- загальний, у якому визначається відношення керівництва ІТС до проблеми безпеки інформації;

- організаційний, у якому наводиться перелік підрозділів, робочих груп, посадових осіб, які відповідають за роботи у сфері захисту інформації, їхніх функції, викладаються підходи, що застосовуються до персоналу (опис посад з точки зору безпеки інформації, організація навчання та перепідготовки персоналу, порядок реагування на порушення режиму безпеки тощо);

- класифікаційний, де визначаються матеріальні та інформаційні ресурси, які є у наявності в ІТС, та необхідний рівень їхнього захисту;

- розділ, у якому визначаються правила розмежування доступу користувачів та процесів до інформаційних ресурсів ІТС (далі - ПРД);

- розділ, у якому визначається підхід щодо керування робочими станціями, серверами, мережевим обладнанням тощо;

- розділ, у якому висвітлюються питання фізичного захисту;

- розділ, де викладено порядок розробки та супроводження ІТС, модернізації апаратного та програмного забезпечення;

- розділ, який регламентує порядок проведення відновлювальних робіт і забезпечення неперервного функціонування ІТС;

- юридичний розділ, у якому приводиться підтвердження відповідності

політики безпеки законодавству України.

Матеріальні та інформаційні ресурси, які є у наявності в ІТС, та необхідний рівень їхнього захисту

У класифікаційному розділі на основі інвентаризації усіх компонентів ІТС, що беруть участь у технологічному процесі обробки інформації, приводиться опис активних і пасивних компонентів ІТС. Інвентаризації (ідентифікації) підлягають:

- організаційно-топологічна структура ІТС, для якої створюється КСЗІ;
- склад і призначення функціональних підсистем ІТС;
- склад служб і протоколів, що реалізують інформаційний обмін між елементами (компонентами) ІТС;
- об'єкти захисту (види і категорії оброблюваної інформації, апаратно-програмні й інформаційні ресурси на відповідних рівнях ієрархічної структури ІТС);
- персонал і користувачі ІТС.

При описі компонентів системи рекомендується скласти структурну схему інформаційних потоків між основними компонентами ІТС, а також описати технологію обробки інформації. При виборі й аналізі об'єктів ІТС важливим моментом є ступінь деталізації розглянутих об'єктів.

Так, для АС-1 (окрема ПЕОМ) припустимо розглядати всю інфраструктуру, тоді як для ІТС 3-го класу (глобальна мережа) всеосяжна оцінка може зажадати неприйнятних витрат часу і сил. У цьому випадку рекомендується зосередитися на описі найбільш важливих компонентів ІТС.

Приводиться перелік інформаційних потоків, що циркулюють між компонентами ІТС. У залежності від класу ІТС структурна схема інформаційних потоків між основними компонентами ІТС може включати:

- внутрішні потоки обміну між активними і пасивними об'єктами усередині однієї ПЕОМ;
- локальні потоки обміну між робочими станціями і серверами усередині однієї ЛОМ (домена);
- міжмережеві потоки обміну між ЛОМ (доменами), що входять до складу однієї ІТС;
- потоки обміну інформацією з вилученими взаємодіючими об'єктами, що не входять до складу ІТС.

У цьому ж розділі можна вказати необхідні завдання захисту інформації, об'єкти захисту та обраний варіант побудови КСЗІ. З урахуванням класу ІТС для кожного компонента і ІТС в цілому перелічуються функціональні послуги

безпеки і вимоги до рівнів реалізації кожної з них, рівень гарантій реалізації послуг. У разі обробки в ІТС таємної інформації для кожного компонента і ІТС в цілому визначаються загальні підходи та рішення щодо захисту інформації від витоку технічними каналами.

Найважливішу частину політики безпеки складають правила розмежування доступу користувачів та процесів до інформаційних ресурсів ІТС (далі - ПРД), що є певним абстрактним механізмом, який виступає посередником при будь-яких взаємодіях об'єктів ІТС.

З урахуванням того, що в ІТС визначено такі ієрархічні ролі як адміністратор безпеки, адміністратор і користувач, загальні ПРД можуть бути такими:

- кожне АРМ повинно мати свого адміністратора, який несе відповідальність за його працездатність та за дотримання всіх вимог і процедур, пов'язаних з обробкою інформації та її захистом. Таку роль може виконувати уповноважений користувач. Цей користувач повинен бути забезпечений відповідними інструкціями і навчений всім вимогам і процедурам;

- для попередження неавторизованого доступу до даних, ПЗ, інших ресурсів ІТС, керування механізмами захисту здійснюється адміністратором безпеки ІТС;

- для попередження поширення комп'ютерних вірусів відповідальність за дотримання правил використання ПЗ несуть: на АРМ - користувачі, адміністратор, в ІТС - адміністратор безпеки. Використовуватись повинно тільки ПЗ, яке дозволено політикою безпеки (ліцензійне, яке має відповідні сертифікати, експертні висновки тощо);

- за всі зміни ПЗ, створення резервних і архівних копій несе відповідальність адміністратор безпеки АС. Такі роботи виконуються за його дозволом;

- кожний користувач має свій унікальний ідентифікатор і пароль. Право видачі цих атрибутів надається адміністратору. Атрибути для адміністраторів надає адміністратор безпеки ІТС. Видача атрибутів дозволяється тільки після документальної реєстрації особи як користувача. Користувачам забороняється спільне використання персональних атрибутів;

- користувачі проходять процедуру автентифікації для отримання доступу до ресурсів ІТС;

- атрибути користувачів періодично змінюються, а ті, що скомпрометовані або не використовуються, видаляються;

- процедури використання активного мережевого обладнання, а також окремих видів ПЗ, яке може суттєво впливати на безпеку (аналізатори трафіку, аналізатори безпеки мереж, засоби адміністрування тощо), авторизовані і

здійснюються під контролем адміністратора безпеки ІТС;

- усі користувачі повинні знати «Інструкцію користувача» (пройти відповідний курс навчання та скласти іспит);

- адміністратор безпеки ІТС і адміністратори повсякденно здійснюють перевірку працездатності засобів захисту інформації, ведуть облік критичних з точки зору безпеки подій і готують звіти щодо цього.

Загальні ПРД мають бути конкретизовані на рівні вибору необхідних функціональних послуг захисту (профілю захищеності) та впровадження організаційних заходів захисту інформації.

Правила розмежування доступу користувачів та процесів до інформаційних ресурсів ІТС (ПРД)

У розділі «ПРД» приводяться обраний метод керування доступом (довірче і адміністративне керування), вимоги до забезпечення безперервності захисту, до набору атрибутів доступу і правилам їхнього використання (присвоєння, застосування, зміна, скасування), до реєстрації дій користувачів при використанні ресурсів ІТС, а також інших подій, що впливають на дотримання реалізованої в ІТС політики безпеки.

Правила розмежування інформаційних потоків формулюються на основі аналізу області (границі) існування, спрямованості (вхідні чи вихідні), джерел і приймачів, функціонального призначення потоків, вимог по забезпеченню конфіденційності, цілісності, спостережності і доступності.

Правила повинні визначати, де і на яких рівнях взаємодії систем повинне здійснюватися розмежування інформаційних потоків і з використанням яких атрибутів і механізмів (ідентифікаторів безпеки, мережних портів, ключів аутентифікації, ключів напрямків і мережних ключів шифрування). Правила повинні також визначати умови й обмеження по ініціюванню і завершенню процесів інформаційного обміну, наприклад, у виді асоціації безпеки.

Правила розмежування доступу користувачів і процесів до пасивних об'єктів визначають склад осіб, яким дозволений доступ до ресурсів ІТС, порядок правильного використання ресурсів ІТС, статус, права і привілеї адміністратора безпеки ІТС, статус, права і привілеї користувачів ІТС.

Порядок проведення відновлювальних робіт і забезпечення неперервного функціонування ІТС

У розділі «Порядок проведення відновлювальних робіт і забезпечення неперервного функціонування ІТС», повинні бути описані підходи щодо планування і порядку виконання відновлювальних робіт після збоїв, аварій,

інших непередбачених ситуацій (надзвичайних ситуацій) з метою забезпечення неперервного функціонування ІТС в захищеному режимі.

Під час планування цих робіт рекомендується враховувати такі питання:

- виявлення критичних з точки зору безпеки процесів у роботі АС;
- визначення можливого негативного впливу надзвичайних ситуацій на роботу АС;
- визначення й узгодження обов'язків персоналу і користувачів, а також порядку їхніх дій у надзвичайних ситуаціях;
- підготовка персоналу і користувачів до роботи в надзвичайних ситуаціях.

Порядок повинен описувати заходи щодо улагодження інцидента, резервування та відновлення, що включає в себе:

- опис типових надзвичайних ситуацій, які потенційно найбільш можливі в ІТС внаслідок наявності вразливих місць, або які реально мали місце під час роботи;
- опис процедур реагування на надзвичайні ситуації, які слід вжити відразу після виникнення інциденту, що може призвести до порушення політики безпеки;
- опис процедур тимчасового переводу ІТС або окремих її компонентів на аварійний режим роботи;
- опис процедур поновлення нормальної виробничої діяльності ІТС або окремих її компонентів;
- порядок проведення тренувань персоналу в умовах імітації надзвичайних ситуацій.

Порядок підлягає перегляду у разі виникнення таких змін в ІТС:

- встановлення нового обладнання або модернізація існуючого, включення до складу ІТС нових компонентів;
- встановлення нових систем життєзабезпечення ІТС (сигналізації, вентиляції, пожежогасіння, кондиціонування та ін.);
- проведення будівельно-ремонтних робіт;
- організаційні зміни у структурі ІТС, виробничих процесах, процедурах обслуговування ІТС;
- зміни у технології обробки інформації;
- зміни у програмному забезпеченні;
- будь-які зміни у складі і функціях КСЗІ.

У разі незначногу обсягу даних Політика безпеки як окремий документ не складається, а оформлюється як розділ Плану захисту.

Календарний план робіт із захисту інформації в ІТС

На підставі Плану захисту складається «**Календарний план робіт із захисту інформації в ІТС**», який може мати такі розділи:

- організаційні заходи;
- контрольно-правові заходи;
- профілактичні заходи;
- інженерно-технічні заходи;
- робота з кадрами.

Організаційні заходи - це комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення завдань захисту інформації шляхом регламентації діяльності персоналу і порядку функціонування засобів (систем) забезпечення інформаційної діяльності та засобів (систем) забезпечення захисту інформації. До плану можуть включатись заходи щодо:

- розробки документів (інструкцій, методик, правил, розпоряджень тощо) з різних напрямів захисту інформації в АС;
- внесення змін та доповнень до чинних в ІТС документів з урахуванням зміни умов (обставин);
- розробки та впровадження нових організаційних заходів з захисту інформації;
- обгрунтування необхідності застосування та впровадження нових засобів захисту інформації;
- координації робіт та взаємодії з іншими підрозділами організації або зовнішніми організаціями на всіх етапах життєвого циклу ІТС;
- розгляду результатів виконання затверджених заходів та робіт з захисту інформації;
- інші.

До контрольно-правових заходів можуть бути віднесені:

- контроль за виконанням персоналом (користувачами) вимог відповідних інструкцій, розпоряджень, наказів;
- контроль за виконанням заходів, розроблених за результатами попередніх перевірок;
- контроль за станом зберігання та використання носіїв інформації на робочих місцях;
- інші.

До профілактичних слід відносити заходи, спрямовані на формування у персоналу (користувачів) мотивів поведінки, які спонукають їх до безумовного виконання у повному обсязі вимог режиму, правил проведення робіт тощо, а

також на формування відповідного морально-етичного стану в колективі.

До інженерно-технічних слід відносити заходи, спрямовані на налагодження, випробування і введення в експлуатацію, супроводження і технічне обслуговування КЗЗ від НСД, засобів захисту інформації від загроз її витоку технічними каналами, інженерне обладнання споруд і приміщень, в яких розміщуються засоби обробки інформації, у тому числі в процесі капітального будівництва тощо.

Планування роботи з кадрами включає заходи з підбору та навчання персоналу (користувачів) встановленим правилам безпеки інформації, новим методам захисту інформації, підвищення їхньої кваліфікації. Навчання персоналу (користувачів) може здійснюватись власними силами, з залученням спеціалістів зовнішніх організацій або в інших організаціях. Навчання повинно здійснюватися за програмою, затвердженою керівництвом організації. Навчальні програми повинні мати теоретичний і практичний курси. Доцільність і необхідність включення до програм окремих розділів визначається особливостями ІТС і технологіями захисту інформації, що використовуються в ній, функціональними завданнями спеціалістів, що входять до складу навчальних груп та іншими чинниками.

Приклад календарного плану робіт із захисту інформації в ІТС

1. Організаційні заходи

Заходи	Виконавець	Регламент робіт	Терміни / період
Розробка ТЗ на КСЗІ	Служба захисту Адміністратори	Згідно НД ТЗІ 3.7-001-99	Після складання Плану захисту
Проектування КСЗІ	Розробник КСЗІ	Згідно НД ТЗІ 3.7-003-05 і НД ТЗІ 2.5-004-99	Після погодження ТЗ з Держспецзв'язку
Попередні випробування КСЗІ	Розробник КСЗІ	Згідно ДСТУ 2853-94 і «Програми та методики попередніх випробувань»	Після пуско-налагоджувальних робіт КСЗІ
Підготовка впровадження КСЗІ	Адміністратори	Призначення відповідальних осіб і підготовка відповідних розпоряджень щодо КСЗІ	Під час попередніх випробувань КСЗІ

Дослідна експлуатація КСЗІ	Служба захисту Адміністратори	Відпрацювання технологій оброблення інформації, проведення навчання персоналу	Після завершення попередніх випробувань
Державна експертиза КСЗІ	Адміністрація Держспецзв'язку	Згідно «Положення про державну експертизу»	Після завершення дослідної експлуатації
Введення в промислову експлуатацію	Служба захисту Адміністратори	Згідно «Інструкції з експлуатації ІТС в частині забезпечення захисту інформації»	Після отримання Атестату відповідності
Реєстрація МНІ і користувачів	Адміністратори	Заведення журналів обліку Реєстрація користувачів і МНІ в системі та журналах	Після наказу про введення ІТС в експлуатацію
Коригування політики безпеки	Служба захисту Адміністратори	Коригування окремих положень Розробка додаткових інструкцій як складових політики безпеки	у разі змін умов функціонування ІТС
Перегляд Плану захисту	Служба захисту Адміністратори	Розробка нових підходів до планування заходів захисту	щорічно
Супровід та модернізація КСЗІ	Служба захисту Адміністратори	Розробка технічних завдань на модернізацію КСЗІ згідно НД ТЗІ 3.7-001-99	згідно плану розвитку та вдосконалення КСЗІ
Чергове категоріювання	Комісія установи	Згідно НД ТЗІ 1.6-005-2013	через 5 років після первинного
Чергова державна експертиза	Адміністрація Держспецзв'язку	Згідно вимог «Положення про державну експертизу»	через 5 років після первинної

2. Контрольно-правові заходи

Заходи	Виконавець	Регламент робіт	Терміни / період
Контрольні заходи	Системний адміністратор	Перевірка справності ОС і ПЗ ІТС	щодня
	Адміністратор безпеки	Перевірка виконання вимог політики безпеки користувачами	щомісячно
	Служба захисту	Перевірка виконання політики безпеки адміністраторами	щоквартально
Перевірка стану захисту інформації	Комісія установи	Згідно «Положення про захист інформації в ІТС»	щорічно
Перевірка наявності МНІ	Комісія установи	Згідно «Інструкції про організацію діловодства»	щорічно

