Міністерство освіти і науки України
Вінницький національний технічний університет

КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Навчальний посібник

Вінниця
ВНТУ
2018

УДК 004.056(075.8)
К63

Автори:
Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.

Рекомендовано до друку Вченою радою Вінницького національного технічного університету Міністерства освіти і науки України (протокол № 15 від 25.05.2017 р.)

Рецензенти:
В. О. Хорошко, доктор технічних наук, професор
С. І. Перевозніков, доктор технічних наук, професор
М. І. Прокофьєв, кандидат технічних наук

Комплексні системи захисту інформації : навчальний посібник / К63 [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця : ВНТУ, 2018. – 118 с.

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

УДК 004.056(075.8)

ЗМІСТ

ВСТУП

Науково-технічна революція останнім часом прийняла грандіозні масштаби в області 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 обхвату в рамках єдиних технологій процесів збору, передачі, накопичення, зберігання, пошуку, переробки інформації і видачі її для використання. Іншими словами, людство приступило до реалізації 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-якому вигляді 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 (включаючи найдрібніші), які не були б озброєні сучасними засобами обробки і передачі інформації. У ЕОМ на носіях даних накопичуються значні обсяги інформації, часто носить конфіденційний характер або становить велику цінність для її власника.

В даний час характерними і типовими стають такі особливості використання обчислювальної техніки:

– зростаючий 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;

– збільшується концентрація в автоматизованих системах обробки даних (АС) інформаційно-обчислювальних ресурсів;

– велика 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 приналежності;

– 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 і встановленого статусу використання інформації, що циркулює і обробляється в інформаційно-обчислювальних установках, центрах, системах і мережах або коротко - в автоматизованих системах обробки даних (АС). Дана проблема увійшла в побут під назвою проблеми захисту інформації або забезпеченням безпеки інформації.

Определеніе1. Інформаційною безпекою називають заходи із захисту інформації від несанкціонованого доступу, руйнування, модифікації, розкриття і затримок у доступі.

Інформаційна безпека включає в себе заходи по захисту процесів створення даних, їх введення, обробки і виводу. Метою інформаційної безпеки є убезпечити цінності системи, захистити і гарантувати точність і цілісність інформації, і мінімізувати руйнування, які можуть 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 наступні 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 проблема захисту інформації вирішувалася досить ефективно застосуванням в основному організаційних заходів. До них ставилися передусім режимні заходи, охорона, сигналізація і найпростіші програмні засоби захисту інформації. Ефективність використання зазначених коштів досягалася за рахунок концентрації інформації на обчислювальних центрах, як правило автономних, що сприяло забезпеченню захисту відносно малими засобами.

"Розподіленням" 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 видобутку 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 складним, що вимагає для свого рішення не просто здійснення деякою сукупністю наукових, науково-технічних і організаційних заходів та застосування специфічних засобів і методів, а створення цілісної системи організаційних заходів та застосування специфічних засобів і методів із захисту інформації.

Координація робіт по 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 із 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 характерний спрощеним підходом до самої проблеми, породженим переконанням, що вже сам факт представлення інформації в ЕОМ у закодованому вигляді та обробкою її за специфічними алгоритмами вже є серйозним захисним засобом, а тому цілком достатньо включити 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 прийшли до висновку про те, що для захисту інформації потрібна деяка цілком організована система з своїм керуючим 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 у весь час функціонування АС, хоча істотно підвищилася увага до організаційних заходів.

Викладений підхід був характерний і для другого етапу. Однак порушення безпеки інформації неухильно росли, що викликало серйозну стурбованість, оскільки могло стати серйозною перешкодою на шляху впровадження обчислювальної техніки. Посилені пошуки виходу з такої майже кризової ситуації привели до висновку, що захисту інформації в сучасних АС є не одноразова акція, а безперервний процес, цілеспрямовано здійснюваний під весь час створення і функціонування систем з комплексним застосуванням всіх наявних засобів, методів і заходів. Формування цього висновку і знаменувало початок третього етапу в розвитку підходів до захисту інформації, який здійснюється в даний час.

Так у найзагальніших рисах може бути охарактеризоване істота 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 наступні 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 установа (закладу, відомства), розташованих на певній території;

По-третє, системність тимчасова, що означає безперервність робіт із захисту інформації, здійснюваних за взаємопов'язані планам;

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 стрункої системи органів, професійно орієнтованих на захист інформації, несуть повну відповідальність за оптимальну організацію надійного захисту інформації в усіх АС і володіє для цього необхідними повноваженнями. 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 обгрунтованих 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 і 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, мети 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.

РОЗДІЛ 1 ЗАГАЛЬНІ ПОЛОЖЕННЯ ПРО КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Комплексні системи захисту інформації (КСЗІ) представляють собою сукупність організаційних та інженерно-технічних заходів, спрямованих на забезпечення захисту інформації від розголошення, витоку і несанкціонованого доступу.

Організаційні заходи є обов'язковою складовою побудови КСЗІ.

Інженерно-технічні заходи здійснюються в міру необхідності.

1.1 Визначення, позначення та скорочення

Технічний захист інформації (ТЗІ) – діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації.

Система ТЗІ – сукупність суб'єктів, об'єднаних цілями та завданнями захисту інформації інженерно-технічними заходами, нормативно-правова та їхня матеріально-технічна база.

Контрольована зона - територія, на якій унеможливлюється несанкціоноване перебування сторонніх осіб.

Модель загроз – формалізований опис методів та засобів здійснення загроз для інформації.

Інформаційна система - автоматизована система, комп'ютерна мережа або система зв'язку.

Виділені приміщення - приміщення, в яких циркулює інформація з обмеженим доступом.

Контрольно-інспекційна робота з питань ТЗІ – діяльність, спрямована на визначення та вдосконалення стану ТЗІ органів, щодо яких здійснюється ТЗІ, та на проведення контролю за виконанням суб'єктами системи ТЗІ завдань або проведенням діяльності в галузі ТЗІ за відповідними дозволами та ліцензіями.

Атестація виділених приміщень – комплекс спрямованих на реалізацію заходів з ТЗІ робіт, метою яких є приведення виділених приміщень у відповідність до вимог нормативних документів з ТЗІ та визначення відповідності захищеності виділеного приміщення встановленій категорії.

Порушення з ТЗІ – невиконання вимог нормативно-правових актів з питань ТЗІ, яке створює умови або реальну можливість порушення конфіденційності, цілісності або доступності інформації.

Інші терміни використовуються згідно з:

– НД ТЗІ 1.1–003–99 “Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу”;

– ДСТУ 3396.2 “Захист інформації. Технічний захист інформації. Терміни та визначення”;

– “Термінологічний довідник з технічного захисту інформації на об’єктах інформаційної діяльності”.

Позначення і скорочення:

БД - база даних;

ДТЗ - допоміжні технічні засоби

ЕОМ – електронно-обчислювальна машина;

ІД - інформаційна діяльність;

ІзОД - інформація з обмеженим доступом;

ІТС – інформаційно-телекомунікаційна система;

КЗЗ - комплекс засобів захисту;

КРТ - копіювально-розмножувальна техніка;

КС - комп’ютерна система;

КСЗІ - комплексна система захисту інформації;

НД - нормативний документ;

НД ТЗІ - нормативний документ системи технічного захисту інформації;

НСД - несанкціонований доступ;

ОС - обчислювальна система;

ОТЗ - основні технічні засоби;

ПЗІ - підрозділ захисту інформації;

ПЕМВН — побічні електромагнітні випромінювання і наведення;

ПЗ - програмне забезпечення;

ПЗП - постійний запам’ятовуючий пристрій;

ПРД - правила розмежування доступу;

ПМА - програми та методики атестації;

ТЗІ - технічний захист інформації.