3. Профілактичні заходи

Заходи	Виконавець	Регламент робіт	Термін / період
Ознайомлення користувачів з порядком робіт та мірою відповідальності за дотримання вимог політики безпеки	Служба захисту	Оформлення допуску до роботи	після прийому на роботу
	Адміністратор безпеки	Згідно «Інструкції користувачу»	під час їхньої реєстрації в ІТС
Проведення занять з персоналом ІТС щодо виконання вимог політики безпеки в установі	Служба захисту	Згідно «Плану навчання в установі»	щоквартально
Підготовка та впровадження в рамках трудової угоди розділу відповідальності за виконання вимог політики безпеки	Служба захисту	Згідно вимог трудового законодавства	за рішенням керівника установи

4. Інженерно-технічні заходи

Заходи	Виконавець	Регламент робіт	Терміни / період
Пуско-налагод-жувальні роботи	Розробник КСЗІ	Згідно технічного завдання на КСЗІ	Після затвердження проекту КСЗІ
Попередні випробування КСЗІ	Розробник КСЗІ	Згідно ДСТУ 2853-94 і «Програми та методики попередніх випробувань»	Після пуско-налагоджувальних робіт КСЗІ
Дослідна експлуатація КСЗІ	Служба захисту Адміністратори	Відпрацювання технологічних процесів в ІТС	Після завершення випробувань
Державна експертиза КСЗІ	Експерт, призначений Держспецзв'язку	Згідно «Програми та методики експертних випробувань»	Після завершення дослідної експлуатації
Введення в промислову експлуатацію	Служба захисту Адміністратори	Згідно «Інструкції з експлуатації ІТС в частині забезпечення захисту»	Після отримання Атестату відповідності
Супровід КСЗІ	Розробник КСЗІ	Гарантійне обслуговування	Гарантійний термін
Технічне обслу-говування ІТС	Адміністратори	Згідно «Регламенту технічного обслуговування»	згідно термінів регламенту
Резервування баз даних і фондів	Адміністратор безпеки	Згідно «Інструкції з резервування баз даних»	щомісячно
Поновлення антивірусних баз	Адміністратор безпеки	Згідно «Інструкції з антивірусного захисту»	щодня
Перевірка МНІ і ІТС на наявність вірусів	Користувач (МНІ)	Згідно «Інструкції з антивірусного захисту»	щодня
	Адміністратори (ІТС)		щотижня
Модернізація КСЗІ	Розробник КСЗІ	Заміна (додавання) окремих компонентів КСЗІ згідно НД ТЗІ 3.7-001-99	згідно плану розвитку та вдосконалення КСЗІ

5. Робота з кадрами

Заходи	**Виконавець**	**Регламент робіт**	**Терміни / період**
Вступне ознайомлення з положеннями політики безпеки інформації (під розпис)	Служба захисту	Оформлення допуску до роботи	після прийому на роботу
	Адміністратор безпеки	Згідно «Інструкції користувачу»	під час їхньої реєстрації в ІТС
Інструктаж користувача щодо дій у випадку нештатної ситуації	Адміністратор безпеки	Згідно «Плану робіт у випадку нештатної ситуації»	щорічно
Проведення занять з професійної підготовки персоналу ІТС	Служба захисту Адміністратори	Згідно «Плану професійної підготовки в установі»	щотижня
Направлення на курси підвищення кваліфікації	Служба захисту	Згідно «Плану підвищення кваліфікації в установі»	згідно термінів плану

Контрольні питання:

1. Які є види політики безпеки?
2. Чого повинна стосуватись політика безпеки?
3. Використання чого повинна передбачати політика безпеки?
4. На яких принципах повинна базуватись політика безпеки?
5. На які об’єкти захисту повинна поширюватись політика безпеки?
6. Які гарантії повинна надавати політика безпеки?
7. З яких розділів складається політика безпеки?
8. Які загальні правила розмежування доступу ви знаєте?
9. Які питання необхідно врахувати для планування відновлювальних робіт?
10. Які заходи необхідно описати для планування відновлювальних робіт?
11. З яких розділів складається Календарний план робіт із захисту інформації?

ЛЕКЦІЯ № 4-5. ПЛАН ЗАХИСТУ ІНФОРМАЦІЇ В ІТС

План захисту інформації в ІТС розробляється на підставі проведеного аналізу технології обробки інформації, аналізу ризиків, сформульованої політики безпеки інформації.

План захисту визначає і документально закріплює об'єкт захисту інформації в ІТС, основні завдання захисту, загальні правила обробки інформації в ІТС, мету побудови та функціонування КСЗІ, заходи з захисту інформації.

План захисту має фіксувати на певний момент часу склад ІТС, перелік оброблюваних відомостей, технологію обробки інформації, склад комплексу засобів захисту інформації, склад необхідної документації тощо.

План захисту повинен регулярно переглядатися та при необхідності змінюватись.

Зміни та доповнення до Плану захисту затверджуються на тому ж рівні та в тому ж порядку, що і основний документ.

Для ІТС, в яких обробляється інформація, що становить державну або іншу встановлену законом таємницю, службова інформація, інформація, яка належить до державних інформаційних ресурсів, або інформація, необхідність захисту якої встановлено законом, План захисту є обов'язковим документом. Склад і зміст Плану захисту для таких ІТС встановлено «**Положенням про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в АС**», затвердженим ПКМУ № 180-98.

План захисту повинен складатись з таких розділів:

1. Завдання захисту, класифікацію, опис технології обробки службової інформації.

2. Модель загроз інформації в АС.

3. Політика (основні правила) захисту інформації в АС.

4. Перелік нормативних, розпорядчих, організаційно-технічних та інших документів, згідно з якими реалізовано захист інформації в АС.

5. Календарний план робіт із захисту інформації в АС.

План захисту рекомендується розробляти і для всіх інших ІТС, в яких обробляється інформація, що підлягає захисту згідно з законодавством України, згідно вимог «**Правил забезпечення захисту інформації в ІТС**», затверджених ПКМУ № 373-2006.

План захисту повинен складатись з таких розділів:

1. Завдання захисту, класифікацію інформації, яка обробляється в системі, опис технології обробки інформації.

2. Визначення моделі загроз для інформації в системі.

3. Основні вимоги щодо захисту інформації та правила доступу до неї в системі.

4. Перелік документів, згідно з якими здійснюється захист інформації в системі.

5. Перелік і строки виконання робіт службою захисту інформації.

Крім того, НД ТЗІ 1.4-001-2000 «**Типове положення про службу захисту інформації в АС**» має додаток «**Методичні вказівки щодо структури та змісту Плану захисту інформації в АС**».

План захисту повинен складатись з таких розділів:

1. Завдання захисту інформації в АС.
2. Класифікація інформації, що обробляється в АС.
3. Опис компонентів ІТС та технології обробки інформації.
4. Загрози для інформації в АС.
5. Політика безпеки інформації в АС.
6. Система документів з забезпечення захисту інформації в АС.

Приклад Плану захисту

План захисту інформації фінансової установи

Зміст

1. Мета і призначення КСЗІ в АС

Метою розробки КСЗІ є впровадження заходів та засобів, які реалізують способи, методи, механізми захисту інформації від несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом:

- підключення до апаратури та ліній зв'язку,
- маскування під зареєстрованого користувача,
- подолання заходів захисту з метою використання інформації або нав'язування хибної інформації,
- застосування закладних пристроїв чи програм,
- використання комп'ютерних антивірусів тощо.

Метою КСЗІ є формування моделі загроз інформації та моделі порушника об'єкта інформаційної діяльності, розробка політики безпеки та системи

документів з забезпечення захисту інформації в АС, розрахунок та оцінка ризиків.

КСЗІ призначена для захисту інформації, що циркулює та зберігається на робочих станціях і серверах установи.

КСЗІ створюється на основі Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», ДСТУ 3396.1-96, НД ТЗІ 1.1-002-99, НД ТЗІ 1.4-001-2000, НД ТЗІ 2.1-001-200, НД ТЗІ 3.7-001-99, НД ТЗІ 3.7-003-05.

2. Загальна характеристика ІТС і умов її функціонування

Фінансова компанія займається аналізом рентабельності підприємств на сучасному економічному ринку, залежно від попиту на товари чи послуги. Компанія веде підрахунки затрат та доходу при відкритті нових підприємств, крім цього компанія займається просуванням на ринок нових підприємств та приватних підприємців. Тому компанія займається аналізом ринку попиту на продукцію, що виробляється підприємствами і визначає основні тенденції виробництва у певний часовий період.

Загальна структурна схема обчислювальної системи АС.

Обчислювальна система даної компанії є локальною мережею, яка складається з 18 комп'ютерів, що знаходяться в одному приміщенні Офіс знаходиться на одному поверсі будівлі. За генеральним планом у компанії 6 робочих кімнат. З яких 4 кімнати - це робочі відділи компанії; кабінет головного директора компанії і приймальня.

Технічна характеристика обладнання

Комп'ютери, що використовуються для роботи персоналу: HPdc5800 (KV488EA)

Характеристика	**Значення**
Чіпсет	Intel Q33
Процесор	
Тип процесора	Intel Pentium Dual-Core E2180
Частота, GHz	2
Оперативна пам'ять	
Об'єм, MB	1024
Стандарт	PC2-6400
Жорсткий диск	
Об'єм, GB	160
Інтерфейс	SATA II
Графічний адаптер	
Чіпсет	Intel GMA 3100
Об'єм пам'яті, MB	256

Оснащення	
Вбудований оптичний накопичувач	DVD-RW
Звукова карта	HD Audio ADI1884
Зовнішні порти	8xUSB, COM, LPT, 2xPS/2, VGA, audio in/out
Мережевий адаптер	10/100/1000

Характеристика програмного забезпечення

На робочих станціях компанії використовується ліцензована ОС «Windows Vista Business», що має позитивний експертний висновок Держспецзв'язку. Вибір цієї ОС оснований на тому, що дана версія «Windows Vista» спеціально розроблена для підприємств і має посилену політику безпеки і системи захисту.

На серверах компанії використовується ліцензована ОС «Windows Server 2008 Standard Edition», що має позитивний експертний висновок Держспецзв'язку.

Для захисту робочих станцій і серверів компанії на них встановлюється ліцензоване антивірусне програмне забезпечення, що має позитивний експертний висновок Держспецзв'язку.

В ІТС компанії використовується ліцензоване прикладне програмне забезпечення, зокрема «Microsoft Office». Для забезпечення цілісності електронних документів можуть використовуваться ліцензійні засоби ЕЦП.

Клас і склад АС

Згідно з НД ТЗІ 2.5-005-99 «Класифікація ІТС і СФПЗ оброблюваної інформації від НСД» в фінансовій компанії інформація циркулює та обробляється в ІТС класу «2».

АС класу «2» - локалізований багатомашинний багатокористувацький комплекс, який обробляє інформацію різних категорій конфіденційності.

В складі ІТС функціонують такі додаткові технічні засоби:

- джерела безперебійного живлення;
- кабельне обладнання.

Характеристики фізичного середовища

Територія компанії охороняється штатом охоронців у кількості 4 осіб. Крім того, ведеться відеонагляд за територією та в середині приміщення.

У компанії запроваджена система електронних перепусток, що зменшує ймовірність загроз вчинити викрадення інформації зловмисником, що не є співробітником фірми, безпосередньо з її території.

Оскільки в ІТС не обробляється інформація, що становить державну таємницю, технічні канали витоку інформації не розглядаються та захист від них не планується.

При побудові плану розташування робочих місць необхідно керуватися такими принципами:

- екрани комп'ютерів не повинні бути повернуті до вікон або дверей;
- робочі місця розміщені таким чином,щоб мінімізувати спостереження за роботою одних користувачів за іншими.

У складі КСЗІ в ІТС функціонують такі засоби захисту:

- відеоспостереження;
- охоронно-пожежна сигналізація;
- сенсори розбиття скла на вікнах офісу;
- сенсори розкриття дверей приміщень;
- металеві грати на вікнах офісу.

Технічні характеристики каналів зв'язку

Для побудови локальної мережі використовується екранована вита пара. Згідно зі стандартами для захисту мережевого кабелю від зовнішніх пошкоджень використовуються екрановані металеві короба.

Характеристики інформації, що обробляється

Інформація, що обробляється в ІТС є власністю даної фірми та її клієнтів. В ІТС даного підприємстві обробляється відкрита та конфіденційна інформація. До конфіденційної інформації відносяться дані, що пов'язані з клієнтами фірми та їх справами, технологічна та ключова інформація. Інформація загального користування є відкритою інформацією.

№	Шифр	Назва	Тип доступу
1	{БД.К}	База даних - клієнтів	конфіденційна
2	{Д}	Договори	відкрита
3	{П.О}	Перелік обладнання	відкрита
4	{БД.П}	База даних - працівників	конфіденційна
5	{БД.З.Р}	База даних засобів і ресурсів	конфіденційна
6	{БД.Т.К}	База даних телефонів клієнтів	конфіденційна
7	{БД.Т.П}	База даних телефонів працівників	відкрита
8	{П}	Партнери	відкрита
9	{Ж.К.}	Журнал користувачів	відкрита
10	{Ж.Д.}	Журнал досягнень	відкрита

Характеристики персоналу та користувачів АС

До середовища персоналу установи та користувачів автоматизованої системи належать технічний та обслуговуючий персонал, системні адміністратори, адміністратор безпеки, працівники служби охорони, бухгалтери, маркетологи, секретар, працівники відділу роботи з клієнтами, керівники відділів, директор.

Найнижчі повноваження щодо допуску до відомостей, які обробляються в ІТС мають технічний та обслуговуючий персонал, а також працівники служби охорони. Достатньо високі повноваження мають працівники маркетингового відділу та відділу інформаційних технологій, дирекція. Найбільше повноваження щодо управління КСЗІ має адміністратор безпеки, дещо нижчий пріоритет у працівників служби безпеки та системних адміністраторів.

Працівники першого поверху мають доступ тільки до даних, що містяться на серверах першого поверху, працівники ж другого поверху переважно мають доступ до інформації, що зберігається на серверах другого поверху.

Вхід до серверних приміщень та приміщень для зберігання документів, звітів про діяльність компанії, зареєстрованих носіїв інформації, даних відео нагляду та спостереження, журнали відвідувань і т. д. мають лише дирекція та особи, яким надається допуск до цих матеріалів.

3. Формування моделі загроз для інформації в ІТС

Основою для проведення аналізу ризиків і формування вимог до КСЗІ є розробка моделі загроз для інформації та моделі порушника.

Для створення моделі загроз необхідно скласти перелік суттєвих загроз, описати методи і способи їхнього здійснення.

Загрози в ІТС можуть здійснюватися шляхом:

- підключення до апаратури та ліній зв’язку,
- маскування під зареєстрованого користувача,
- подолання заходів захисту з метою використання інформації або нав’язування хибної інформації,
- застосування закладних пристроїв чи програм,
- використання комп’ютерних антивірусів тощо.

Загрози для інформації, що обробляється в ІТС, залежать від характеристик ОС, персоналу, технологій обробки та інших чинників і можуть мати об'єктивну або суб'єктивну природу. Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні. Мають бути визначені основні види загроз для безпеки інформації, які можуть бути реалізовані стосовно ІТС і повинні враховуватись у моделі загроз, наприклад:

- зміна умов фізичного середовища (стихійні лиха і аварії, як землетрус, повінь, пожежа або інші випадкові події);

- збої і відмови у роботі обладнання та технічних засобів ІТС;

- наслідки помилок під час проектування та розробки компонентів ІТС (технічних засобів, технології обробки інформації, програмних засобів, засобів захисту, структур даних тощо);

- помилки персоналу (користувачів) ІТС під час експлуатації;

- навмисні дії (спроби) потенційних порушників.

Необхідно визначити перелік можливих загроз і класифікувати їх за результатом впливу на інформацію, тобто на порушення яких властивостей вони спрямовані (конфіденційності, цілісності та доступності інформації), а також порушення спостережності та керованості ІТС.

Випадковими загрозами суб'єктивної природи (дії, які здійснюються персоналом або користувачами по неуважності, недбалості, незнанню тощо, але без навмисного наміру) можуть бути:

- дії, що призводять до відмови ІТС (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв'язку, видалення даних, програм та ін.);

- ненавмисне пошкодження носіїв інформації;

- неправомірна зміна режимів роботи ІТС (окремих компонентів, обладнання, ПЗ тощо), ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації);

- ненавмисне зараження ПЗ комп'ютерними вірусами;

- невиконання організаційних заходів захисту згідно вимог чинних в ІТС розпорядчих документів;

- помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо;

- будь-які дії, що можуть призвести до розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів тощо;

- неправомірне впровадження і використання забороненого політикою безпеки ПЗ (наприклад, навчальні та ігрові програми, системне і прикладне забезпечення та ін.);

- наслідки некомпетентного застосування засобів захисту;

- інші.

Навмисними загрозами суб'єктивної природи, спрямованими на дезорганізацію роботи ІТС (окремих компонентів) або виведення її з ладу,

проникнення в систему і одержання можливості несанкціонованого доступу до її ресурсів, можуть бути:

- порушення фізичної цілісності ІТС (окремих компонентів, пристроїв, обладнання, носіїв інформації);

- порушення режимів функціонування (виведення з ладу) систем життєзабезпечення ІТС (електроживлення, заземлення, охоронної сигналізації, вентиляції та ін.);

- порушення режимів функціонування ІТС (обладнання і ПЗ);

- впровадження і використання комп'ютерних вірусів, закладних (апаратних і програмних) і підслуховуючих пристроїв, інших засобів розвідки;

- використання (шантаж, підкуп тощо) з корисливою метою персоналу ІТС;

- крадіжки носіїв інформації, виробничих відходів (роздруків, записів, тощо);

- несанкціоноване копіювання носіїв інформації;

- читання залишкової інформації з оперативної пам'яті ЕОМ, зовнішніх накопичувачів;

- одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача («маскарад»);

- неправомірне підключення до каналів зв'язку, перехоплення даних, що передаються, аналіз трафіку тощо;

- впровадження і використання забороненого політикою безпеки ПЗ або несанкціоноване використання ПЗ, за допомогою якого можна одержати доступ до критичної інформації (наприклад, аналізаторів безпеки мереж);

- інші.

Класифікація потенційних загроз інформації, що обробляється в ІТС

№	Джерело	Природа	Загроза	Наслідки порушення				Ресурси
				К	Ц	Д	С	
1	Зовнішнє	Об'єктивна	Стихійні явища		+	+		Всі
2	Зовнішнє	Об'єктивна	Збої та відмови системи електроживлення		+	+		Всі
3	Внутрішнє	Об'єктивна	Збої та відмови обчислювальної техніки		+	+		Всі
4	Внутрішнє	Об'єктивна	Збої, відмови та пошкодження носіїв інформації		+	+		Всі

5	Внутрішнє	Об’єктивна		Збої та відмови програмного забезпечення		+	+		Всі
6	Внутрішнє	Об’єктивна		Відмова в доступі користувачу ІТС в результаті помилки ПЗ			+		Окремі
7	Зовнішнє	Суб’єктивна	Навмисна/ ненавмисна	Ураження програмного забезпечення комп’ютерними вірусами	+	+	+	+	Всі
8	Внутрішнє	Суб’єктивна	Навмисна/ ненавмисна	Несанкціоноване внесення змін до технічних засобів, в програмне забезпечення, що призводять до		+	+	+	Окремі
9	Внутрішнє	Суб’єктивна	Навмисна/ ненавмисна	Порушення адміністратором безпеки реалізації ПРД	+	+	+	+	Окремі
10	Внутрішнє	Суб’єктивна	Ненавмисна	Втрата атрибутів розмежування доступу	+	+	+		всі
11	Внутрішнє	Суб’єктивна	Навмисна	Неправомірне впровадження і використання забороненого політикою безпеки ПЗ	+	+	+	+	всі
12	Зовнішнє	Суб’єктивна	Навмисна	Використання з корисливою метою персоналу ІТС	+	+	+	+	Окремі

13	Зовнішнє	Суб’єктивна	Навмисна	Несанкціонований доступ до приміщення ІТС	+	+	+	+	всі
14	Зовнішнє	Суб’єктивна	Навмисна	Вербування працівників підприємства	+	+			всі
15	Зовн./ Внутр.	Суб’єктивна	Навмисна	Розкрадання матеріальних носіїв інформації	+	+			всі
16	Внутрішнє	Суб’єктивна	Навмисна	Читання залишеної інформації	+				Окремі
17	Внутрішнє	Суб’єктивна	Ненавмисна	Ненавмисне псування матеріальних носіїв інформації			+		всі

4. Формування моделі порушника політики безпеки

Під порушником розуміється особа, яка зробила спробу виконання заборонених операцій помилково, не знаючи або навмисно зі злим помислом (корисним інтересом) або без таких (заради гри, самоствердження), заради самоствердження або помсти, використовуючи для цього різні способи і методи, можливості і засоби.

Порушник може використовувати різноманітні методи та засоби для доступу до ІзОД. Якщо порушник діє навмисне, з корисних мотивів, то будемо називати його зловмисником. Зловмисники винятково якісно вивчають системи безпеки в ІТС перед проникненням до неї.

Необхідно оцінити збитки, які можуть мати місце у випадку витоку інформації або при будь-якому іншому порушенні системи безпеки, а також ймовірність нанесення подібних збитків. Для визначення адекватності вартості системи захисту, слід зіставити розміри збитків і ймовірність їх нанесення з розмірами затрат на забезпечення захисту. Проте, реальну вартість інформації оцінити дуже важко, тому зазвичай використовують не кількісні, а якісні експертні оцінки. Найчастіше будується неформалізована модель порушника (зловмисника), що відображає причини й мотиви дій, його можливості, знання, цілі, основні шляхи досягнення поставлених цілей - способи реалізації загроз, місце і характер дії, можлива тактика і т. д. Для досягнення поставлених цілей зловмисник повинен прикласти деякі зусилля і затратити деякі ресурси.

Порушники класифікуються за рівнем можливостей, що надаються їм штатними засобами ІТС. Виділяються чотири рівні цих можливостей. Класифікація є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього:

- **перший рівень** визначає найнижчий рівень можливостей проведення діалогу з ІТС - можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;

- **другий рівень** визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;

- **третій рівень** визначається можливістю управління функціонуванням ІТС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;

- **четвертий рівень** визначається всім обсягом можливостей осіб, що забезпечують функцінування КЗЗ в ІТС, аж до включення до складу ІТС власних засобів з новими функціями обробки та захисту інформації.

Порушником по відношенню до ІТС можуть бути особи з персоналу і користувачів системи, а також сторонні особи.

Можливі внутрішні порушники :

- кінцеві користувачі (оператори системи), персонал (перший рівень);

- співробітники служби безпеки установи (перший рівень);

- керівники різних рівнів (перший рівень).

- системний адміністратор та особи, що обслуговують технічні засоби (третій рівень);

- адміністратор безпеки в ІТС (четвертий рівень);

Можливі зовнішні порушники (сторонні особи):

- технічний персонал, обслуговуючий будівлю (перший рівень);

- клієнти (перший рівень);

- представники організацій-конкурентів (другий рівень);

- відвідувачі, запрошені з будь-якого приводу (другий рівень).

Припускається, що в своєму рівні порушник - це фахівець вищої кваліфікації, який має повну інформацію про ІТС і КЗЗ.

Порушник може здійснювати несанкціонований доступ до інформації або під час роботи автоматизованої системи, або в період неактивності автоматизованої системи, або ж суміщаючи робочий і не робочий час.

У КСЗІ в ІТС передбачаються, розглядаються і розробляються усі 4 рівні порушників.

Модель порушника

№	**Користувач ІТС**	**Рівень порушника**
1.	Внутрішні	
1.1	Адміністратор безпеки	IV
1.2	Системний адміністратор	III
1.3	Персонал	I
2.	Зовнішні	
2.1	Працівник служби охорони	I
2.2	Працівник комунальних служб	I
2.3	Конкуренти	II
2.3	Клієнт	I

5. Розробка політики безпеки

Мета реалізації політики безпеки

Основною метою реалізації політики безпеки є забезпечення ефективного функціонування компанії, для чого необхідно забезпечити захист оброблюваної на підприємстві інформації від несанкціонованого доступу. Політика безпеки має на меті розробку та впровадження правил та норм внутрішнього режиму праці на підприємстві, режиму доступу та допуску до важливих об’єктів, їх охорона, середовище розміщень.

Загальні вимоги політики безпеки

Під час розробки політики безпеки були враховані технологія обробки інформації, описані вище моделі порушників і загроз, особливості ОС, фізичного середовища та інші чинники. В ІТС реалізовано декілька різних політик безпеки, які істотно відрізняються. Як складові частини загальної політики безпеки в ІТС

існують політики забезпечення конфіденційності, цілісності, доступності оброблюваної інформації.

Політика безпеки стосується: інформації (рівня критичності ресурсів ІТС), взаємодії об'єктів (правил, відповідальності за захист інформації, гарантій захисту), області застосування (яких складових компонентів ІТС політика безпеки стосується, а яких - ні).

Політика безпеки розроблена таким чином, що вона не потребує частої модифікації. Політика безпеки передбачає використання всіх можливих заходів захисту інформації(правові та морально-етичні норми, організаційні, фізичні, технічні заходи) і визначає правила та порядок застосування в ІТС кожного з цих видів.

Політика безпеки базується на наступних основних принципах:

- системності;
- комплексності;
- неперервності захисту;
- достатності механізмів і заходів захисту та їхньої адекватності загрозам;
- гнучкості керування системою захисту, простоти і зручності її використання;
- відкритості алгоритмів і механізмів захисту, якщо інше не передбачено окремо.

Політика безпеки дає гарантії того, що:

- в ІТС забезпечується адекватність рівня захисту інформації рівню її критичності;
- реалізація заходів захисту інформації є рентабельною;
- в будь-якому середовищі функціонування ІТС забезпечується оцінюваність і перевіряємість захищеності інформації;
- забезпечується персоніфікація положень політики безпеки (стосовно суб'єктів ІТС), звітність (реєстрація, аудит) для всіх критичних з точки зору безпеки ресурсів, до яких здійснюється доступ в процесі функціонування ІТС;
- персонал і користувачі забезпечені достатньо повним комплектом документації стосовно порядку забезпечення захисту інформації;
- всі критичні з точки зору безпеки інформації технології (функції) ІТС мають відповідні плани забезпечення неперервної роботи та її поновлення у разі виникнення непередбачених ситуацій;
- враховані вимоги всіх документів, які регламентують порядок захисту інформації в ІТС, та забезпечується їхнє суворе дотримання.

Вибір ФПЗ оброблюваної інформації від НСД

З точки зору забезпечення безпеки інформації ІТС або КЗЗ можна розглядати як набір функціональних послуг. Кожна послуга являє собою набір функцій, що дозволяють протистояти деякій множині загроз.

Згідно з аналізом роботи ІТС та відповідних експертиз визначено, що в ІТС циркулює інформація, яка потребує захисту. Ця інформація поділяється на відкриту інформацію, що потребує захисту, та інформацію з обмеженим доступом (далі - ІзОД), а саме: конфіденційну інформацію (персональні дані).

Згідно вимог ДСТУ 3396.1-96 найбільш підходящим варіантом захисту є такий варіант: досягнення необхідного рівня захисту ІзОД за допустимих затрат і заданого рівня обмежень видів інформаційної діяльності.

Відповідно до НД ТЗІ 2.5-005-99 потрібно визначити ФПЗ інформації. Перш за все нам потрібно забезпечити конфіденційність інформації, яка визначена як ІзОД. Крім того, у компанії обробляється відкрита інформація, що потребує захисту (деякі номери рахунків активів компанії, інформація про діяльність компанії і т.д.). Для такої інформації потрібно забезпечити цілісність.

Відповідно до НД ТЗІ 2.5-005-99 застосуємо функціональний профіль захищеності в ІТС класу «2» з підвищеними вимогами до забезпечення конфіденційності і цілісності інформації:

2.КЦ.5 = {КД-3, КА-3, КО-1, КК-1, ЦД-1, ЦА-3, ЦО-2, НР-4, НИ-2, НК-1, НО-3, НЦ-3, НТ-2}

Позначення послуг конфіденційності:

КД - довірча конфіденційність;

КА - адміністративна конфіденційність;

КО - повторне використання об’єктів.

КК - аналіз прихованих каналів

Позначення послуг цілісності:

ЦД - довірча цілісність;

ЦА - адміністративна цілісність;

ЦО - відкат.

Позначення послуг спостережності:

НР - реєстрація;

НИ - ідентифікація і автентифікація;

НК - достовірний канал;

НО - розподіл обов’язків;

НЦ - цілісність КЗЗ;

НТ - самотестування при старті.

Правила розмежування доступу користувачів та процесів до інформації в ІТС (ПРД)

ПРД забезпечуються виконанням таких заходів:

- налагоджуються засоби захисту ОС та, за необхідності, встановлюється додаткове КЗЗ;

- усі особи, які беруть участь в обробленні ІзОД в ІТС, повинні бути зареєстровані як користувачі ІТС;

- користувачі проходять процедуру автентифікації для отримання доступу до ресурсів ІТС;

- кожний користувач має свій унікальний ідентифікатор і пароль. Право видачі цих атрибутів надається адміністратору. Атрибути для адміністраторів надає адміністратор безпеки ІТС. Видача атрибутів дозволяється тільки після документальної реєстрації особи як користувача. Користувачам забороняється спільне використання персональних атрибутів;

- атрибути користувачів періодично змінюються, а невикористовувані і скомпрометовані – видаляються;

- надання доступу до ІзОД здійснюється з урахуванням наданих згідно зі службовою необхідністю повноважень, за умови достовірного розпізнавання користувачів встановленим КЗЗ. КЗЗ забезпечує можливість своєчасного доступу зареєстрованих користувачів до ІзОД;

- кожний користувач має машинні носії ІзОД (далі - МНІ), які закріплені за ним персонально, які він отримує за своїм підписом та підписом адміністратора безпеки в «Журналі обліку МНІ»;

- усі користувачі повинні знати «Інструкцію користувача» (пройти відповідний курс навчання та скласти іспит);

- кожне АРМ повинно мати свого адміністратора, який несе відповідальність за його працездатність та за дотримання всіх вимог і процедур, пов’язаних з обробкою інформації та її захистом. Таку роль може виконувати уповноважений користувач. Цей користувач повинен бути забезпечений відповідними інструкціями і навчений всім вимогам і процедурам;

- для попередження неавторизованого доступу до даних, ПЗ, інших ресурсів ІТС, керування механізмами захисту здійснюється адміністратором безпеки ІТС;

- для попередження поширення комп’ютерних вірусів відповідальність за дотримання правил використання ПЗ несуть: на АРМ - користувачі та адміністратор, в ІТС - адміністратор безпеки ІТС. Використовуватись повинно тільки ПЗ, яке дозволено політикою безпеки (ліцензійне, яке має відповідні сертифікати, експертні висновки тощо);

- за всі зміни ПЗ, створення резервних і архівних копій несе відповідальність адміністратор безпеки ІТС, такі роботи виконуються тільки з його дозволу;

- процедури використання активного мережевого обладнання, а також окремих видів ПЗ, яке може суттєво впливати на безпеку (аналізатори трафіку, аналізатори безпеки мереж, засоби адміністрування тощо), авторизовані і здійснюються під контролем адміністратора безпеки ІТС;

- адміністратори безпеки та КСЗІ ІТС повсякденно здійснюють перевірку працездатності всіх механізмів захисту інформації в ІТС, ведуть облік критичних з точки зору безпеки подій і готують звіти щодо цього.