1.2 Сутність та задачі комплексної системи захисту інформації

1.2.1 Основні підходи до створення комплексної системи захисту інформації

Існує думка, що проблеми захисту інформації відносяться виключно до інформації, що обробляється комп'ютером. Це, мабуть, пов'язано з тим, що комп'ютер, і зокрема персональний комп'ютер, є «ядром», центром зберігання інформації. Об'єкт інформатизації, по відношенню до якого спрямовані дії щодо захисту інформації, видається більш широким поняттям порівняно з персональним комп'ютером.

У реальному житті всі ці окремі «об'єкти інформатизації» розташовані в межах одного підприємства і являють собою єдиний комплекс компонентів, пов'язаних спільними цілями, завданнями, структурними відносинами, технологією інформаційного обміну і т. д.

Сучасне підприємство - велика кількість різнорідних компонентів, об'єднаних в складну систему для виконання поставлених цілей, які в процесі функціонування підприємства можуть модифікуватися.

Різноманіття і складність впливу внутрішніх та зовнішніх чинників, які часто не піддаються суворої кількісної оцінки, призводять до того, що ця складна система може набувати нові якості, не властиві складовим її компонентів.

Характерною особливістю подібних систем є насамперед наявність людини в кожній з яких складається підсистем і віддаленість людини від об'єкта його діяльності. Це відбувається у зв'язку з тим, що безліч компонентів, що складають об'єкт інформатизації, інтегрально може бути представлено сукупністю трьох груп систем: 1) люди (біосоціальні системи); 2) техніка (технічні системи та приміщення, в яких вони розташовані); 3) програмне забезпечення, яке є інтелектуальним посередником між людиною і технікою (інтелектуальні системи). Сукупність цих трьох груп утворює соціотехнічну систему. Таке уявлення про соціотехнічну систему є досить широким і може бути поширене на багато об'єктів. Коло наших інтересів обмежується дослідженням безпеки систем, призначених для обробки вхідної на їх вхід інформації і видачі результату.

Якщо звернутися до історії цієї проблеми, то можна умовно виділити три періоди розвитку засобів захисту інформації (ЗІ):

– перший відноситься до того часу, коли обробка інформації здійснювалася за традиційними (ручним, паперовим) технологій;

– другий - коли для обробки інформації на регулярній основі застосовувалися засоби електронної обчислювальної техніки перших поколінь;

– третій - коли використання засобів електронно-обчислювальної техніки набрав масового і повсюдний характер (поява персональних комп'ютерів).

У 60–70 рр. проблема захисту інформації вирішувалася досить ефективно застосуванням в основному організаційних заходів. До них належали: режимні заходи, охорона, сигналізація і найпростіші програмні засоби захисту інформації. Ефективність використання цих коштів досягалася за рахунок концентрації інформації в певних місцях (спец. сховища, обчислювальні центри), що сприяло забезпеченню захисту відносно малими засобами.

«Розподілення» інформації по місцях зберігання і обробки загострило ситуацію з її захистом. З'явилися дешеві персональні комп'ютери. Це дало можливість побудови мереж ЕОМ (локальних, глобальних, національних і транснаціональних), які можуть використовувати різні канали зв'язку. Ці чинники сприяють створенню високоефективних систем розвідки і отримання інформації. Вони знайшли відображення і в сучасних підприємствах.

Сучасне підприємство являє собою складну систему, в рамках якої здійснюється захист інформації.

Розглянемо основні особливості сучасного підприємства:

– складна організаційна структура;
– багатоаспектність функціонування;
– висока технічна оснащеність;
– широкі зв'язки по кооперації;
– необхідність розширення доступу до інформації;
– зростаюча питома вага цифрової технології обробки інформації;
– зростаючий питома вага автоматизованих процедур в загальному обсязі процесів обробки даних;
– важливість і відповідальність рішень, прийнятих в автоматизованому режимі, на основі автоматизованої обробки інформації;
– висока концентрація в автоматизованих системах інформаційних ресурсів;
– велике територіальне розподілення компонентів автоматизованих систем;
– накопичення на технічних носіях величезних обсягів інформації;
– інтеграція в єдиних базах даних інформації різного призначення і різної приналежності;
– довгострокове зберігання великих обсягів інформації на машинних носіях;
– безпосередній і одночасний доступ до ресурсів (в т.ч. і до інформації) автоматизованих систем великого числа користувачів різних категорій і різних установ;
– інтенсивна циркуляція інформації між компонентами автоматизованих систем, в тому числі і віддалених один від одного.

Таким чином, створення індустрії переробки інформації, з одного боку, створює об'єктивні передумови для підвищення рівня продуктивності праці та життєдіяльності людини, з іншого боку, породжує цілий ряд складних і великомасштабних проблем. Однією з них є забезпечення збереження і встановленого статусу інформації, що циркулює і оброблюваної на підприємстві, організації.

1.2.2 Поняття комплексної системи захисту інформації

Роботи із захисту інформації у нас в країні ведуться досить інтенсивно і вже тривалий час. Накопичено значний досвід. Зараз вже ніхто не думає, що досить провести на підприємстві ряд організаційних заходів, включити до складу автоматизованих систем деякі технічні і програмні засоби - і цього буде достатньо для забезпечення безпеки.

Головний напрямок пошуку нових шляхів захисту інформації полягає не просто в створенні відповідних механізмів, а являє собою реалізацію регулярного процесу, здійснюваного на всіх етапах життєвого циклу систем обробки інформації при комплексному використанні всіх наявних засобів захисту. При цьому всі кошти, методи і заходи, які використовуються для ЗІ, найбільш раціональним чином об'єднуються в

єдиний цілісний механізм – причому не тільки від зловмисників, але і від некомпетентних або недостатньо підготовлених користувачів і персоналу, а також позаштатних ситуацій технічного характеру.

Основною проблемою реалізації систем захисту є:

– з одного боку, забезпечення надійного захисту, що знаходиться в системі інформації: виключення випадкового і навмисного отримання інформації сторонніми особами, розмежування доступу до пристроїв і ресурсів системи всіх користувачів, адміністрації і про обслуговуючого персоналу;

– з іншого боку, системи захисту не повинні створювати помітних незручностей користувачам в ході їх роботи з ресурсами системи.

Проблема забезпечення бажаного рівня захисту інформації досить складна, що вимагає для свого рішення не просто здійснення деякою сукупністю наукових, науково-технічних і організаційних заходів і застосування спеціальних засобів і методів, а створення цілісної системи організаційно-технологічних заходів і застосування комплексу спеціальних засобів і методів по ЗІ .

На основі теоретичних досліджень і практичних робіт в області ЗІ сформульований системно-концептуальний підхід до захисту інформації.

Під системністю як основною частиною системно-концептуального походу розуміється:

– системність цільова, захищеність інформації розглядається як основна частина загального поняття якості інформації;

– системність просторова, яка пропонує взаємопов'язані рішення всіх питань захисту на всіх компонентах підприємства;

– системність тимчасова, що означає безперервність робіт по ЗІ, що здійснюються відповідно до планів;

– системність організаційна, що означає єдність організації всіх робіт по ЗІ і управління ними.

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 цілеспрямованої організації всіх робіт по ЗІ.

Комплексний (системний) підхід до побудови будь-якої системи включає в себе: перш за все, вивчення об'єкта впроваджуваної системи; оцінку загроз безпеки об'єкта; аналіз засобів, якими будемо оперувати при побудові системи; оцінку економічної доцільності; вивчення самої системи, її властивостей, принципів роботи та можливість збільшення її ефективності; співвідношення всіх внутрішніх і зовнішніх чинників; можливість додаткових змін в процесі побудови системи і повну організацію всього процесу від початку до кінця.

Комплексний (системний) підхід – це принцип розгляду проекту, при якому аналізується система в цілому, а не її окремі частини. Його

завданням є оптимізація всієї системи в сукупності, а не поліпшення ефективності окремих частин. Це пояснюється тим, що, як показує практика, поліпшення одних параметрів часто призводить до погіршення інших, тому необхідно намагатися забезпечити баланс протиріч вимог і характеристик.