Для кожного відділу створено свою робочу групу (домен) і користувачів, які можуть працювати лише у даній робочій групі, де вони мають наперед встановлені права. Користувача однієї робочої групи не може бути аутентифіковано у іншій. При вході у систему на ПЕОМ ІТС завантажуються особисті дані з файлового сервера та сервера баз даних. Розподіл обов'язків щодо виконання заходів, передбачених політикою безпеки

Адміністратор безпеки володіє всіма правами по установці і налаштуванню КСЗІ створює, видаляє облікові записи співробітників, слідкує за додержанням правил розмежування доступу, вносить зміни до них при зміні посади певного співробітника, а також при допуску до певної інформації.

Системний адміністратор слідкую за правильним функціонуванням комп'ютерної системи, проводить планові перевірки її компонентів, вирішує технічні проблеми ІТС при їх виникненні.

Працівник служби охорони проводить відео спостереження, реєструє відвідувачів у відповідному журна відповідає за дотриманням правил допуску до серверних приміщень та приміщень для зберігання документів, звітів про діяльність компанії, зареєстрованих носіїв інформації, даних відео нагляду та спостереження, журнали відвідувань і т. д., відповідає за безпеку установи і співробітників.

Дирекція координує роботу адміністратора безпеки та служби безпеки.

Служба безпеки, системні адміністратори та адміністратори безпеки узгоджують свою роботу.

6. Система документів з забезпечення захисту інформації в АС

Захист інформації в ІТСрегламентується такими документами:

- Закон України «Про захист інформації в ІТС»;

- Правила забезпечення захисту інформації в ІТС, затверджені ПКМУ № 373-2006;

- ДСТУ 3396.0-96 Технічний захист інформації. Основні положення;

- ДСТУ 3396.1-96 Технічний захист інформації. Порядок проведення робіт;

- ДСТУ 3396.2-97 Технічний захист інформації. Терміни та визначення;

- НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу;

- НД ТЗІ 1.1-003-99 Термінологія у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу;

- НД ТЗІ 1.4-001-00 Типове положення про службу захисту інформації в автоматизованій системі;

- НД ТЗІ 1.6-005-2013 Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці;

- НД ТЗІ 2.1-001-01 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення;

- НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу;

- НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу;

- НД ТЗІ 2.5-008-2002 Вимоги із захисту службової інформації від НСД під час оброблення в ІТС класу 2;

- НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі;

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

Нормативні, організаційно-розпорядчі та інші документи, що використовуються у АС:

- положення про захист інформації в АС;

- інструкції про порядок реалізації організаційних, первинних технічних та основних технічних заходів захисту, інструкції про порядок введення в експлуатацію КСЗІ, про порядок її модернізації, про порядок обробки ІзОД в АС, про порядок використання криптографічних засобів;

- правила управління паролями в АС, правила видачі, вилучення та обміну персональних ідентифікаторів, атрибутів розмежування доступу;

- інструкції, що встановлюють повноваження та відповідальність персоналу і користувачів;

- плани виконання робіт та здійснення окремих заходів з захисту інформації в АС.

В ІТС також складається календарний план робіт з реалізації заходів захисту інформації в АС, який містить такі розділи:

- організаційні заходи;
- контрольно-правові заходи;
- профілактичні заходи;
- інженерно-технічні заходи.
- робота з кадрами.

Контрольні питання:

1. Які ПКМУ вимагають складання Плану захисту?
2. Який НД ТЗІ визначає складання Плану захисту?
3. З яких розділів складається План захисту?

ЛЕКЦІЯ № 6-7. ВИБІР ОС, АВПЗ І КЗЗ

Перед початком розробки технічного завдання на створення КСЗІ в ІТС здійснюється вибір технічних і програмно-апаратних засобів, які реалізують задані вимоги щодо надійного функціонування ІТС та захисту інформації, яка в ній обробляється. В першу чергу, це операційна система (далі - ОС), антивірусне програмне забезпечення (далі - АВПЗ) і у разі потреби комплекс засобів захисту від НСД (далі - КЗЗ).

Стаття 8 Закону України «Про захист інформації в ІТС» визначає, що для створення комплексної системи захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері захисту інформації.

Тобто засоби захисту інформації, інші технічні засоби та програмне забезпечення ІТС, що планується задіяти в КСЗІ, повинні мати підтвердження їхньої відповідності НД ТЗІ (атестат, сертифікат відповідності, експертний висновок) і використовуватись згідно з вимогами НД ТЗІ.

Здійснення сертифікації, підтвердження відповідності та проведення державної експертизи таких засобів здійснює Адміністрація Держспецзв'язку. Вона веде **«Перелік засобів загального призначення, які дозволені для забезпечення ТЗІ, необхідність охорони якої визначено законодавством України»** (далі - Перелік), який формується відповідно до пункту 17 «Положення про ТЗІ в Україні», затвердженого Указом Президента України від 27.09.99 № 1229.

Перелік призначений для використання суб'єктами системи ТЗІ під час розроблення, модернізації та впровадження комплексів ТЗІ на ОІД та КСЗІ в ІТС і складається з 2-х розділів.

Розділ 1 містить номенклатуру технічних засобів із захистом інформації, засобів ТЗІ, засобів контролю за ефективністю ТЗІ, засобів виявлення та індикації загроз безпеці інформації, відповідність яких вимогам нормативних документів з питань ТЗІ засвідчено сертифікатом відповідності або позитивним експертним висновком, одержаними у порядку, який встановлено нормативно-правовими актами: «Правилами проведення робіт із сертифікації засобів захисту інформації», затвердженими спільним наказом Адміністрації Держспецзв'язку та Держспоживстандарту України від 25.04.2007 № 75/91 і зареєстрованими в Міністерстві юстиції України 14.05.2007 за № 498/13765, та «Положенням про державну експертизу в сфері ТЗІ», затвердженим наказом Адміністрації

Держспецзв'язку від 16.05.2007 № 93 і зареєстрованим в Міністерстві юстиції України 16.07.2007 за № 820/14087.

Розділ 2 містить номенклатуру технічних засобів, які за принципом дії не створюють каналів витоку оброблюваної інформації і можуть застосовуватися для оброблення інформації, необхідність охорони якої визначена законодавством. Він формується на підставі висновків державної експертизи або узгоджених із Держспецзв'язку результатів інших досліджень щодо цих технічних засобів, які засвідчують відсутність у них каналів витоку оброблюваної інформації.

Використання засобів цього Переліку під час розроблення, модернізації та впровадження комплексів ТЗІ на ОІД та КСЗІ в ІТС не звільняє від необхідності оцінювання відповідності досягнутого рівня захисту інформації встановленому вимогами нормативних документів з ТЗІ, яке здійснюється шляхом атестації комплексів ТЗІ на ОІД або експертизи КСЗІ в ІТС.

Можливість подальшого використання засобів, які не ввійшли до цього Переліку, в діючих комплексах ТЗІ на ОІД та КСЗІ в ІТС визначається за результатами їх чергової атестації або експертизи. Оновлення інформації, яка міститься в Переліку, здійснюється шляхом періодичного внесення змін до попередньої редакції. Перелік та його доповнення публікуються в засобах масової інформації та розміщуються на WEB-сайті Держспецзв'язку (www.dsszzi.gov.ua).

Вибір програмного забезпечення з Переліку здійснюється з урахуванням відповідності його обсягу функцій, що визначаються функціональним профілем захищеності (далі - ФПЗ), визначеному ФПЗ ІТС з відповідним рівнем гарантій, а також термін дії Експертного висновку.

Використання засобів ТЗІ, які на момент проектування КСЗІ не мають підтвердження відповідності у сфері ТЗІ

У разі необхідності використання в КСЗІ засобів ТЗІ, які на момент проектування КСЗІ не мали документа (сертифіката відповідності або експертного висновку), що підтверджує їх відповідність у сфері ТЗІ, ці засоби згідно з «Правилами забезпечення захисту інформації в ІТС», затвердженими ПКМУ від 29 березня 2006 року № 373, мають піддаватися відповідному оцінюванню під час проведення державної експертизи КСЗІ.

При цьому має оцінюватися відповідність засобів ТЗІ вимогам НД ТЗІ в обсязі показників тих функцій захисту, які реалізовані для захисту інформації, що обробляється в даній ІТС. Також має оцінюватися можливість створення

цими засобами ТЗІ технічних каналів витоку інформації (в тому числі через закладні пристрої).

Має бути проведений аналіз особливостей застосування засобів ТЗІ в даній ІТС, за результатами якого мають бути встановлені (ідентифіковані, уточнені) функції захисту, які реалізовані для захисту інформації саме в даній ІТС, та показники цих функцій.

Програма та методика проведення державної експертизи КСЗІ має містити перелік робіт щодо визначення (вимірювання) встановлених за результатами аналізу показників функцій захисту засобів ТЗІ, оцінки відповідності цих показників вимогам НД ТЗІ та оцінки можливості створення цими засобами ТЗІ технічних каналів витоку інформації. Також мають бути наведені нормативні документи з питань ТЗІ, які визначають вимоги до цих показників.

Результати визначення (вимірювань) показників функцій захисту засобів ТЗІ, результати їх порівняння з вимогами нормативних документів та результати оцінювання можливості створення цими засобами ТЗІ технічних каналів витоку інформації мають відображатися у відповідних протоколах, які подаються на розгляд Експертної ради Адміністрації Держспецзв'язку разом з матеріалами державної експертизи КСЗІ (з Протоколом державної експертизи КСЗІ та Експертним висновком).

Засоби ТЗІ, які пройшли оцінювання під час державної експертизи КСЗІ, можуть використовуватись для захисту інформації виключно у складі цієї КСЗІ.

1. Вибір ОС

Розглянемо тільки 3 популярні ОС, дані яких для зручного порівняння викладемо у табличному вигляді.

1	Комплекс засобів захисту операційної системи	**OpenBSD, шифр «BBOS»**	**Microsoft Windows Server 2019 Datacenter**	**Windows 8 Professional**
2	Виробник	Україна, ТОВ «АТМНІС»	США, Microsoft Corporation	США, Microsoft Corporation
3	Експертний висновок дійсний до	№ 373 31.08.2015	№ 1090 20.02.2023	№ 485 20.12.2016
4	Рівень гарантій	Г2	Г2	Г2
Послуги конфіденційності				
1	базова адміністр. конфіденційність	КА-2	-	-
2	базова довірча конфіденційність	КД-2	КД-2	КД-2
3	повторне використання об'єктів	КО-1	КО-1	КО-1

4	конфіденційність при обміні (баз/мін)	КВ-2	КВ-1	КВ-1
Послуги цілісності				
1	мінімальна адміністративна цілісність	ЦА-1	-	-
2	мінімальна довірча цілісність	ЦД-1	ЦД-1	ЦД-1
3	обмежений відкат	ЦО-1	ЦО-1	ЦО-1
4	мінімальна цілісність при обміні	ЦВ-1	ЦВ-1	ЦВ-1
Послуги доступності				
1	незахоплення ресурсів / квота	ДР-2	ДР-1	ДР-1
2	стійкість з погіршенням характеристик / при обмежених відмовах	ДС-2	ДС-1	-
3	обмежена гаряча заміна	ДЗ-2	ДЗ-2	ДЗ-2
4	автоматизоване відновлення	ДВ-2	ДВ-2	ДВ-2
Послуги спостережності				
1	захищений журнал	НР-2	НР-2	НР-2
2	одиночна ідентифікація і автентифікація	НИ-2	НИ-2	НИ-2
3	однонаправлений достовірний канал	НК-1	НК-1	НК-1
4	виділення адміністратора / розподіл обов'язків на підставі привілеїв	НО-1	НО-3	НО-3
5	КЗЗ з контролем цілісності / гарантованою цілісністю	НЦ-1	НЦ-2	НЦ-2
6	самотестування при старті	НТ-2	НТ-2	НТ-2
7	автентифікація вузла	НВ-1	НВ-1	НВ-1

Здійснивши порівняльний аналіз послуг безпеки ФПЗ механізмів захисту вище зазначених ОС, можна зробити такі висновки:

- КЗЗ ОС обох «Windows» майже однакові та відрізняються лише послугою стійкості до відмов, яка взагалі відсутня в ОС «Windows 8 Professional»;

- КЗЗ ОС «OpenBSD» на відміну від «Windows» забезпечує послуги адміністративної конфіденційності та цілісності на рівні КА-2 і ЦА-1, що дає можливість захисту інформації від несанкціонованого і неконтрольованого ознайомлення, модифікації, знищення, копіювання та розповсюдження.

Крім того, у разі використання тільки штатних засобів ОС «Windows» стає можливою умисна або випадкова реалізація будь-яким авторизованым користувачем (якому у зв'язку з виробничою необхідністю наданий доступ до каталога жорсткого диска, в якому зберігаються файли даних певного типу,

наприклад, файли текстових документів у форматі «MS Word», з метою читання і модифікації) наступних погроз:

- несанкціонованого копіювання файлів даних, що містять ІзОД, з використанням штатних засобів ОС (наприклад, програми «Провідник»), в каталоги жорсткого диска, які містяться у профайлі користувача (наприклад, каталог «Мої документи»), з отриманням можливості самостійно надавати права доступу до відповідного файлу іншим користувачам, а також безконтрольно його поширювати, що приведе до порушення конфіденційності ІзОД;

- несанкціонованого експорту даних, ІзОД, що містять, на з'ємні носії, розмежування доступу до яких засобами ОС «Windows» не здійснюється, що приведе до порушення конфіденційності ІзОД;

- несанкціонованій модифікації файлів даних з використанням штатних засобів ОС (наприклад, програми «Блокнот»), які не призначені для обробки файлів даних відповідного типу, що не тільки приведе до порушення цілісності ІзОД, але може взагалі привести до блокування можливості подальшої роботи авторизованих користувачів з відповідним файлом даних, тобто до порушення доступності інформації.

Крім того, засоби захисту ОС «Windows» не забезпечують виконання вимог пунктів 6 і 7 Правил щодо забезпечення захисту ІзОД від несанкціонованого і неконтрольованого ознайомлення, модифікації, знищення, копіювання, розповсюдження і забезпечення можливості надання користувачу права на виконання однієї або декількох операцій з оброблення конфіденційної інформації або позбавлення його такого права. Ці вимоги можуть бути задоволені тільки за умови реалізації адміністративного управління доступом (КА), тоді як у всіх ОС «Windows» реалізовано довірче управління доступом (КД).