Комплексний (системний) підхід не рекомендує приступати до створення системи до тих пір, поки не визначені наступні її компоненти:

1. Вхідні елементи. Це ті елементи, для обробки яких створюється система. В якості вхідних елементів виступають види загроз безпеки, можливі на даному об'єкті;

2. Ресурси. Це кошти, які забезпечують створення та функціонування системи (наприклад, матеріальні витрати, енергоспоживання, допустимі розміри і т. Д.). Зазвичай рекомендується чітко визначати види і допустиме споживання кожного виду ресурсу як в процесі створення системи, так і в ході її експлуатації;

3. Навколишнє середовище. Слід пам'ятати, що будь-яка реальна система завжди взаємодіє з іншими системами, кожен об'єкт пов'язаний з іншими об'єктами. Дуже важливо встановити межі області інших систем, які не підкоряються керівнику даного підприємства і не входять в сферу його відповідальності.

Характерним прикладом важливості вирішення цього завдання є розподіл функцій по захисту інформації, переданої сигналами в кабельної лінії, що проходить по територіях різних об'єктів. Як би не встановлювалися кордону системи, не можна ігнорувати її взаємодія з навколишнім середовищем, бо в цьому випадку прийняті рішення можуть виявитися марними.

4. Призначення і функції. Для кожної системи повинна бути сформульована мета, до якої вона (система) прагне. Ця мета може бути описана як призначення системи, як її функція. Чим точніше і конкретніше вказано призначення або перераховані функції системи, тим швидше і правильніше можна вибрати кращий варіант її побудови. Так, наприклад, мета, сформульована в найзагальнішому вигляді як забезпечення безпеки об'єкта, змусить розглядати варіанти створення глобальної системи захисту. Якщо уточнити її, визначивши, наприклад, як забезпечення безпеки інформації, що передається по каналах зв'язку всередині будівлі, то коло можливих рішень істотно звузиться. Слід мати на увазі, що, як правило, глобальна мета досягається через досягнення безлічі менш загальних локальних цілей. Побудова такого «дерева цілей» значно полегшує, прискорює і здешевлює процес створення системи;

5. Критерій ефективності. Необхідно завжди розглядати кілька шляхів, що ведуть до мети, зокрема декількох варіантів побудови системи, що забезпечує задані цілі функціонування. Для того щоб оцінити, який із шляхів краще, необхідно мати інструмент порівняння – критерій ефективності. Він повинен: характеризувати якість реалізації заданих

функцій; враховувати витрати ресурсів, необхідних для виконання функціонального призначення системи; мати ясний і однозначний фізичний зміст; бути пов'язаним з основними характеристиками системи і допускати кількісну оцінку на всіх етапах створення системи.

Таким чином, з огляду на різноманіття потенційних загроз інформації на підприємстві, складність його структури, а також участь людини в технологічному процесі обробки інформації, мети захисту інформації можуть бути досягнуті тільки шляхом створення СЗІ на основі комплексного підходу

1.2.3 Призначення комплексної системи захисту інформації

Головна мета створення системи захисту інформації - її надійність. Система ЗІ - це організована сукупність об'єктів і суб'єктів ЗІ, використовуваних методів і засобів захисту, а також здійснюваних захисних заходів.

Але компоненти ЗІ, з одного боку, є складовою частиною системи, з іншого - самі організовують систему, здійснюючи захисні заходи.

Оскільки система може бути визначена як сукупність взаємопов'язаних елементів, то призначення СЗІ полягає в тому, щоб об'єднати всі складові захисту в єдине ціле, в якому кожен компонент, виконуючи свою функцію, одночасно забезпечує виконання функцій іншими компонентами і пов'язаний з ними логічно і технологічно.

Надійність захисту інформації прямо пропорційна системності. При неузгодженості між собою окремих складових ризик «проколів» в технології захисту збільшується.

По-перше, необхідність комплексних рішень полягає в об'єднанні в одне ціле локальних СЗІ, при цьому вони повинні функціонувати в єдиній «зв'язці». Як локальних СЗІ можуть бути розглянуті, наприклад, види захисту інформації (правова, організаційна, інженерно-технічна).

По-друге, необхідність комплексних рішень обумовлена призначенням самої системи. Система повинна об'єднати логічно і технологічно всі складові захисту. Але з її сфери випадають питання повноти цих складових, вона не враховує всіх факторів, які надають або можуть впливати на якість захисту. Наприклад, система включає в себе якісь об'єкти захисту, а всі вони включені чи ні - це вже поза межами системи.

Тому якість, надійність захисту залежать не тільки від видів складових системи, але і від їх повноти, яка забезпечується при врахуванні всіх чинників і обставин, що впливають на захист. Саме повнота всіх складових системи захисту, що базується на аналізі таких факторів і обставин, є другим призначенням комплексності.

При цьому повинні враховуватися всі параметри уразливості інформації, потенційно можливі загрози її безпеці, охоплюватися всі необхідні об'єкти захисту, використовуватися всі можливі види, методи і

засоби захисту та необхідні для захисту кадрові ресурси, здійснюватися всі виходячи з цілей і завдань захисту заходу.

По-третє, тільки при комплексному підході система може забезпечувати безпеку всієї сукупності інформації, що підлягає захисту, і при будь-яких обставинах. Це означає, що повинні захищатися всі носії інформації, у всіх компонентах її збору, зберігання, передачі і використання, в усі час і при всіх режимах функціонування систем обробки інформації.

У той же час комплексність не виключає, а, навпаки, передбачає диференційований підхід до захисту інформації, в залежності від складу її носіїв, видів таємниці, до яких віднесена інформація, ступеня її конфіденційності, засобів зберігання і обробки, форм і умови прояву уразливості, каналів і методів несанкціонованого доступу до інформації.

Таким чином, значимість комплексного підходу до захисту інформації складається:

– в інтеграції локальних систем захисту;

– в забезпеченні повноти всіх складових системи захисту;

– в забезпеченні всеосяжність захисту інформації.

Виходячи з цього, можна сформулювати наступне визначення:

«Комплексна система захисту інформації – система, повно і всебічно охоплює всі предмети, процеси і фактори, які забезпечують безпеку всієї інформації, що захищається».

1.3 Основні стратегії захисту інформації

Усвідомлення необхідності розробки стратегічних підходів до захисту формувалося в міру усвідомлення важливості, натхнення і проблеми захисту і неможливості ефективного її здійснення простим використанням деякого набору засобів захисту.

Під стратегією взагалі розуміється загальна спрямованість в організації відповідної діяльності, що розробляється з урахуванням об'єктивних потреб в даному виді діяльності, потенційно можливих умов її здійснення і можливостей організації.

Відомий канадський фахівець в області стратегічного управління Г. Мінцберг запропонував визначення стратегії в рамках системи «5-Р». На його думку, вона включає:

1) план (Plan) - заздалегідь намічені в деталях і контрольовані дії на певний термін, що переслідують конкретні цілі;

2) прийом, або тактичний хід (Ploy), що представляє собою короткочасну стратегію, що має обмежені цілі, спроможну змінюватися, маневр з метою використати їх проти противника;

3) модель поведінки (Patten of behaviour) - часто спонтанного, неусвідомленого, що не має конкретних цілей;

4) позицію по відношенню до інших (Position in respect to others);

5) перспективу (Perspective).

Завдання стратегії полягає в створенні конкурентної переваги, усунення негативного ефекту нестабільності навколишнього середовища, забезпеченні прибутковості, врівноваженість зовнішніх вимог і внутрішніх можливостей. Через її призму розглядаються всі ділові ситуації, з якими організація стикається в повсякденному житті.

Здатність компанії, організації проводити самостійну стратегію у всіх областях робить її більш гнучкою, стійкою, дозволяє адаптуватися до вимог часу і обставин.