Таким чином, у разі використання ОС «Windows» необхідно встановлення додаткового КЗЗ від НСД.

2. Вибір АВПЗ

Розглянемо тільки саме відоме АВПЗ під керуванням операційної системи «Windows», оскільки це найпоширеніша ОС.

1	Програмне забезпечення антивірусного захисту інформації під керуванням операційної системи «Windows»	McAfee MVISION Protect Standard	ESET Endpoint Antivirus 8.X	Zillya! Антивірус для Бізнесу версія 1.1

2	Виробник	США	Словаччина, ТОВ «ESET»	Україна, ТОВ «Олайті Сервіс»
3	Експертний висновок дійсний до	№ 1152 27.08.2023	№ 1257 17.05.2024	№ 1110 28.05.2023
4	Рівень гарантій	Г2	Г2	Г2
Послуги конфіденційності				
1	адміністративна конфіденційність	КА-2	КА-2	КА-2
Послуги цілісності				
1	базова адміністративна цілісність	ЦА-1	ЦА-2	ЦА-1
2	обмежений відкат	ЦО-1	ЦО-1	-
3	мінімальна цілісність при обміні	ЦВ-1	-	ЦВ-1
Послуги доступності				
1	використання ресурсів - квота	ДР-1	-	-
2	стійкість при обмежених відмовах	ДС-1	ДС-1	ДС-1
3	модернізація	ДЗ-1	ДЗ-1	ДЗ-1
4	ручне відновлення	ДВ-1	ДВ-1	ДВ-1
Послуги спостережності				
1	захищений журнал	НР-2	НР-2	НР-2
2	одиночна ідентифікація і автентифікація	НИ-2	НИ-2	НИ-2
3	однонаправлений достовірний канал	НК-1	НК-1	НК-1
4	виділення адміністратора	НО-1	НО-2	НО-1
5	КЗЗ з контролем цілісності	НЦ-1	НЦ-1	НЦ-1
6	самотестування при старті	НТ-2	-	НТ-2
7	автентифікація вузла	НВ-1	-	-

Здійснивши порівняльний аналіз послуг безпеки ФПЗ механізмів захисту вище зазначених АВПЗ, можна зробити такі висновки:

- «McAfee MVISION Protect Standard» є найсильнішим ПЗ, оскільки додатково забезпечує послуги ручного відновлення ДР-1 і автентифікації вузла НВ-1;

- «Zillya! Антивірус» у порівнянні з «ESET Endpoint Antivirus 5.0.X» додатково забезпечує послуги мінімальної цілісності при обміні ЦВ-1 і самотестування при старті НТ-2;

- «ESET Endpoint Antivirus 5.0.X» у порівнянні з «Zillya! Антивірус» додатково забезпечує послугу обмеженого відкату ЦО-1.

Порядок оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері ТЗІ

(затверджений наказом Адміністрації Держспецзв'язку від 26.03.2007 № 45 і зареєстрований в Міністерстві юстиції України 10.04.2007 за № 320/13587)

3. Поняття, що використовуються у цьому Порядку, мають таке значення:

- центр антивірусного захисту інформації (далі - ЦАЗІ) - організаційно-технічний комплекс, призначений для вирішення питання захисту ІТС від комп'ютерних вірусів з подальшим розвитком комплексного підходу до проблеми антивірусного захисту ІТС;

- комп'ютерний вірус - програма, що здатна створювати свої копії, модифіковані копії, які можуть цілком не відповідати оригіналу, і впроваджувати їх у різні об'єкти/ресурси ІТС безвідома користувача, й направлена на деструктивну дію;

- антивірусний програмний засіб (далі - АВПЗ) – програмне забезпечення, яке призначене для захисту об'єктів/ресурсів ІТС відушкодження комп'ютерними вірусами;

- антивірусне оновлення АВПЗ - складова частина АВПЗ, яка розробляється після створення засобу та призначена для пристосування АВПЗ до захисту об'єктів/ресурсів ІТС від ушкодженнята зараження новими вірусами.

5. Оновлення АВПЗ здійснюється шляхом організації та забезпечення процесу отримання та впровадження в АВПЗ антивірусних оновлень.

6. Оновлення АВПЗ, який пройшов державну експертизу та має позитивний експертний висновок Адміністрації Держспецзв'язку, здійснюється з використанням антивірусних оновлень, які розміщуються на веб-сайті ЦАЗІ (www.cazi.dsszzi.gov.ua).

7. На веб-сайті ЦАЗІ розміщуються тільки антивірусні оновлення АВПЗ, які пройшли експрес-експертизу. Крім того, на веб-сайті можна подивитись перелік АВПЗ, що отримало позитивний експертний висновок Держспецзв'язку.

8. Експрес-експертиза антивірусного оновлення АВПЗ здійснюється ЦАЗІ шляхом перевірки АВПЗ з впровадженим антивірусним оновленням на його

відповідність експертному висновку, виданому за результатами державної експертизи.

У подальшому під антивірусним оновленням АВПЗ розуміється антивірусне оновлення АВПЗ, яке пройшло експрес-експертизу.

9. Органи державної влади, органи місцевого самоврядування, утворені відповідно до законів України військові формування, підприємства, установи і організації державної форми власності:

- не менше ніж раз на день отримують антивірусні оновлення АВПЗ за допомогою веб-серверу ЦАЗІ;

- інсталюють отримані за допомогою веб-серверу ЦАЗІ антивірусні оновлення АВПЗ відповідно до технічної документації АВПЗ;

- для забезпечення авторизованого доступу до ресурсів веб-серверу ЦАЗІ щороку до 1 березня та, у разі внесення змін, протягом 3 днів надають до Адміністрації Держспецзв'язку відомості щодо кожного користувача у паперовому вигляді за визначеною формою.

10. Адміністрація Держспецзв'язку:

- організовує за допомогою спеціалізованого програмного забезпечення отримання органами державної влади, органами місцевого самоврядування, утвореними відповідно до законів України військовими формуваннями, підприємствами, установами та організаціями державної форми власності антивірусних оновлень для антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації, та забезпечує функціонування веб-серверу ЦАЗІ;

- заносить надану органами державної влади, органами місцевого самоврядування, утвореними відповідно до законів України військовими формуваннями, підприємствами, установами та організаціями державної форми власності реєстраційну інформацію до бази даних користувачів ЦАЗІ. Реалізує автентифікацію та ідентифікацію користувачів відповідно до цієї бази даних;

- проводить експрес-експертизу антивірусних оновлень АВПЗ;

- розробляє рекомендації щодо тримання антивірусних оновлень антивірусного програмного засобу та їх розміщення на веб-сайті ЦАЗІ;

- використовує механізм електронно-цифрового підпису для підтвердження цілісності антивірусних оновлень АВПЗ та ідентифікації підписувача після впровадження в органі державної влади, органі місцевого самоврядування, утворених відповідно до законів України військових формуваннях,

підприємствах, установах та організаціях державної форми власності електронно-цифрового підпису.

3. Вибір КЗЗ від НСД

3.1. Системи захисту в ІТС класу «1»

1	Система захисту інформації	**«ЛОЗА-1» версія 4**	**«Гриф» версія 4**	
2	Виробник	ТОВ НДІ «Автопром», м. Київ	ТОВ «ІКТ», м. Київ	
3	Експертний висновок дійсний до	№ 1095 02.04.2023	№ 1171 08.10.2023	
4	Рівень гарантій	Г4	Г4	
5	Рівень безпеки	Підвищен.	Стандарт.	-
Послуги конфіденційності				
1	адміністративна конфіденційність	КА-3	КА-2	КА-2
2	базова довірча конфіденційність	-	КД-2	-
3	повторне використання об’єктів	КО-1	КО-1	КО-1
Послуги цілісності				
1	мінімальна адміністративна цілісність	ЦА-1	ЦА-1	ЦА-1
2	мінімальна довірча цілісність	-	ЦД-1	-
3	обмежений відкат	-	-	ЦО-1
Послуги доступності				
1	стійкість при обмежених відмовах	ДС-1	ДС-1	ДС-1
2	модернізація	ДЗ-1	ДЗ-1	ДЗ-1
3	ручне відновлення	ДВ-1	ДВ-1	ДВ-1
Послуги спостережності				
1	захищений журнал	НР-2	НР-2	НР-3
2	множинна ідентифікація і автентифікація	НИ-3	НИ-3	НИ-3
3	однонаправлений достовірний канал	НК-1	НК-1	НК-1
4	розподіл обов'язків адміністратора	НО-2	НО-2	НО-2
5	КЗЗ з гарантованою цілісністю / контролем цілісності	НЦ-2	НЦ-2	НЦ-2
6	самотестування при старті	НТ-2	НТ-2	НТ-2

Здійснивши порівняльний аналіз послуг безпеки ФПЗ механізмів захисту вище зазначених КЗЗ, можна зробити такі висновки:

- КЗЗ на відміну від ОС «Windows» забезпечує послуги адміністративної конфіденційності КА та цілісності ЦА, що дає можливість захисту інформації від несанкціонованого і неконтрольованого ознайомлення, модифікації, знищення, копіювання та розповсюдження;

- «ЛОЗА-1» у порівнянні з «Гриф» має вищий рівень гарантій та забезпечує додатково такі послуги безпеки як стійкість при обмежених відмовах ДС-1 і модернізація ДЗ-1, однак не забезпечує послуги обмежений відкат ЦО-1;

- «ЛОЗА-1» для конфігурації «Стандартна безпека» у порівнянні з «Підвищеною безпекою» та «Гриф» забезпечує додатково послуги довірчої конфіденційності КД-2 та цілісності ЦД-1.

3.2. Системи захисту в ІТС класу «2»

1	Система захисту інформації	**«ЛОЗА-2» версія 3.X.Y**		**«Гриф-Мережа» версія 3** (базова)
2	Виробник	ТОВ НДІ «Автопром», м. Київ		ТОВ «ІКТ», м.Київ
3	Експертний висновок дійсний до	№ 383 16.10.2015		№ 1034 24.10.2022
4	Рівень гарантій	Г4		Г4
5	Рівень безпеки	Підвищен.	Стандарт.	-
Послуги конфіденційності				
1	адміністративна конфіденційність	КА-3	КА-2	КА-2
2	базова довірча конфіденційність	-	КД-2	-
3	повторне використання об’єктів	КО-1	КО-1	КО-1
Послуги цілісності				
1	адміністративна цілісність (мінім./базова)	ЦА-1	ЦА-1	ЦА-2
2	мінімальна довірча цілісність	-	ЦД-1	-
3	обмежений відкат	-	-	ЦО-1
Послуги доступності				
1	використання ресурсів - квота	-	-	ДР-1
2	стійкість при обмежених відмовах	ДС-1	ДС-1	ДС-1
3	модернізація	ДЗ-1	ДЗ-1	ДЗ-1
4	ручне відновлення	ДВ-1	ДВ-1	ДВ-1
Послуги спостережності				
1	детальна реєстрація / захищений журнал	НР-4	НР-4	НР-2
2	множинна ідентифікація і автентифікація	НИ-3	НИ-3	НИ-3

3	однонаправлений достовірний канал	НК-1	НК-1	НК-1
4	розподіл обов'язків адміністратора	НО-2	НО-2	НО-2
5	КЗЗ з гарантованою цілісністю	НЦ-2	НЦ-2	НЦ-2
6	самотестування при старті	НТ-2	НТ-2	НТ-2

Здійснивши порівняльний аналіз послуг безпеки ФПЗ механізмів захисту вище зазначених КЗЗ, можна зробити такі висновки:

- «ЛОЗА-2» у порівнянні з «Гриф-Мережа» забезпечує додатково такі послуги, як «детальна реєстрація» (НР-4), «стійкість при обмежених відмовах» (ДС-1) і «модернізація» (ДЗ-1), однак не забезпечує послуг «обмежений відкат» (ЦО-1) і «використання ресурсів» (ДР-1);

- «ЛОЗА-2» для конфігурації «Стандартна безпека» у порівнянні з «Підвищеною безпекою» та «Гриф-Мережа» забезпечує додатково послуги довірчої конфіденційності (КД-2) та цілісності (ЦД-1).

3.3. Системи захисту Web-ресурсів

1	Система захисту інформації	**«Захищена електрона пошта «Бриз»»**	**«Тайфун-PKI PKCS#11» версії 1.02**
2	Виробник	ТОВ «ІКТ», м.Київ	ТОВ «ІКТ», м.Київ
3	Експертний висновок дійсний до	№ 139 31.07.2011*	№ 691 06.03.2024
4	Рівень гарантій	Г4	Г4
Послуги конфіденційності			
1	базова адміністративна конфіденційність	-	КА-2
2	повторне використання об’єктів	-	КО-1
3	базова конфіденційність при обміні	КВ-2	КВ-2
Послуги цілісності			
1	мінімальна адміністративна цілісність	-	ЦА-1
2	обмежений відкат	-	-
3	базова цілісність при обміні	ЦВ-2	ЦВ-2
Послуги доступності			
1	стійкість при обмежених відмовах	ДС-1	ДС-1
2	модернізація	ДЗ-1	ДЗ-1
3	ручне відновлення	ДВ-1	ДВ-1
Послуги спостережності			
1	захищений журнал / зовнішній аналіз	НР-2	НР-1
2	одиночна / зовнішня ідентифікація і автентифікація	НИ-1	НИ-1

3	однонаправлений достовірний канал	-	-
4	розподіл обов'язків / виділення адміністратора	НО-2	НО-1
5	КЗЗ з контролем цілісності	НЦ-1	НЦ-1
6	самотестування при старті	НТ-2	НТ-2
7	автентифікація вузла / джерела даних	-	НВ-2
8	автентифікація відправника з підтвердженням	НА-2	-
9	автентифікація отримувача з підтвердженням	НП-2	-

*Поновлення ЕВ не вимагається

Здійснивши порівняльний аналіз послуг безпеки ФПЗ механізмів захисту вище зазначених КЗЗ, можна зробити такі висновки:

- «Тайфун-PKI PKCS#11» у порівнянні з «Захищена електрона пошта «Бриз»» має вищий рівень гарантій та забезпечує додатково такі послуги, як «базова конфіденційність при обміні» (КВ-2), «базова цілісність при обміні» (ЦВ-2), «стійкість при обмежених відмовах» (ДС-1) і «модернізація» (ДЗ-1);

- «Захищена електрона пошта «Бриз»» у порівнянні з «Тайфун-PKI PKCS#11» забезпечує додатково такі послуги, як «одиночна ідентифікація і автентифікація» (НИ-2), «захищений журнал» (НР-2), «розподіл обов’язків адміністраторів» (НО-2), «однонаправлений достовірний канал» (НК-1) і «обмежений відкат» (ЦО-1).

Кінцевий результат вибору ОС, АВПЗ і КЗЗ залежить від необхідності та достатності послуг безпеки, які повинні забезпечити обраний ФПЗ ІТС.

Контрольні питання:

1. Які операційні системи мають позитивний експертний висновок?
2. Які антивірусні програми мають позитивний експертний висновок?
3. Які КЗЗ від НСД в ІТС класу 1 мають позитивний експертний висновок?
4. Які КЗЗ від НСД в ІТС класу 2 мають позитивний експертний висновок?
5. Які КЗЗ від НСД Web-ресурсів мали позитивний експертний висновок?
6. Як повинні здійснювати оновлення АВПЗ державні органи?
7. Де розміщуються антивірусні оновлення, що мають позитивний експертний висновок?
8. Який нормативний документ визначає оновлення АВПЗ, що мають позитивний експертний висновок?
9. Яким чином можна використовувати засоби захисту, що не входять до Переліку дозволених засобів?

ЛЕКЦІЯ 8-9. ОПИС ФУНКЦІЙ І МОЖЛИВОСТЕЙ КЗЗ ВІД НСД

1. Системи захисту в ІТС класу «1»

1.1. Комплекс засобів захисту операційної системи Microsoft Windows 10 Professional

Комплекс засобів захисту операційної системи Microsoft Windows 10 Professional є клієнтською багатозадачною, багатокористувацькою, багатопроцесорною, мережевою ОС. ОС Microsoft Windows 10 Professional призначена для використання в крупних підприємствах та організаціях та має відповідні засоби розгортання та підтримки.

Комплекс засобів захисту ОС Microsoft Windows 10 Professional – це сервіси безпеки операційної системи Microsoft Windows 10 Professional призначені для забезпечення конфіденційності, цілісності, доступності та спостережності об’єктів захисту.

Розмежування доступу користувачів різних категорій до ресурсів комп’ютерної системи, захисту інформаційних об’єктів від НСД, забезпечення доступності об’єктів захисту, моніторингу подій комп’ютерної системи.

Відповідає вимогам НД з ТЗІ в обсязі функцій, зазначених у документі “Державна експертиза за критеріями технічного захисту інформації операційної системи Microsoft Windows 10 Professional. Технічні вимоги”, що визначаються функціональним профілем: КД-2, КВ-1, КО-1, ЦД-1, ЦА-1, ЦВ-1, ЦО-1, ДР-1, ДЗ-2, ДВ-2, НР-1, НР-2, НИ-1, НИ-2, НК-1, НО-3, НЦ-2, НТ-2, НВ-1 з рівнем гарантій Г-2 оцінки коректності їх реалізації згідно з НД ТЗІ 2.5-004-99 та має Експертний висновок №1027 дійсний з 26.09.2019.

1.2. Система ЛОЗА™-1

Система ЛОЗА™-1 — це програмний засіб захисту інформації від несанкціонованого доступу в автоматизованих системах класу «1» (зазвичай це автономний комп’ютер). Система ЛОЗА™-1 може працювати під керуванням операційних систем Windows 7/8/8.1/10/ Server 2008/2012/2016/2019 (32- та 64-розрядних версіях).

Система ЛОЗА™-1 не підтримує операційні системи Microsoft Windows початкової та домашньої редакцій (Starter edition, Home edition).

Система ЛОЗА™-1 реалізує всі стандартні функції, необхідні для надійного захисту інформації від несанкціонованого доступу і для побудови комплексної системи захисту інформації.

Система ЛОЗА™-1 може використовуватись для захисту інформації, що становить державну таємницю, — це підтверджено експертним висновком

№1095 , виданим Державною службою спеціального зв'язку та захисту інформації України 02 квітня 2020р.

ЛОЗА™-1 постачається у двох конфігураціях:

- «Підвищена безпека» — для захисту інформації, що становить державну таємницю;
- «Стандартна безпека» — для захисту службової та конфіденційної інформації (в тому числі персональних даних).
- Захист від несанкціонованого доступу до інформації:
- система ЛОЗА™-1 забезпечує надійний захист документів Microsoft Word та Microsoft Excel за рахунок тісної інтеграції з Microsoft Office (відключаються небезпечні команди, макроси, шаблони тощо); підтримуються версії Microsoft Office 2007/2010/2013/2016/2019;
- система ЛОЗА™-1 дозволяє захистити будь-які дані на знімних та стаціонарних носіях; захист здійснюється на рівні папок Windows та знімних дисків.
- система ЛОЗА™-1 дозволяє контролювати роботу із знімними дисками: дискетами, компакт-дисками та «флешками», для «флешек» дозволи на доступ до диска можуть встановлюватись для окремих носіїв (вони ідентифікуються за «залізним» серійним номером);
- система ЛОЗА™-1 дозволяє встановлювати дозволи або заборони на запуск процесів.

Контроль друку та експорту:

- система ЛОЗА™-1 забезпечує можливість встановлення дозволу/заборони друку та експорту на рівні окремих документів;
- для підсилення контролю система ЛОЗА™-1 дозволяє забезпечити присутність адміністратора або іншої уповноваженої особи під час друку та експорту (за рахунок необхідності введення пароля).

Контроль входу користувачів до системи:

- у конфігурації «Підвищена безпека» вхід здійснюється тільки після введення пароля та встановлення ключового диска (може використовуватись звичайна дискета, «флешка» або CD/DVD-диск); діє жорстка політика паролів та політика блокування користувачів, яка протидіє підбору паролів;
- у конфігурації «Стандартна безпека» для входу достатньо ввести пароль; політика паролів менш жорстка, ніж в конфігурації «Підвищена безпека».

Реєстрація подій:

- система ЛОЗА™-1 веде захищений журнал, в якому реєструються всі події, важливі для захисту інформації;

- аналіз журналу та протоколів роботи не потребує спеціальної кваліфікації;
- журнал подій ніколи не перезаписується: після досягнення граничного розміру журналу всі події зберігаються у файлі на жорсткому диску;
- система ЛОЗА™-1 забезпечує докладну реєстрацію подій друку та експорту; поряд із стандартною інформацією у журналі фіксуються гриф та обліковий номер документа, а також серійний номер носія, на якому зберігається документ, та носія, на який здійснюється експорт; адміністратор має можливість формування протоколу друку документів.

Профіль системи:

Для конфігурації «Підвищена безпека»:

КА-3, КО-1, ЦА-1, ДС-1, ДЗ-1, ДВ-1, НР-4, НИ-3, НК-1, НО-2, НЦ-2, НТ-2

Для конфігурації «Стандартна безпека»:

КД-2, КА-2, КО-1, ЦД-1, ЦА-1, ДС-1, ДЗ-1, ДВ-1, НР-4, НИ-2/НИ-3, НК-1, НО-2, НЦ-2, НТ-2

Рівень гарантій: Г-4.

До комплекту поставки системи ЛОЗА™-1 входять:

документація у друкованому вигляді:

- Паспорт;
- Інструкція з інсталяції;

документація в електронному вигляді:

- Паспорт ;
- Інструкція з інсталяції ;
- Загальний опис системи , Додаток А , Додаток Б;
- Інструкція адміністратора безпеки ;
- Інструкція системного адміністратора ;
- Інструкція адміністратора документів ;
- Інструкція користувача ;
- Програма «Захищені документи». Інструкція користувача ;
- Програмні засоби адміністрування системи. Інструкція користувача

Ціна одного комплекту – 7200 грн без ПДВ відповідно до пункту 26-1 підрозділу 2 розділу XX "Перехідні положення" Податкового кодексу України.

1.3. Комплекс «Гриф» версії 4

Засіб технічного захисту інформації від несанкціонованого доступу (НСД) «Комплекс **«Гриф» версії 4** (надалі – комплекс «Гриф» версії 4) призначений для забезпечення захисту інформації з обмеженим доступом (ІзОД) (у тому числі інформації, що становить державну таємницю; службової інформації; конфіденційної інформації про особу (персональних даних); інформації, що

становить комерційну таємницю і т.п.), оброблюваної в автоматизованих системах (АС) класу 1 та в ІТС класу 2, що побудовані на базі ПЕОМ (у випадку ІТС класу 2 – об'єднаних в однорангову локальну обчислювальну мережу), які функціонують під керуванням операційних систем (ОС) корпорації Microsoft:

- Windows 7 (в т.ч. 64-розрядних) - всі версії крім Home Basic, Home Premium Starter (без пакетів оновлень і з пакетом оновлень SP1);
- Windows 8.1 (в т.ч. 64-розрядних) - всі версії крім Core та SL;
- Windows 10 - всі версії крім Home;
- Windows Server 2008 R2 - без пакетів оновлень і з пакетом оновлень SP1;
- Windows Server 2012 R2 - без пакетів оновлення або з пакетами оновлення;
- Windows Server 2016/2019 - без пакетів оновлення або з пакетами оновлення.

Комплекс може також використовуватись на робочих станціях та серверах розподілених обчислювальних мереж, які функціонують під керуванням вищевказаних ОС (крім випадків, коли робочі станції і сервери обчислювальної мережі об'єднані в єдиний домен Active Directory. В цьому випадку необхідно використовувати комплекс «Гриф-Мережа»).

На відміну від політики довірчого керування доступом, яка реалізується штатними засобами захисту вищевказаних ОС, використання комплексу «Гриф» версії 4 дозволяє забезпечити реалізацію політики адміністративного керування доступом до ІзОД, тобто такого розмежування доступу, при якому призначати права доступу користувачів до захищених інформаційних ресурсів можуть тільки спеціально уповноважені користувачі (адміністратори). Комплекс повністю заміняє штатні засоби ОС власними засобами, які підримують реалізацію адміністративного розмежування доступу до захищених ресурсів.

Комплекс забезпечує захист інформації, яка представлена у вигляді файлів даних довільного типу (електронних документів, електронних таблиць, конструкторських креслень, даних геоінформаційних систем і т.п.).

Комплекс «Гриф» версії 4 реалізує такі основні функції захисту:

- ідентифікацію та автентифікацію користувачів на підставі імені (псевдоніма), пароля та персонального носія даних автентифікації (дискети, пристрою Flash Drive, CD-RW, DVD-RW або іншого знімного файлового носія);
- розподіл обов'язків користувачів та виділення декількох ролей адміністраторів, які можуть виконувати різні функції з адміністрування (реєстрацію захищених ресурсів, реєстрацію користувачів, призначення прав доступу, оброблення протоколів аудиту, тощо);

- розмежування доступу користувачів до обраних каталогів файлової системи незнімних носіїв ПЕОМ (у тому числі різних ПЕОМ, що функціонують у складі ЛОМ) та файлів, що містяться у них, що дозволяє організувати спільну роботу декількох користувачів, які мають різні службові обов'язки та права по доступу до захищеної інформації;
- курування потоками інформації та блокування потоків інформації, що можуть призвести до зниження її рівня конфіденційності;
- керування створеними на знімних або незнімних носіях ПЕОМ захищеними логічними дисками, вся інформація на яких зберігається у зашифрованому вигляді, та розмежування доступу до їх вмісту з використанням механізмів "прозорого" розшифрування/ зашифрування даних у момент їх читання/ запису, що дозволяє забезпечити захист конфіденційності збереженої інформації навіть у випадку крадіжки ПЕОМ або відповідних носіїв;
- контроль цілісності захищених логічних дисків, що дозволяє забезпечити захист від несанкціонованої модифікації збереженої на них інформації при відключених засобах захисту або у випадку крадіжки відповідних носіїв;
- контроль за виведенням інформації на пристрої друку з можливістю маркування друкованих аркушів документів (у форматі "Office Open XML") відповідно до вимог діючих нормативних документів в сфері охорони державної таємниці;
- контроль за експортом інформації на знімні носії та за імпортом інформації зі знімних носіїв із забезпеченням можливості реєстрації змінних носіїв та обмеження (для певних користувачів) переліку використовуваних знімних носіїв тільки зареєстрованими;
- гарантоване знищення інформації з обмеженим доступом при видаленні відповідних файлів;
- розмежування доступу прикладних програм до обраних каталогів та файлів, що містяться у них, що дозволяє забезпечити захист інформації від випадкового видалення або пошкодження, а також забезпечити дотримання технології її оброблення;
- контроль цілісності прикладного програмного забезпечення (ПЗ) та ПЗ комплексу, а також блокування завантаження програм, цілісність яких порушено, що дозволяє забезпечити захист від шкідливих програм (комп'ютерних вірусів) та дотримання технології оброблення ІзОД;
- контроль за використанням дискового простору користувачами, що виключає можливість блокування одним із користувачів можливості роботи інших користувачів;

- можливість блокування пристроїв інтерфейсу користувача (клавіатури, миші, монітора) на час його відсутності;
- контроль цілісності та самотестування комплексу при старті та за запитом адміністратора;
- відновлення функціонування комплексу у випадку збоїв, що гарантує доступність інформації при дотриманні правил доступу до неї;
- реєстрацію, аналіз та надання уповноваженим адміністраторам можливості оброблення інформації про події, які мають безпосереднє відношення до безпеки оброблюваної інформації, що дозволяє адміністраторам контролювати доступ до ІзОД, слідкувати за тим, як використовується комплекс, а також правильно його конфігурувати;
- ведення архівів зареєстрованих даних аудита;
- взаємодію з прикладними програмними системами (ППС) через визначений розробником комплексу інтерфейс, що дозволяє забезпечити безперервність захисту ІзОД при її обробці як штатними засобами ОС, так і засобами різноманітних ППС.

Розробка комплексу «Гриф» версії 4 виконана у відповідності з вимогами НД ТЗІ 2.5-012-2015, НД ТЗІ 2.5-008-2002 та рекомендаціями НД ТЗІ 2.4-015-2018. За результатами державної експертизи за критеріями технічного захисту інформації (експертний висновок зареєстрований в Адміністрації Держспецзв'язку 08.10.2020 г. за № 1171) встановлено, що сукупність функцій та механізмів захисту інформації, реалізованих в комплексі «Гриф» версії 4, забезпечує реалізацію такого функціонального профілю захищеності:

КА-2, КО-1, ЦА-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-3, НИ-3, НК-1, НО-2, НЦ-2, НТ-2.

Розробка комплексу «Гриф» версії 4 виконана у відповідності з вимогами до рівня гарантій Г-4. Це означає, що експертний висновок розповсюджується не тільки на поточну версію комплексу, а і на всі оновлення, які будуть випускатися у майбутньому.

Порівняння послуг безпеки ФПЗ механізмів захисту ОС і КЗЗ

№	Комплекс засобів захисту	**ФПЗ АС-1**	**Windows 8 Profes-sional**	**ЛОЗА-1 версія 4 «СБ»**	**Рубіж-РСО версія 2**
1	рівень гарантій	**Г2**	Г2	Г4	Г3
2	мінім./ базова адміністративна конфіденційність	**КА-1**	-	КА-2	КА-2
3	базова довірча конфіденційність	**КД-2**	КД-2	КД-2	-
4	повторне використання об’єктів	**КО-1**	КО-1	КО-1	КО-1
5	мінімальна адміністративна цілісність	**ЦА-1**	-	ЦА-1	ЦА-1
6	обмежений відкат	**ЦО-1**	ЦО-1	-	ЦО-1
7	ручне відновлення	**ДВ-1**	ДВ-2	ДВ-1	ДВ-1
8	захищений журнал	**НР-2**	НР-2	НР-4	НР-2
9	один. / множинна ідентифікація і автентифікація	**НИ-2**	НИ-2	НИ-2	НИ-3
10	однонаправлений достовірний канал	**НК-1**	НК-1	НК-1	НК-1
11	розподіл обов'язків на підставі привілеїв / розподіл обов'язків адміністратора	**НО-1**	НО-3	НО-2	НО-2
12	КЗЗ з гарантованою цілісністю / контролем цілісності	**НЦ-1**	НЦ-2	НЦ-2	НЦ-1
13	самотестування при старті	**НТ-1**	НТ-2	НТ-2	НТ-2

Здійснивши порівняльний аналіз послуг безпеки ФПЗ механізмів захисту ОС і вище зазначених КЗЗ, можна зробити висновок, що з урахуванням послуг безпеки ОС обидва КЗЗ забезпечують визначений ФПЗ АС-1 (в першу чергу, КА-2 і ЦА-1). У такому випадку вибір КЗЗ залежить від його вартості та якості сервісного обслуговування.

http://ict.com.ua/?lng=1&sec=8&art=51

2. Системи захисту в ІТС класу «2»

2.1. Система ЛОЗА-2

Система ЛОЗА-2 - це програмний засіб захисту інформації від несанкціонованого доступу в автоматизованих системах класу «2» (ЛОМ). Система ЛОЗА-2 може працювати під керуванням операційних систем

Windows XP / Vista / 7 / 2003 Server / 2008 Server / 2008 Server R2 (32- та 64-розрядних версіях).