Стратегія формується під впливом внутрішнього і зовнішнього середовища, постійно розвивається, бо завжди виникає щось нове, на що потрібно реагувати.

Фактори, які можуть мати для фірми вирішальне значення в майбутньому, називаються стратегічними. На думку одного з провідних західних фахівців Б. Карлофа, вони, впливаючи на стратегію будь-якої організації, надають і специфічні властивості. До таких факторів належать:

1) мета, яка відображає філософію фірми, організації її призначення. При перегляді мети, що відбувається в результаті зміни суспільних пріоритетів;

2) конкурентні переваги, якими організація володіє в своїй сфері діяльності в порівнянні з суперниками або до яких прагне (вважається, що вони надають на стратегію найбільший вплив). Конкурентні переваги будь-якого типу забезпечують більш високу ефективність використання ресурсів підприємства;

3) характер продукції, що випускається, особливості її збуту, після продажного обслуговування, ринки та їх межі;

4) організаційні чинники, серед яких виділяється внутрішня структура компанії і її очікувані зміни, система управління, ступінь інтеграції і диференціації внутрішніх процесів;

5) наявні ресурси (матеріальні, фінансові, інформаційні, кадрові та ін.). Чим вони більші, тим масштабніше можуть бути інвестиції в майбутні проекти. Сьогодні для розробки і реалізації стратегії велике значення мають, перш за все, структурні, інформаційні та інтелектуальні ресурси. Порівнюючи значення параметрів готівки і потрібних ресурсів, можна визначити ступінь їх відповідності стратегії;

6) потенціал розвитку організації, вдосконалення діяльності, розширення масштабів, зростання ділової активності, інновацій;

7) культура, філософія, етичні погляди і компетентність управлінців, рівень їх домагань і підприємливості, здатність до лідерства, внутрішній клімат в колективі.

На стратегічний вибір впливають: ризик, на який готова йти фірма; досвід реалізації діючих стратегій, позиції власників, наявність часу.

Розглянемо особливості стратегічних рішень. За ступенем регламентованості вони відносяться до контурним (надають широку

свободу виконавцям в тактичному відношенні), а за ступенем обов'язковості проходження головним установкам – директивним.

За функціональним призначенням такі рішення найчастіше бувають організаційними або розпорядчими спосіб здійснення в певних ситуаціях тих чи інших дій. З точки зору визначеності, це рішення запрограмовані. Вони приймаються в нових, неординарних обставинах, коли необхідні кроки важко заздалегідь точно розписати. З точки зору важливості, стратегічні рішення кардинальні: стосуються основних проблем і напрямків діяльності фірми, визначають основні шляхи розвитку її в цілому, окремих підрозділів або видів діяльності на тривалу перспективу (не менше 5–10 років). Вони випливають насамперед із зовнішніх, а не з внутрішніх умов, повинні враховувати тенденції розвитку ситуації і інтереси безлічі суб'єктів. Практична незворотність стратегічних рішень обумовлює необхідність їх ретельного і всебічної підготовки. Стратегічним рішенням притаманна комплексність. Стратегія зазвичай являє собою не одне, а сукупність взаємопов'язаних рішень, об'єднаних спільною метою, узгоджених між собою за термінами виконання та ресурсів. Такі рішення визначають пріоритети і напрямки розвитку фірми, її потенціалу, ринків, способи реакції на непередбачені події. Практика сформувала наступні вимоги до стратегічних рішень:

1. Реальність, що передбачає її відповідність ситуації, цілям, технічного та економічним потенціалом підприємства, досвіду і навичок працівників і менеджерів, культурі, існуючій системі управління;

2. Логічність, зрозумілість, прийнятність для більшості членів організації, внутрішня цілісність, несуперечність окремих елементів, підтримка ними один одного, що породжує синергетичний ефект;

3. Своєчасність (реалізація рішення повинна встигнути призупинити негативне розвиток ситуації або не дозволити упустити вигоду);

4. Сумісність із середовищем, що забезпечує можливість взаємодії з нею (стратегія перебуває під впливом змін в оточенні підприємства і сама може формувати ці зміни);

5. Спрямованість на формування конкурентних переваг;

6. Збереження свободи тактичного маневру;

7. Усунення причин, а не наслідків існуючої проблеми;

8. Чіткий розподіл за рівнями організації роботи з підготовки та прийняття рішень, а також відповідальності за них конкретних осіб;

9. Облік прихованих і явних, бажаних і небажаних наслідків, які можуть виникнути при реалізації стратегії або відмову від неї для фірми, її партнерів; від існуючого законодавства, етичної сторони справи, допустимого рівня ризику та ін.

Розробка науково обґрунтованої системи стратегій організації як ключової умови її конкурентоспроможності та довгострокового успіху є однією з основних функцій її менеджерів, перш за все вищого рівня. Від них вимагається:

– виділяти, відстежувати і оцінювати ключові проблеми;

– адекватно і оперативно реагувати на зміни всередині і в оточенні організації;

– вибирати оптимальні варіанти дій з урахуванням інтересів основних суб'єктів, причетних до її діяльності;

– створювати сприятливий морально-психологічний клімат, заохочувати підприємницьку і творчу активність низових керівників і персоналу.

Вихідний момент формування стратегії – постановка глобальних якісних цілей і параметрів діяльності, які організація повинна досягти в майбутньому. В результаті ув'язки цілей і ресурсів формуються альтернативні варіанти розвитку, оцінка яких дозволяє вибрати кращу стратегію. Єдиних рецептів вироблення стратегій не існує. В одному випадку доцільно стратегічне планування (програмування) в іншому – ситуаційний підхід.

Виходячи з великої різноманітності умов, при яких може виникнути необхідність захисту інформації, загальна цільова установка на вирішення стратегічних питань полягала в розробці безлічі стратегій захисту, і вибір такого мінімального їх набору, який дозволяв би раціонально забезпечувати необхідний захист в будь-яких умовах.

Відповідно до найбільш реальними варіантами поєднань значень розглянутих факторів виділено три стратегії захисту:

– оборонна – захист від вже відомих загроз здійснювана автономно, т. Е. Без надання істотного впливу на інформаційно-керуючу систему;

– наступальна – захист від усієї множини потенційно можливих загроз, при здійсненні якої в архітектурі інформаційно-керуючої системи і технології її функціонування повинні враховуватися умови, продиктовані потребами захисту;

– упереджувальний – створення інформаційного середовища в якій загрози інформації не мали б умов для прояву.

1.4 Розробка політики безпеки

Перш ніж пропонувати будь-які рішення по організації системи захисту інформації, належить розробити політику безпеки. Політика безпеки – набір законів, правил і практичних рекомендацій, на основі яких будується управління, захист і розподіл критичної інформації в системі. Вона повинна охоплювати всі особливості процесу обробки інформації, визначаючи поведінку системи в різних ситуаціях. Політика безпеки реалізується за допомогою організаційних заходів та програмно-технічних засобів, що визначають архітектуру системи захисту, а також за допомогою засобів управління механізмами захисту. Для конкретної організації політика безпеки повинна бути індивідуальною, залежною від

конкретної технології обробки інформації, використовуваних програмних і технічних засобів, розташування організації і т. Д.

Організаційно політика безпеки визначає порядок подання та використання прав доступу користувачів, а також вимоги звітності користувачів за свої дії в питаннях безпеки. Система захисту інформації виявиться ефективною, якщо вона буде надійно підтримувати виконання правил політики безпеки, і навпаки. Етапи побудови організаційної політики безпеки – це внесення в опис об'єкта структури цінностей і проведення аналізу ризику, і визначення правил для будь-якого процесу користування даним видом доступу до ресурсів об'єкта автоматизації, які мають даний ступінь цінності. Перш за все необхідно скласти детальний опис загальної мети побудови системи безпеки об'єкта, яке виражається через сукупність факторів або критеріїв, уточнюючих мета. Сукупність факторів є базисом для визначення вимог до системи (вибір альтернатив). Фактори безпеки, в свою чергу, можуть поділятися на правові, технологічні, технічні та організаційні.

Розробка політики безпеки організації, як формальної, так і неформальної, – безумовно, нетривіальне завдання. Експерт повинен не тільки володіти відповідними стандартами і добре розбиратися в комплексних підходах до забезпечення захисту інформації організації, але і, наприклад, виявляти детективні здібності при виявленні особливостей побудови інформаційної системи та існуючих заходів по організації захисту інформації. Аналогічна проблема виникає в подальшому при необхідності аналізу відповідності рекомендацій політики безпеки реальному стану речей: необхідно за деяким критерієм відібрати свого роду «контрольні точки» і порівняти їх практичну реалізацію з еталоном, що задається політикою безпеки.

У загальному випадку можна виділити наступні процеси, пов'язані з розробкою і реалізацією політики безпеки.

1. Комплекс заходів, пов'язаних з проведенням аналізу ризиків. До цієї групи можна віднести:

– облік матеріальних або інформаційних цінностей;

– моделювання загроз інформації системи;

– власне аналіз ризиків з використанням того чи іншого підходу – наприклад, вартісний аналіз ризиків.

2. Заходи з оцінки відповідності заходів щодо забезпечення захисту інформації системи деякого еталонному зразку: стандарту, профілем захисту і т. П.

3. Дії, пов'язані з розробкою різного роду документів, зокрема звітів, діаграм, профілів захисту, заданої з безпеки.

4. Дії, пов'язані зі збором, зберіганням і обробкою статистики щодо подій безпеки для організації;

Основу політики безпеки складає спосіб керування доступом, що визначає порядок доступу суб'єктів системи до об'єктів системи. Назва цього способу, як правило, визначає назву політики безпеки.

Для вивчення властивостей способу управління доступом, створюється його формальний опис – математична модель. При цьому модель повинна відображати стан всієї системи, її переходи з одного стану в інший, а також враховувати, які стани і переходи можна вважати безпечними в сенсі даного управління. Без цього говорити про які-небудь властивості системи, і тим більше гарантувати їх, щонайменше некоректно. Відзначимо лише, що для розробки моделей застосовується широкий спектр математичних методів (моделювання, теорії інформації, графів і ін.).

В даний час найкраще вивчені два види політики безпеки: виборча і повноважна, засновані, відповідно, на виборчому і повноважному способах керування доступом.

Крім того, існує набір вимог, що підсилюють дію цих політик і призначений для управління інформаційними потоками в системі. Прямуєте відзначити, що засоби захисту, призначені для реалізації будь-якого з названих способів управління доступом, тільки надають можливості надійного управління доступом або інформаційними потоками.

Основою виборчої політики безпеки є виборче керування доступом, що має на увазі, що

• всі суб'єкти і об'єкти системи повинні бути ідентифіковані;

• права доступу суб'єкта до об'єкта системи визначаються на підставі деякого правила (властивість вибірковості).

Для опису властивостей виборчого управління доступом застосовується модель системи на основі матриці доступу, іноді її називають матрицею контролю доступу. Така модель отримала назву матричної. Матриця доступу являє собою прямокутну матрицю, в якій об'єкту системи відповідає рядок, а суб'єкту стовпець. На перетині шпальти і рядки матриці вказується тип дозволеного доступу суб'єкта до об'єкта. Зазвичай виділяють такі типи доступу суб'єкта до об'єкта, як «доступ на читання», «доступ на запис», «доступ на виконання» і ін.

Безліч об'єктів і типів доступу до них суб'єкта може змінюватися відповідно до деякими правилами, що існують в даній системі. Визначення і зміна цих правил також є завданням матриці доступу.

Рішення на доступ суб'єкта до об'єкта приймається відповідно до типу доступу, зазначеним у відповідній клітинці матриці доступу. Зазвичай виборче управління доступом реалізує принцип «що не дозволено, то заборонено», який передбачає явне дозвіл доступу суб'єкта до об'єкта. Матриця доступу – найбільш простий підхід до моделювання систем доступу.

Виборча політика безпеки найбільш широко застосовується в комерційному секторі, так як її реалізація на практиці відповідає вимогам комерційних організацій щодо розмежування доступу і підзвітності, а також має прийнятну вартість і невеликі накладні витрати.

Основу повноважної політики безпеки складає повноважне управління доступом, що має на увазі, що

– всі суб'єкти і об'єкти системи повинні бути однозначно ідентифіковані;

– кожному об'єкту системи привласнена мітка критичності, що визначає цінність міститься в ньому інформації;

– кожному суб'єкту системи привласнений рівень прозорості, що визначає максимальне значення мітки критичності об'єктів, до яких суб'єкт має доступ.

Коли сукупність міток має однакові значення, кажуть, що вони належать до одного рівня безпеки. Організація міток має ієрархічну структуру, і, таким чином, в системі можна реалізувати ієрархічно висхідний потік інформації (наприклад, від рядових виконавців до керівництва). Чим важливіше об'єкт чи суб'єкт, тим вище його мітка критичності. Тому найбільш захищеними виявляються об'єкти з найбільш високими значеннями мітки критичності.

Кожен суб'єкт крім рівня прозорості має поточне значення рівня безпеки, яке може змінюватися від деякого мінімального значення до значення його рівня прозорості.

Основне призначення повноважною політики безпеки – регулювання доступу суб'єктів системи до об'єктів з різним рівнем критичності і запобігання витоку інформації з верхніх рівнів посадової ієрархії в нижні, а також блокування можливого проникнення з нижніх рівнів в верхні. При цьому вона функціонує на тлі виборчої політики, надаючи її вимогам ієрархічно упорядкований характер (відповідно до рівнів безпеки).

Вибір політики безпеки – це прерогатива керівника системи захисту інформації. Але якою б вона не була, важливо, щоб впроваджена система захисту інформації відповідала ряду вимог, які будуть розглянуті в наступному розділі.

РОЗДІЛ 2 ЗАХОДИ ЗАХИСТУ ІНФОРМАЦІЇ

2.1 Методика визначення складу інформації, що захищається

Визначення складу інформації, що захищається – це перший крок на шляху побудови системи захисту. Від того, наскільки він буде точно виконано, залежить результат функціонування системи, що розробляється. Загальний підхід полягає в тому, що захисту підлягає вся інформація з обмеженим доступом (ІзОД). Інформація, яка становить державну таємницю (секретна інформація), інформація, що становить комерційну таємницю і визначається власником (володільцем) частина відкритої інформації. При цьому ІзОД повинна захищатися від витоку і втрати, а відкрита тільки від втрати.

Часто можна почути думку, що будь-яка відкрита інформація не може бути предметом захисту. Не всі згодні з включенням інформації, віднесеної до державної таємниці, до складу ІзОД.

Тому розглянемо ці питання докладніше.

Захист відкритої (публічної) інформації існував завжди і проводився шляхом реєстрації її носіїв, обліку їх руху і місцезнаходження. Створювалися безпечні умови зберігання. Відкритість інформації не применшує її цінності, а цінна інформація потребує захисту від втрати. Цей захист не повинна бути спрямована на обмеження загальнодоступності інформації. Не може бути відмови в доступі до інформації, але доступ повинен здійснюватися з дотриманням вимог по її збереження відповідно до вимог обробки та використання (наприклад, бібліотека).

Інформація – це характеристика взаємодії повідомлення з користувачем.

Публічна інформація – це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана, або створена в процесі виконання суб’єктами владних повноважень своїх обов’язків, передбачених чинним законодавством, або яка знаходиться у володінні суб’єктів владних повноважень інших розпорядників публічної інформації визначених законом України «Про доступ до публічної інформації».

Інформація з обмеженим доступом поділяється на:

- конфіденційна;
- таємна;
- службова.