Система ЛОЗА-2 на теперішній час не підтримується виробником в зв'язку з тим що системи «ЛОЗА-1» при встановлені на кожен комп'ютер реалізує функції захисту мережі аналогічно «ЛОЗА-2».

2.2. Комплекс «Гриф-Мережа»

Комплекс «Гриф-Мережа» призначений для забезпечення захисту інформації з обмеженим доступом (ІзОД), яка обробляється в локальних обчислювальних мережах (ЛОМ). До складу ЛОМ можуть входити файлові сервери, які функціонують під керуванням операційних систем (ОС) MS Windows Server 2003/ MS Windows Server 2008 R2/ MS Windows Server 2012 R2/ MS Windows Server 2016/2019, та робочі станції, які функціонують під керуванням ОС MS Windows XP Professional/ MS Windows 7 (Professional, Enterprise, Ultimate у т.ч. 64-розрядних)/ MS Windows 8.1 (Professional, Enterprise у т.ч. 64-розрядних)/ MS Windows 10 (Professional, Enterprise у т.ч. 64-розрядних), об'єднаних в єдиний домен.

Комплекс дозволяє створити на базі ЛОМ спеціалізовану автоматизовану систему класу 2 для оброблення ІзОД та забезпечити захист оброблюваної ІзОД від загроз порушення цілісності, конфіденційності та доступності при реалізації політики адміністративного керування доступом до інформації.

Комплекс постачається в двох конфігураціях: у базовій та в конфігурації для умов з підвищеними вимогами до забезпечення спостережності. Відміна між зазначеними конфігураціями комплексу полягає в тому, що в конфігурації для умов з підвищеними вимогами до забезпечення спостережності реалізована можливість збору та аналізу в реальному часі інформації про критичні з точки зору захищеності інформації події, зареєстровані на серверах, робочих станціях та активних мережевих пристроях, які функціонують у складі захищеної ЛОМ. В базовій конфігурації в реальному часі виконується тільки збереження інформації про критичні з точки зору захищеності інформації події, зареєстрованих на серверах та робочих станціях, які функціонують у складі захищеної ЛОМ, її аналіз виконується у відкладеному режимі.

Комплекс у базовій конфігурації доцільно використовувати для захисту інформації в ЛОМ, кількість робочих станцій в яких відносно невелике (до 30) та при цьому всі робочі станції розміщені в одному або кількох суміжних приміщеннях.

Комплекс у конфігурації для умов з підвищеними вимогами до забезпечення спостережності доцільно використовувати для захисту інформації в ЛОМ,

кількість робочих станцій в яких достатньо велика (більше 30) або в яких робочі станції розміщені у великій кількості територіально віддалених приміщень (наприклад, по кілька робочих станцій в приміщеннях на різних поверхах багатоповерхової будівлі).

Комплекс «Гриф-Мережа» версії 3.04 реалізує такі функції:

- ідентифікацію та автентифікацію користувачів на підставі імені (псевдоніма), паролю та носія даних автентифікації (знімного файлового носія (пристрій Flash Drive, CD-RW, DVD-RW, дискета тощо)) при завантаженні ОС робочої станції до завантаження будь-яких програмних засобів з дисків, що дозволяє заблокувати використання робочої станції сторонньою особою, а також розпізнати конкретного легального користувача та в подальшому реагувати на запити цього користувача відповідно до його повноважень;
- блокування пристроїв інтерфейсу користувача (клавіатури, миші, монітора) на час його відсутності;
- контроль цілісності та самотестування КЗЗ при старті та за запитом адміністратора, що дозволяє забезпечити стале функціонування КЗЗ та не допустити обробку ІзОД у випадку порушення його працездатності;
- розподіл обов’язків користувачів та виділення кількох ролей адміністраторів, які можуть виконувати різні функції з адміністрування (реєстрацію захищених ресурсів, реєстрацію користувачів, призначення прав доступу, оброблення протоколів аудита, тощо);
- розмежування доступу користувачів до вибраних каталогів (папок), розміщених на робочих станціях та файлових серверах ЛОМ, та до файлів, які в них знаходяться, що дозволяє організувати одночасну спільну роботу кількох користувачів ЛОМ, які мають різні службові обов’язки та права по доступу до ІзОД;
- керування потоками інформації та блокування потоків інформації, що можуть призвести до зниження рівня її конфіденційності;
- контроль за виводом інформації на друк з можливістю маркування друкованих листів документів (в форматі "Office Open XML") відповідно до вимог діючих нормативних документів з охорони державної таємниці;
- контроль за експортом інформації на знімні носії з можливістю обмеження переліку знімних носіїв, які використовуються;
- контроль за імпортом інформації зі знімних носіїв;
- гарантоване видалення інформації шляхом затирання вмісту файлів, які містять ІзОД, при їх видаленні;

- розмежування доступу прикладних програм до вибраних каталогів та файлів, які в них знаходяться, що дозволяє забезпечити захист ІзОД від випадкового видалення, модифікації, а також забезпечити дотримання технології її оброблення;
- контроль цілісності прикладного та системного програмного забезпечення (ПЗ) та ПЗ КЗЗ, а також блокування завантаження програм, цілісність яких порушена, що дозволяє забезпечити захист від вірусів та дотримання технології оброблення ІзОД;
- контроль за використанням користувачами дискового простору файлових серверів (квоти), що виключає можливість блокування одним з користувачів можливості роботи інших;
- відновлення функціонування КЗЗ після збоїв, що гарантує доступність інформації з забезпеченням дотримання правил доступу до неї;
- безперервну реєстрацію, аналіз та обробку подій (входу користувачів в ОС, спроб несанкціонованого доступу, фактів запуску програм, роботи з ІзОД, виводу на друк і т.п.) в спеціальних протоколах аудита, що дозволяє адміністраторам контролювати доступ до ІзОД, слідкувати за тим, як використовується КЗЗ, а також правильно його конфігурувати;
- негайне оповіщення адміністратора безпеки про всі виявлені порушення встановлених правил розмежування доступу (у конфігурації для умов з підвищеними вимогами до забезпечення спостережності);
- ведення архіву зареєстрованих даних аудита;
- взаємодію з прикладними програмними системами через визначений виробником КЗЗ інтерфейс.

До складу комплексу «Гриф-Мережа» входять:

- засоби розмежування доступу та реєстрації даних аудита, які встановлюються на робочих станціях та файлових серверах ЛОМ;
- автоматизоване робоче місце (АРМ) адміністратора засобів захисту. Основні функції: реєстрація користувачів, вироблення даних ідентифікації та автентифікації із збереженням їх на носії даних автентифікації; реєстрація ресурсів, які підлягають захисту; керування розмежуванням доступу користувачів до вибраних каталогів; контроль цілісності та самотестування КЗЗ за запитом адміністратора; керування розмежуванням доступу прикладних програм до вибраних каталогів; керування квотами користувачів; встановлення контролю програмного забезпечення (заборона запуску незареєстрованих програм);

- АРМ аналізу локальних даних аудита. Основні функції: перегляд, аналіз та обробка протоколів аудита; робота з архівом даних аудита;
- АРМ адміністратора безпеки (використовується в конфігурації для умов з підвищеними вимогами до забезпечення спостережності). Основні функції: налаштування та керування параметрами аудиту захищених ресурсів; керування параметрами сповіщення та приймання сповіщень про критичні для безпеки події в реальному режимі часу; перегляд, аналіз та обробка протоколів аудита; робота з архівом даних аудита.

В термінах НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» комплекс «Гриф-Мережа» реалізує такі функціональні профілі захищеності.

Функціональний профіль захищеності, який реалізує комплекс «Гриф-Мережа» в базовій конфігурації:

{КА-2, КО-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-2, НИ-3, НК-1, НО-2, НЦ-2, НТ-2}

Функціональний профіль захищеності, який реалізує комплекс «Гриф-Мережа» в конфігурації для умов з підвищеними вимогами до забезпечення спостережності:

{КА-2, КО-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-5, НИ-3, НК-1, НО-2, НЦ-2, НТ-2}

Розробка комплексу виконана у відповідності з вимогами до рівня гарантій Г-4 коректності реалізації функціональних послуг безпеки. Відповідно до експертного висновку, зареєстрованого в Адміністрації Держспецзв'язку 24.10.2019 за № 1034, реалізовані функціональні профілі захищеності, політика функціональних послуг безпеки та рівень гарантій відповідають вимогам НД ТЗІ 2.5-008-2002 «Вимоги щодо захисту службової інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2» та НД ТЗІ 2.4-015-2018, при цьому комплекс «Гриф-Мережа» без обмежень може використовуватись для захисту: інформації, що становить державну таємницю; службової інформації; таємної інформації, що не становить державну таємницю; конфіденційної інформації, яка знаходиться у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України «Про доступ до публічної інформації»; іншої інформації з обмеженим доступом, необхідність захисту якої встановлена законом; конфіденційної інформації фізичних та юридичних осіб.

Порівняння послуг безпеки ФПЗ механізмів захисту ОС і КЗЗ

№	Комплекс засобів захисту	**ФПЗ АС-2**	**Microsoft Windows Server 2019 Datacenter**	**ЛОЗА-2 версія 3**	**Гриф-Мережа версія 3**
1	рівень гарантій	**Г2**	Г2	Г4	Г4
2	мінім./ базова адміністративна конфіденційність	**КА-2**	-	КА-2	КА-2
3	базова довірча конфіденційність	**КД-2**	КД-2	КД-2	-
4	повторне використання об’єктів	**КО-1**	КО-1	КО-1	КО-1
5	мінімальна адміністративна цілісність	**ЦА-2**	-	ЦА-1	ЦА-2
6	мінімальна довірча цілісність	**ЦД-1**	ЦД-1	ЦД-1	-
7	обмежений відкат	**ЦО-1**	ЦО-1	-	ЦО-1
8	використання ресурсів - квота	**ДР-1**	ДР-1	-	ДР-1
9	стійкість при обмежених відмовах	**ДС-1**	ДС-1	ДС-1	ДС-1
10	модернізація	**ДЗ-1**	ДЗ-2	ДЗ-1	ДЗ-1
11	ручне відновлення	**ДВ-1**	ДВ-2	ДВ-1	ДВ-1
	захищений журнал	**НР-2**	НР-2	НР-4	НР-2
12	один. / множинна ідентифікація і автентифікація	**НИ-2**	НИ-2	НИ-2	НИ-3
13	однонаправлений достовірний канал	**НК-1**	НК-1	НК-1	НК-1
14	розподіл обов'язків на підставі привілеїв / розподіл обов'язків адміністратора	**НО-2**	НО-3	НО-2	НО-2
15	КЗЗ з гарантованою цілісністю / контролем цілісності	**НЦ-2**	НЦ-2	НЦ-2	НЦ-2
16	самотестування при старті	**НТ-2**	НТ-2	НТ-2	НТ-2

Здійснивши порівняльний аналіз послуг безпеки ФПЗ механізмів захисту ОС і вище зазначених КЗЗ, можна зробити висновок, що з урахуванням послуг безпеки ОС «Гриф-Мережа» забезпечує визначений ФПЗ АС-2 у повному обсязі (в першу чергу, КА-2 і ЦА-2). КЗЗ «ЛОЗА-2» у даному випадку не забезпечує послугу ЦА-2.

3. Системи захисту Web-ресурсів від НСД

3.1. Система «Захищена електронна пошта «Бриз»

Система «Захищена електронна пошта «Бриз» (далі – пошта «Бриз») призначена для забезпечення автоматизації обміну повідомленнями між користувачами пошти або віддаленими компонентами інформаційних систем (наприклад, компонентами систем електронного документообігу різних підприємств) з використанням розподілених мереж передачі даних довільного типу, яких підтримується стек протоколів TCP/IP, а також обробки повідомлень, що містять як відкриту інформацію, яка потребує захисту (відкриту інформацію, яка не є власністю держави, і відкриту інформацію, що є власністю держави), так і інформацію з обмеженим доступом (персональні дані, конфіденційну інформацію , що не є власністю держави, та конфіденційну інформацію, що є власністю держави), із забезпеченням безперервного захисту оброблюваних та збережених на робочих станціях (РС) клієнтів повідомлень.

До складу програмних засобів пошти "Бриз" в загальному випадку входять:

- програмні засоби серверів центрального та регіональних вузлів (доменів) пошти, що функціонують на серверах центрального або регіональних вузлів та взаємодіють між собою по каналах розподіленої мережі передачі даних;
- програмні засоби автоматизованих робочих місць (АРМ) адміністраторів вузлів пошти, що функціонують на РС адміністраторів вузлів та взаємодіють з програмними засобами серверів вузлів пошти каналами локальних обчислювальних мереж;
- програмні засоби АРМ клієнтів пошти, що функціонують на РС клієнтів та взаємодіють із програмними засобами серверів вузлів по каналах локальних обчислювальних мереж або каналів розподіленої мережі передачі даних.