Конфіденційна інформація – це та, доступ до якої обмежений фізичною або юридичною особою крім суб’єктів владних повноважень, та яка може поширюватись у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов.

Таємна інформація – це та інформація, доступ до якої обмежується, розголошення якої може завдати шкоду особі, суспільству, державі. Таємною визначається інформація, яка містить державну, професійну, банківську таємницю, таємницю розслідування та іншу передбачену законом таємницю.

До службової може належати така інформація:

1. Що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендацію, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень.

2. Зібрану в процесі оперативно-розшукової контррозвідувальної діяльності у сфері оборони України, яку не віднесено до державної таємниці.

Інформаційна безпека – це стан інформації, в якому забезпечується збереження визначеною політикою безпеки властивостей інформації. Складові інформаційної безпеки, такі як конфіденційність, цілісність, доступність.

Конфіденційність – це властивість не відлягає розголошенню, секретність, суто приватність.

Цілісність – це властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем або процесом. Інформація зберігає цілісність, якщо документуються встановлені правила її модифікації та видалення.

Доступність – це властивість інформаційного ресурсу, що полягає в тому, що користувач або процес, який володіє відповідними повноваженнями може використовувати цей ресурс відповідно до правил, встановлених політикою безпеки.

2.2 Організаційні заходи

Організаційні заходи включають в себе створення концепції інформаційної безпеки, а також:

– складання посадових інструкцій для користувачів та обслуговуючого персоналу;

– створення правил адміністрування компонентів інформаційної системи, обліку, зберігання, розмноження, знищення носіїв інформації, ідентифікації користувачів;

– розробка планів дій у разі виявлення спроби несанкціонованого доступу до інформаційних ресурсів системи, виходу з ладу засобів захисту, виникнення надзвичайної ситуації;

– навчання правилам інформаційної безпеки користувачів.

У разі необхідності, в рамках проведення організаційних заходів може бути створена служба інформаційної безпеки, режимно-пропускний відділ, проведена реорганізація системи діловодства та зберігання документів.

2.3. Інженерно-технічні заходи

Інженерно-технічні заходи – сукупність спеціальних технічних засобів та їх використання для захисту інформації. Вибір інженерно-технічних заходів залежить від рівня захищеності інформації, який необхідно забезпечити.

Інженерно-технічні заходи, що проводяться для захисту інформаційної інфраструктури організації, можуть включати використання захищених підключень, міжмережевих екранів, розмежування потоків інформації між сегментами мережі, використання засобів шифрування і захисту від несанкціонованого доступу.

У разі необхідності, в рамках проведення інженерно-технічних заходів, може здійснюватися установка в приміщеннях систем охоронно-пожежної сигналізації, систем контролю і управління доступом.

Окремі приміщення можуть бути обладнані засобами захисту від витоку акустичної (мовної) інформації.

2.4 Суб'єкти КСЗІ

У процес створення КСЗІ залучаються наступні сторони:

– Організація, для якої здійснюється побудова КСЗІ (Замовник);

– Організація, що здійснює заходи з побудови КСЗІ (Виконавець);

– Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ) (Контролюючий орган);

– Організація, що здійснює державну експертизу КСЗІ (Організатор експертизи);

– Організація, у разі необхідності, залучена Замовником або Виконавцем для виконання деяких робіт зі створення КСЗІ (Підрядник).

2.5 Об'єкти захисту КСЗІ

Захист інформації повинна бути системною, що включає в себе різні взаємопов'язані компоненти. Найважливішим із цих компонентів є об'єкти захисту, бо від їх складу залежать і методи, і засоби захисту, і склад захисних заході.

Інформація є предметом захисту, але захищати її як таку неможливо, оскільки вона не існує сама по собі, а фіксується (відображається) в певних матеріальних об'єктах або пам'яті людей, які виступають в ролі її носіїв і складають основний, базовий об'єкт захисту.

Для запису як секретної, так і несекретної інформації використовуються одні й ті ж носії.

Як правило, носії ІзОД охороняються власником цієї інформації.

Носії інформації, що захищається можна класифікувати як документи; вироби (предмети); речовини і матеріали; електромагнітні, теплові, радіаційні та інші випромінювання; акустичні та інші поля і т. п.

Особливим носієм інформації є людина, мозок якого представляє виключно складну систему, що зберігає і переробну інформацію, що надходить із зовнішнього світу. Властивість мозку відображати і пізнавати зовнішній світ, накопичувати в пам'яті колосальні обсяги інформації ставлять людини на особливе місце як носія інформації. Людина має можливість генерувати нову інформацію. І як носій інформації він володіє позитивними і негативними рисами.

Позитивні – без згоди суб'єкта-носія інформації, що захищається з його пам'яті, як правило, ніяка інформація не може бути вилучено. Він може оцінювати важливість наявної у нього інформації і відповідно до цього звертатися з нею. Він може ранжувати і споживачів інформації, що захищається, знати, кому і яку інформацію він може довірити.

Негативні – він може помилятися щодо істинності споживача інформації, що захищається або навмисне не зберігати довірену йому інформацію: зрада чи просто поширити.

Серед найбільш поширених видів носіїв конфіденційної інформації можна виділити наступні.

Паперові носії, в яких інформація фіксується рукописним, машинописним, електронним, типографським і іншими способами в формі тексту, креслення, схеми, формули.

Магнітні носії: аудіокасети (аудіоплівки) для магнітофонів і диктофонів; відеокасети (відеоплівки) Для відеомагнітофонів та деяких відеокамер; жорсткі (тверді) диски, дискети, магнітні стрічки для ЕОМ. У цих носіях інформація фіксується (наноситься) за допомогою магнітного накопичення (записи сигналів), що здійснюється магнітним пристроєм, а відображається у вигляді символів. Відтворення (зчитування) інформації здійснюється також магнітним пристроєм за допомогою відновлення сигналів.

Магнітооптичні та оптичні носії (лазерні диски, компакт–диски). Запис даних в них виконується лазерним променем (у магнітооптичних і магнітним полем), інформація відображається у вигляді символів, а її зчитування (відтворення) здійснюється за допомогою лазерного променя.

Продукція, що випускається (вироби). Ці вироби виконують своє пряме призначення і одночасно є носіями інформації, що захищається. У цьому випадок інформація відображається у вигляді технічних рішень.

Технологічні процеси виготовлення продукцій які включають в себе як технологію виробництва продукції, так і застосовуються при її виготовленні компоненти (засоби виробництва): обладнання, прилади,

матеріали, речовини, сировину, паливо та ін. Інформація відображається у вигляді технічних процесів (перша складова) і технічних рішень (друга складова).

Фізичні поля, в яких інформація фіксується шляхом зміни їх інтенсивності, кількісних характеристик, відображається у вигляді сигналів, а в електромагнітних полях і в вигляді образів.

Носії ІзОД як об'єкти захисту повинні захищатися, в залежності від їх видів, від несанкціонованого доступу до них, від втрати і від витоку міститься в них інформації.

Але, щоб забезпечити захист, необхідно захищати і об'єкти, які є підступами до носіїв, і їх захист виступає в ролі певних рубежів захисту носіїв. І чим таких рубежів більше, ніж складніше їх подолати, тим надійніше забезпечується захист носіїв.

В якості першого рубежу розглянемо прилеглу до підприємства територію. Деякі підприємства на периметрі встановлюють і пропускний пункт. Прилегла територія захищається від несанкціонованого проникнення осіб до будівель підприємства і відходів виробництва (при наявності відходів). Іншим об'єктом захисту є будівлі підприємства. Їх захист здійснюється тими ж способами і має ту ж мету, що і охорона території. Захист будівель є другим рубежем захисту носіїв.

Наступний об'єкт захисту – приміщення, в яких розташовані сховища носіїв, проводиться обробка носіїв і здійснюється управлінсько-виробнича діяльність з використанням носіїв. До таких приміщень належать:

– приміщення підрозділів захисту інформації, в яких розташовані сховища носіїв і здійснюється обробка носіїв. Ці приміщення повинні бути захищені від несанкціонованого проникнення;

– приміщення, в яких проводиться робота з носіями інформації або протягом робочого дня, або цілодобово: кімнати, в яких працює з носіями персонал; кімнати, в яких проводяться закриті заходи (наради, засідання, семінари та ін.); виробничі ділянки по виготовленню продукції. Ці приміщення повинні захищатися під час перебування в них носіїв від несанкціонованого проникнення, від візуального спостереження за носіями, а також, в разі необхідності, від прослуховування ведуться в них конфіденційних розмов. Захист здійснюється Працюючими в приміщеннях співробітниками, різними технічними засобами, в тому числі в неробочий час засобами охоронної сигналізації.

Ще одним об'єктом захисту є безпосередньо сховища носіїв. Сховища захищаються від несанкціонованого доступу до носіїв. Їх захист здійснюється відповідальними зберігачами, за допомогою замків, а у позаробочий час вони можуть, крім замків захищатися засобами охоронної сигналізації.

Крім того, об'єктами захисту повинні бути:

– засоби відображення, обробки, відтворення і передачі конфіденційної інформації, в тому числі ЕОМ, які повинні захищатися від

несанкціонованого підключення, побічних електромагнітних випромінювань, зараження вірусом, електронних закладок, візуального спостереження, виведення з ладу, порушення режиму роботи; копіювально-розмножувальна техніка, що захищається від візуального спостереження і побічних електромагнітних випромінювань під час обробки інформації; засоби відео- , звукозаписувальної та відтворювальної техніки, які вимагають захисту від прослуховування, візуального спостереження і побічних електромагнітних випромінювань;

– засоби транспортування носіїв конфіденційної інформації, що підлягають захисту від проникнення сторонніх осіб до носіїв або їх знищення під час транспортування;

– засоби радіо- і кабельного зв'язку, радіомовлення і телебачення, які використовуються для передачі конфіденційної інформації, які захищаються від прослуховування, виведення з ладу, порушення режиму роботи;

– системи забезпечення функціонування підприємства (електро-, водопостачання, кондиціонування і ін.) Які повинні захищатися від використання їх для виведення з ладу засобів обробки і передачі інформації прослуховування конфіденційних розмов, візуального спостереження за носіями;

– технічні засоби захисту інформації та контролю за ними, що вимагають захисту від несанкціонованого доступу з метою виведення їх з ладу.

2.6. Основні вимоги до комплексної системи захисту інформації

– Система захисту інформації повинна забезпечувати виконання АС своїх основних функцій без істотного погіршення характеристик останньої.

– Вона повинна бути економічно доцільною, оскільки вартість системи захисту інформації включається у вартість АС.

– Захист інформації в АС повинен забезпечуватися на всіх етапах життєвого циклу, при всіх технологічних режимах обробки інформації, в тому числі при проведенні ремонтних і регламентних робіт.

– В систему захисту інформації повинні бути закладені можливості її вдосконалення і розвитку відповідно до умов експлуатації та конфігурації АС.

– У відповідності до встановлених правил КСЗІ повинна забезпечувати розмежування доступу до ІзОД з відволіканням порушника на помилкову інформацію, тобто мати властивості активного і пасивного захисту.

– При взаємодії захищеної АС з незахищеними АС система захисту повинна забезпечувати дотримання встановлених правил розмежування доступу.

– Система захисту повинна дозволяти проводити облік і розслідування випадків порушення безпеки інформації в АС.

– Застосування системи захисту не повинно погіршувати екологічну обстановку, не бути складною для користувача, не викликати психологічного протидії та бажання обійтися без неї.

2.7. Завдання комплексної системи захисту інформації

Перелік основних завдань, які повинні вирішуватися комплексною системою захисту інформації:

• управління доступом користувачів до ресурсів АС з метою її захисту від неправомірного випадкового або навмисного втручання в роботу системи та несанкціонованого (з перевищенням наданих повноважень) доступу до її інформаційних, програмних і апаратних ресурсів з боку сторонніх осіб, а також осіб з числа персоналу організації та користувачів;

• захист даних, переданих по каналах зв'язку;

• реєстрація, збір, зберігання, обробка і видача відомостей про всі події, що відбуваються в системі і які мають відношення до її безпеки;

• контроль роботи користувачів системи з боку адміністрації та оперативне сповіщення адміністратора безпеки про спроби несанкціонованого доступу до ресурсів системи;

• контроль і підтримку цілісності критичних ресурсів системи захисту та середовища виконання прикладних програм;

• забезпечення замкнутої середовища перевіреного програмного забезпечення з метою захисту від безконтрольного впровадження в систему потенційно небезпечних програм (у яких можуть міститися шкідливі закладку або небезпечні помилки) і засобів подолання системи захисту, а також від впровадження і розповсюдження комп'ютерних вірусів;

• управління засобами системи захисту.

2.8. Основні принципи організації КСЗІ

Захист інформації в АС повинен ґрунтуватися на таких основних принципах:

• системності;

• комплексності;

• безперервності захисту;

• розумної достатності;

• гнучкості управління і застосування;

• відкритості алгоритмів і механізмів захисту;

• простоти застосування захисних заходів і засобів.

2.8.1 Принцип системності

Системний підхід до захисту комп'ютерних систем передбачає необхідність врахування всіх взаємозв'язаних, взаємодіючих і змінюються в часі елементів, умов та факторів, істотно значущих для розуміння і вирішення проблеми забезпечення безпеки АЕС.

При створенні системи захисту необхідно враховувати всі слабкі, найбільш вразливі місця системи обробки інформації, а також характер, можливі об'єкти і напрямки атак на систему з боку порушників (особливо висококваліфікованих зловмисників), шляхи проникнення в розподілені системи і НСД до інформації. Система захисту повинна будуватися з урахуванням не тільки всіх відомих каналів проникнення і НСД до інформації, але і з урахуванням можливості появи принципово нових шляхів реалізації загроз безпеці.

2.8.2 Принцип комплексності

У розпорядженні фахівців з комп'ютерної безпеки є широкий спектр заходів, методів і засобів захисту комп'ютерних систем. Комплексне їх використання передбачає узгоджене застосування різнорідних засобів при побудові цілісної системи захисту, що перекриває всі істотні канали реалізації загроз і не містить слабких місць на стиках окремих її компонентів. Захист повинна будуватися ешелонована. Зовнішня захист повинен забезпечуватися фізичними засобами, організаційними та правовими заходами. Однією з найбільш укріплених ліній оборони покликані бути засоби захисту, реалізовані на рівні операційних систем (ОС) в силу того, що ОС – це якраз та частина комп'ютерної системи, яка управляє використанням всіх її ресурсів. Прикладний рівень захисту, що враховує особливості предметної області, представляє внутрішній рубіж оборони.

2.8.3 Принцип безперервності захисту

Захист інформації – це не разовий захід і навіть не певна сукупність проведених заходів та встановлених засобів захисту, а безперервний цілеспрямований процес, який передбачає прийняття відповідних заходів на всіх етапах життєвого циклу АС, починаючи з самих ранніх стадій проектування, а не тільки на етапі її експлуатації.

Розробка системи захисту повинна вестися паралельно з розробкою самої захищається системи. Це дозволить врахувати вимоги безпеки при проектуванні архітектури і, в кінцевому рахунку, дозволить створити більш ефективні (як за витратами ресурсів, так і по стійкості) захищені системи.

Більшості фізичних і технічних засобів захисту для ефективного виконання своїх функцій необхідна постійна організаційна

(адміністративна) підтримка (своєчасна зміна та забезпечення правильного зберігання та застосування імен, паролів, ключів шифрування, перевищення повноважень тощо). Перерви в роботі засобів захисту можуть бути використані зловмисниками для аналізу застосовуваних методів і засобів захисту, для впровадження спеціальних програмних і апаратних "закладок" та інших засобів подолання системи захисту після відновлення її функціонування.