З метою забезпечення надійного обміну повідомленнями між користувачами (клієнтами) пошти або віддаленими компонентами інформаційних систем, а також для забезпечення ефективної роботи клієнтів пошти та в системі Бриз реалізовані:

- можливість створення в АРМ адміністратора/ клієнта та передачі повідомлень у вигляді сукупності текстової частини (об'ємом до 64 Кбайт) та приєднаних файлів довільного типу (до 256 файлів в одному повідомленні);
- можливість передачі повідомлень з АРМ адміністраторів/ клієнтів в електронну пошту Internet та можливість прийому в АРМ адміністраторів/ клієнтів повідомлень із пошти Internet (шлюзування повідомлень виконується на сервері вузла пошти);

- пріоритетне відправлення повідомлень з АРМ адміністраторів/ клієнтів (підтримується п'ять рівнів пріоритетів, повідомлення з максимальним пріоритетом передаються в першу чергу);
- ведення архівів усіх оброблених в АРМ адміністратора/ клієнта повідомлень з можливістю пошуку та перегляду відповідних повідомлень;
- гнучка можливість групування відправлених/прийнятих повідомлень у реєстрах повідомлень АРМ адміністратора/ клієнта з можливістю сортування та пошуку повідомлень за їх реквізитами;
- можливість передачі повідомлень з АРМ адміністратора/ клієнта як одному одержувачу, так і групі одержувачів за сформованим та збереженим у спеціальному довіднику списку розсилки;
- можливість формування списків розсилки як безпосередньо в АРМ відповідного клієнта, так і в АРМ адміністратора вузла пошти з подальшим пересиланням в АРМ клієнта;
- оповіщення відправника про факт доставки/недоставки повідомлення одержувачу шляхом автоматичного формування та доставки відправнику відповідної квитанції при обробці повідомлення в АРМ клієнта - одержувача;
- можливість ведення адміністратором вузла пошти загальної та індивідуальних адресних книг користувачів вузла з автоматичним розсиланням змінених адресних книг на сервер вузла пошти та в АРМ клієнтів;
- можливість віддаленого управління адміністратором вузла пошти параметрами конфігурації АРМ клієнтів вузла (дозвіл самостійного налаштування параметрів захисту, виконання лише захищеної передачі повідомлень, використання адрес одержувачів лише з адресної книги тощо);
- можливість автоматичного архівування повідомлень, що передаються з АРМ адміністратора/ клієнта, що істотно знижує навантаження на використовувані канали передачі даних і скорочує час передачі/приймання повідомлень;
- автоматичне виявлення в АРМ адміністратора/ клієнта фактів дублювання прийнятих повідомлень з метою захисту від повторного прийому та обробки таких повідомлень;
- автоматична (за гнучко налаштованим правилам) передача між АРМ клієнтів повідомлень, представлених у вигляді файлів довільного типу, що дозволяє без втручання операторів здійснювати обмін даними між компонентами розподілених інформаційних систем;

- автоматичне відновлення передачі даних у разі обриву з'єднання з «докачуванням» даних з точки обриву, що знижує вимоги до якості каналів передачі даних, що використовуються, і дозволяє передавати повідомлення великого розміру (сотні мегабайт);
- управління передачею службових повідомлень інфраструктури відкритих ключів (запитів на отримання сертифікатів, запитів на блокування/відкликання/відновлення сертифікатів, запитів про статус сертифікатів), а також прийомом та опрацюванням відповідей на них;
- надання пріоритету обробки (маршрутизації) повідомлень на серверах вузлів пошти (підтримується п'ять рівнів пріоритетів, повідомлення з максимальним пріоритетом маршрутизуються одержувачам насамперед);
- ведення архівів усіх оброблених сервером вузла пошти повідомлень з можливістю виконання адміністратором вузла ЗЕП пошуку повідомлень в архіві та повторного надсилання повідомлень одержувачам;
- можливість віддаленого керування адміністратором вузла пошти параметрами конфігурації сервера вузла (тимчасовими параметрами циклів маршрутизації повідомлень з різним пріоритетом, тимчасовими параметрами контролю за працездатністю сервера, параметрами керування взаємодією з серверами інших вузлів пошти, параметрами взаємодії з серверами електронної пошти Internet тощо);
- протоколювання всіх подій щодо обробки повідомлень на сервері вузла пошти та в АРМ адміністратора/ клієнта з можливістю перегляду та аналізу відповідних протоколів адміністратором вузла пошти або уповноваженими користувачами;
- автоматичний контроль (відповідно до заданих адміністраторів вузла пошти параметрів) працездатності сервера вузла з перезапуском модулів сервера, що втратили працездатність, або повним перезапуском сервера у разі його порушення працездатності. З метою забезпечення надійного захисту пошти, що передаються між користувачами (клієнтами) або адміністраторів/ клієнтів повідомлень, що зберігаються в реєстрах АРМ, в системі «Бриз» реалізовані:
- ідентифікація та аутентифікація користувачів АРМ адміністратора/ клієнта на підставі атрибутів, одержуваних від операційної системи, при запуску відповідного АРМ, що дозволяє заблокувати можливість використання АРМ адміністратора/ клієнта сторонньою особою, а також упізнати конкретного легального користувача та надалі реагувати на запити з його повноваженнями;

- зашифровування/розшифрування переданих/прийманих повідомлень за алгоритмом гамування зі зворотним зв'язком, встановленому ГОСТ 28147-89, що забезпечує захист від несанкціонованого ознайомлення зі змістом повідомлень на всьому шляху їх від відправника до одержувача (криптографічні перетворення реалізуються з використанням бібліотеки процедур криптограф Тайфун-PKI PKCS#11»);
- вироблення/перевірка електронного цифрового підпису (ЕЦП) переданих/прийманих/ збережених у реєстрах АРМ адміністратора/ клієнта повідомлень за алгоритмами, встановленими ДСТУ 4145-89 та ГОСТ 34.310-95, що забезпечує виявлення фактів порушення цілісності повідомлень, а також підтвердження) відправників – авторів повідомлень (криптографічні перетворення реалізуються за допомогою бібліотеки процедур криптографічного захисту інформації «Тайфун-PKI PKCS#11»);
- вироблення/перевірка ЕЦП переданих/прийманих/ збережених у реєстрах АРМ адміністратора/ клієнта квитанцій про отримання повідомлень, що забезпечує виявлення фактів порушення цілісності квитанцій, а також підтвердження причетності (автентифікацію) одержувачів повідомлень;
- можливість використання для зберігання особистих ключів користувачів системи як незахищених (дискета, flash-drive тощо), і захищених (пристрою eToken, SecureToken, смарт-карти тощо) носіїв.

Для створення особистих ключів користувачів системи «Бриз», а також для управління сертифікатами відкритих ключів користувачів системи використовуються компоненти комплексу реалізації інфраструктури відкритих ключів «Тайфун-PKI».

Згідно з експертним висновком № 139 від 31.07.2008 р., зареєстрованим Адміністрацією Державної служби спеціального зв'язку та захисту інформації України, до системи ЗЕП «Бриз» реалізує (у термінах НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності комп'ютерних систем від несанкціонованого доступу»)) наступний функціональний профіль захищеності:
{КВ-2, ЦВ-2, ДС-1, ДЗ-1, ДВ-1, НР-2, НД-1, АЛЕ-2, НЦ-1, НТ-2, НА-2 , НП-2}.

Зазначений функціональний профіль захищеності реалізовано відповідно до вимог до рівня гарантій Г-4 коректності реалізації функціональних послуг безпеки, встановленого НД ТЗІ 2.5-004-99.

Програмні засоби пошти Бриз забезпечують передачу повідомлень через мережі передачі даних довільного типу, в яких підтримується стек протоколів TCP/IP. Налаштування активного мережного обладнання, що використовується в мережі передачі даних, повинні дозволяти можливість передачі даних між АРМ

адміністраторів/клієнтів і серверами вузлів пошти, а також між серверами вузлів пошти з використанням протоколу FTP. Програмні засоби АРМ клієнта/адміністратора функціонують на IBM-сумісних комп'ютерах під керуванням ОС MS Windows 2000/XP/Vista. Програмні засоби сервера вузла пошти функціонують на IBM-сумісних комп'ютерах під керуванням Windows 2000/2003/2008. Мінімальні вимоги до конфігурації комп'ютерів для забезпечення стійкої роботи системи визначаються вимогами відповідних ОС, а також наявністю жорстких дисків, обсяг яких достатній для збереження архів пошти та/або АРМ адміністратора/ клієнта пошти.

3.2. Комплекс програмних засобів реалізації інфраструктури відкритих ключів “Тайфун-РКІ”

Комплекс програмних засобів реалізації інфраструктури відкритих ключів “Тайфун-РКІ” версії 1.02 містить процедури, призначені для забезпечення захисту цілісності та конфіденційности інформації, автентифікації відправників повідомлень (авторів документів) з використанням механізмів криптографічного захисту (електронний цифровий підпис, шифрування, вироблення імітовставок та геш-функцій) шляхом вбудовування в конкретні прикладні системи, які функціонують на ПЕОМ з операційними системами Windows XP/Server 2003/7/8.1/10/Server 2008 R2/Server 2012 R2/Server 2016 (як 32-розрядними, так і 64-розрядними).

Бібліотека "Тайфун-PKI PKCS#11"версії 1.02 реалізована у вигляді динамічної бібліотеки у відповідності з вимогами стандарту PKCS#11 і підтримує специфікації інтерфейсу прикладного програмування (API), встановлені версією 2.20 вказаного стандарту (RSA Laboratories. PKCS#11 v2.20: Cryptographic Token Interface Standard).

Процедури, які входять до складу бібліотеки "Тайфун-PKI PKCS#11", реалізують:

- шифрування/розшифрування даних по алгоритму, встановленому ДСТУ ГОСТ 28147:2009;
- вироблення/перевірку імітовставки по алгоритму, встановленному ДСТУ ГОСТ 28147:2009;
- вироблення/перевірку електронного цифрового підпису (ЕЦП) по алгоритмам, встановленим ДСТУ 4145-2002, ГОСТ 34.311-95;
- вираболення ключів шифрування по схемі Діффі-Хеллмана по протоколам узгодження ключів, які (протоколи) визначені діючими в Україні нормативними документами системи криптографічного захисту інформації;

- кодування/ декодування інформаційних та службових повідомлень (сертифікатів відкритих ключів, списків відозваних сертифікатів, даних з ЕЦП, повідомлень протоколу фіксації часу, повідомлень протоколу визначення статусу сертифіката, криптографічних повідомлень) у форматах, які визначені діючими в Україні нормативними документами системи криптографічного захисту інформації.

Відповідно до експертного висновку№ 04/03/02-690 від 12.03.2019 р., виданому Державною службою спеціального зв'язку та захисту інформації України, бібліотека процедур криптографічного захисту інформації «Тайфун-PKI PKCS#11» версії 1.02 може використовуватись:

- як засіб вироблення ключів та засіб шифрування даних - для криптографічного захисту відкритї інформації та інформації з обмеженим доступом (крім службової інформації та інформації, що становить державну таємницю);
- як засіб вироблення/ перевірки ЕЦП даних - для криптографічного захисту відкритої інформації та інформації з обмеженим доступом (в том числі службової інформації та інформації, що становить державну таємницю).

Бібліотека процедур криптографічного захисту інформації «Тайфун-PKI PKCS#11» версії 1.02 випускається серійно відповідно до технічного завдання, погодженого з Адміністрацією Держспецзв'язку.

В комплект постачання бібліотеки «Тайфун-PKI PKCS#11» версії 1.02 входять:

- файли виконуваного коду бібліотеки;
- файл ліцензії;
- настанова програмісту в електронному вигляді;
- вихідні тексти прикладу використання бібліотеки (на мові програмування C).

Порівняння послуг безпеки ФПЗ механізмів захисту ОС і КЗЗ

№	Комплекс засобів захисту	**ФПЗ WEB**	**Microsoft Windows Server 2019 Datacenter**	**Портал Менеджер 1.0**	**Тайфун-Web версія 1**
1	рівень гарантій	**Г2**	Г2	Г2	Г4
2	мінім./ базова адміністративна конфіденційність	**КА-2**	-	КА-2	КА-2
3	базова довірча конфіденційність	**КД-2**	КД-2	-	-
4	мінімальна / базова конфіденційність при обміні	**КВ-1**	КВ-1	-	КВ-2
5	мінімальна адміністративна цілісність	**ЦА-1**	-	ЦА-1	ЦА-1
6	обмежений відкат	**ЦО-1**	ЦО-1	-	ЦО-1
7	мінімальна / базова цілісність при обміні	**ЦВ-1**	ЦВ-1	-	ЦВ-2
8	використання ресурсів - квота	**ДР-1**	ДР-1	-	-
9	ручне відновлення	**ДВ-1**	ДВ-2	ДВ-1	ДВ-1
10	захищений журнал	**НР-2**	НР-2	НР-2	НР-1
11	один. / множинна ідентифікація і автентифікація	**НИ-2**	НИ-2	НИ-2	НИ-1
12	однонаправлений достовірний канал	**НК-1**	НК-1	НК-1	-
13	розподіл обов'язків на підставі привілеїв / виділення адміністратора	**НО-1**	НО-3	НО-2	НО-1
14	КЗЗ з гарантованою цілісністю / контролем цілісності	**НЦ-1**	НЦ-2	НЦ-1	НЦ-1
15	самотестування при старті	**НТ-1**	НТ-2	НТ-2	НТ-2
16	автентифікація вузла / джерела даних	**НВ-1**	НВ-1	НВ-1	НВ-2

Здійснивши порівняльний аналіз послуг безпеки ФПЗ механізмів захисту ОС і вище зазначених КЗЗ, можна зробити висновок, що з урахуванням послуг безпеки ОС і «Портал Менеджер», і «Тайфун-Web» забезпечує визначений ФПЗ WEB-сайту (в першу чергу, КА-2 і ЦА-1). У такому випадку вибір КЗЗ залежить від його ціни та якості сервісного обслуговування.

При цьому треба зазначити, що КЗЗ «Тайфун-Web» забезпечує більш надійний захист WEB-сайту, оскільки у порівнянні з КЗЗ «Портал Менеджер» виконує додатково такі послуги безпеки, як «базова конфіденційність при обміні» (КВ-2), «обмежений відкат» (ЦО-1) і «базова цілісність при обміні» (ЦВ-2).

Контрольні питання:

1. Які КЗЗ від НСД можна використати в ІТС класу 1?
2. Які КЗЗ від НСД можна використати в ІТС класу 2?
3. Які КЗЗ від НСД можна використати для захисту WEB-сайту?
4. Який КЗЗ від НСД може працювати спільно з комплексом ТЗІ?
5. Який КЗЗ від НСД працює тільки в середовищі Windows 2000/XP?
6. Які конфігурації має КЗЗ «ЛОЗА»?
7. Чим конфігурація «Підвищена безпека» КЗЗ «ЛОЗА» відрізняється від «Стандартної безпеки»?
8. Яку послугу безпеки в КЗЗ «ЛОЗА» забезпечує ключовий диск?
9. Які конфігурації має КЗЗ «ГРИФ» версії 4?
10. Чим конфігурація для умов з підвищеними вимогами до забезпечення спостережності КЗЗ «ГРИФ» відрізняється від базової конфігурації?
11. Яка головна відмінність КЗЗ «Тайфун-Web» від КЗЗ «Портал Менеджер»?

СПИСОК ЛІТЕРАТУРИ

[1] Захист інформації в автоматизованих системах управління : навчальний посібник / Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226 с

[2] Комплексні системи захисту інформації : навчальний посібник / Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В. – Вінниця : ВНТУ, 2018. – 118 с.

[3] Логінова Н. І. Правовий захист інформації : навчальний посібник / Н. І. Логінова, Р. Р. Дробожур. – Одеса : Фенікс, 2015. – 264 с., іл.

[4] Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник / В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін. – Київ. : ДУТ-КНУ, 2016. – 178 с.

[5] Яремчук Ю. Є. Дослідження комбінаційних характеристик вітчизняних радіонепрозорих тканин М1, М2 та М3 / Ю. Є. Яремчук, В. С. Катаєв, В. В. Сінюгін // Реєстрація, зберігання та обробка даних. – 2015. – Том 17. № 3 – С. 56–65

[6] НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

[7] НД ТЗІ 2.1-002-07 Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення.

[8] НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі».

[9] НД ТЗІ 2.7-011-2012 «Захист інформації на об’єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв».

[10] ДСТУ 3396.2-97 «Захист інформації. Технічний захист інформації. Терміни та визначення».

[11] НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу».

[12] Закон України «Про телекомунікації» (Відомості Верховної Ради України ВВР, 2004, №12, ст..155).

[13] Закон України „Про захист інформації в інформаційно-телекомунікаційних системах” (Відомості Верховної Ради України (ВВР), 1994, N 31, ст.286).

[14] НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі».

Навчальне видання

ХЛАПОНІН Юрій Іванович

КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Конспект лекцій

Редагування та коректура *М.М. Власенко*
Комп’ютерне верстання *М.М. Власенко*

Підписано до друку 05.05.2022 Формат 60 х 84 1/ 16
Ум. друк. арк. 4,88 Обл.-вид. арк. 3,79
Електронний документ. Вид. № 10/І-16 Зам. 40/1-16

Видавець і виготовлювач
Київський національний університет будівництва і архітектури

Повітрофлотський проспект, 31, Київ, Україна, 03680
Свідоцтво про внесення до Державного реєстру суб’єктів
видавничої справи ДК № 808 від 13.02.2002 р.