2.8.4 Розумна достатність

Створити абсолютно неперебoрну систему захисту принципово неможливо. При достатній кількості часу і коштів можна подолати будь-який захист. Тому має сенс вести мову тільки про деяке прийнятному рівні безпеки. Високоефективна система захисту коштує дорого, використовує при роботі істотну частину потужності й ресурсів комп'ютерної системи і може створювати відчутні додаткові незручності користувачам. Важливо правильно вибрати той достатній рівень захисту, при якому витрати, ризик і розмір можливого збитку були б прийнятними (задача аналізу ризику).

2.8.5 Гнучкість системи захисту

Часто доводиться створювати систему захисту в умовах великої невизначеності. Тому прийняті заходи та встановлені засоби захисту, особливо в початковий період їх експлуатації, можуть забезпечувати як надмірний, так і недостатній рівень захисту. Природно, що для забезпечення можливості варіювання рівнем захищеності, засоби захисту повинні мати певну гнучкістю. Особливо важливим це властивість є в тих випадках, коли встановлення засобів захисту необхідно здійснювати на працюючу систему, не порушуючи процесу її нормального функціонування. Крім того, зовнішні умови і вимоги з плином часу змінюються. У таких ситуаціях властивість гнучкості рятує власників АС від необхідності прийняття кардинальних заходів по повній заміні засобів захисту на нові.

2.8.6 Відкритість алгоритмів і механізмів захисту

Суть принципу відкритості алгоритмів і механізмів захисту полягає в тому, що захист не повинна забезпечуватися тільки за рахунок обмеження доступу структурної організації та алгоритмів функціонування її підсистем. Знання алгоритмів роботи системи захисту не повинно давати можливості її подолання (навіть авторові). Проте, це зовсім не означає, що інформація про конкретну систему захисту повинна бути загальнодоступною.

2.8.7 Принцип простоти застосування засобів захисту

Механізми захисту повинні бути інтуїтивно зрозумілі і прості у використанні. Застосування засобів захисту не повинно бути пов'язане зі знанням спеціальних мов або з виконанням дій, що вимагають значних додаткових трудовитрат при звичайній роботі законних користувачів, а також не повинно вимагати від користувача виконання рутинних малозрозумілих йому операцій (введення декількох паролів та імен і т.д.).

2.9. Концептуальні підходи до проектування систем захисту

Зараз можна виділити три різних концептуальних підходи до проектування систем захисту:

Підхід перший: "від продукту". Цього підходу дотримуються, як правило, компанії-виробники систем захисту інформації, що мають у своєму складі проектну групу. Фактично, в таких компаніях інтеграція виросла з просто впроваджувального напрямку, в той момент, коли замовник попросив не просто продукт, а проект. Таким чином, вся технологія проектування орієнтована на те, щоб продукт, вироблений компанією, був центральним незалежно від розв'язуваної задачі. Даний підхід не завжди реально обґрунтований, особливо в умовах агресивного маркетингу і позиціонування продукту, як "панацеї" від більшості загроз безпеки.

Однак, у разі, коли замовник має достатню кваліфікацію, щоб широко дивитися на проблему захисту інформації в цілому і уникати однобоких рішень, реалізуються проекти високої якості, що зрозуміло – ніхто крім виробника не знає продукту краще. Але в цьому випадку потрібно або наявність власних висококласних фахівців, системних архітекторів, або залучення зовнішніх консалтингових компаній.

Позиція друга – компанія виступає постачальником рішень в області захисту інформації. Розуміючи відсутність єдиного продукту, що захищає від усіх загроз, компанія пропонує комплексне вирішення проблеми. Воно складається з комбінації декількох технологій захисту, наприклад, міжмережевих екранів для захисту від атак з Інтернету, VPN – для закриття каналів зв'язку і т.п. Ось, здавалося б, оптимальна позиція: кожна технологія, кожен продукт займає свою нішу і закривають певні загрози. Але тут існує одна проблема.

Формально схема виглядає наступним чином: зараз існують чотири основні технології захисту – міжмережеве екранування, VPN, криптографічний захист, активний аудит. У кожної технології є по 3–4 дійсно працюють продукту. Тобто, чотири технології по чотири продукти утворюють 16 кубиків, з яких може будуватися система безпеки. Тоді завдання архітектора системи захисту зводиться до того, щоб знайти, куди прилаштувати кожен кубик. Виникає спокуса починати будувати систему, відштовхуючись не від потреб замовника, а від наявних засобів захисту.

Може бути, така технологія роботи була б виправдана в умовах повністю електронного документообігу в організації, але російські реалії такі, що більшість комп'ютерних систем в наших організаціях є 300–400 друкарських машинок, об'єднаних мережею. В умовах паперового документообігу всі документи готуються на комп'ютері, роздруковуються, а потім у паперовому вигляді рухаються по організації. У мережі існують лише вогнища автоматизації, наприклад, у бухгалтерії, в конструкторському відділі і т.п. А всі інші співробітники спілкуються один з одним, в кращому випадку, на e-mail або через спільні папки. Тому буває важко пояснити, навіщо використовувати, наприклад, VPN, якщо вся інформація надсилається поштою або факсом. Або навіщо встановлювати на комп'ютери електронні замки, якщо всі документи зберігаються в shared папках, не закриті паролями, і їх може отримати практично будь-який співробітник.

Не можна говорити, що підхід від "кубиків" не прийнятний і не життєздатний. В даний час існує великий неосвоєний ринок середніх і дрібних компаній, для яких занадто дорого купувати серйозні консалтингові послуги компаній-інтеграторів. Таким компаніям як раз і потрібен деякий набір продуктів і рішень, які могли б просто об'єднуватися в систему, надаючи їй необхідну функціональність.

І існує третя позиція – найскладніша і досить рідко зустрічається на нашому ринку. Яка стандартна схема продажу певного продукту або системи? Постачальник приходить до замовника, вивчає його проблему і пропонує те чи інше рішення, продукт або варіанти рішення, або замовник організує тендер, отримує кілька пропозицій. І в тому і в іншому випадку замовник самостійно приймає рішення про те, яку систему, технологію впроваджувати. Тобто відповідальність за прийняття рішень щодо захисту інформації покладається на замовника, який, взагалі кажучи, не є експертом в галузі захисту інформації. Найскладніше завдання, яка може і повинна стояти перед компанією-інтегратором, – це прийняти на себе відповідальність за вибір стратегії забезпечення безпеки організації, розвиток системи, її адекватність розвиваються технологіями. Системний інтегратор повинен реалізовувати єдину комплексну політику, як технічну, так і організаційну, проводячи її на всіх рівнях організації-замовника.

Перед виробленням рішення з інформаційної безпеки інтегратор повинен провести всебічне глибоке обстеження не просто інформаційної системи замовника, а всієї "інформаційного життя" організації. Обстеження має вестися на трьох рівнях: на рівні бізнес-процесів, який виявляє документальні потоки, типи оброблюваної інформації, рівні її конфіденційності; на інфраструктурному рівні – для виявлення вразливих місць серверного парку, мережевого обладнання; на рівні додатків, на якому виявляються уразливості в програмному забезпеченні , помилки в налаштуваннях механізмів розмежування доступу та ін..

На основі отриманих даних необхідно формувати спочатку концептуальне рішення по захисту інформації, що складається з комплексу організаційних, процедурних і програмно-апаратних засобів захисту, а потім, чітко обґрунтовуючи вибір, пропонувати впровадження тих чи інших технологій захисту. При цьому потрібно враховувати, що підсистема інформаційної безпеки є підтримуючої системою по відношенню до всієї інформаційної системі організації. Вона не повинна грати домінуючу роль у розвитку організації та її інформаційної системи. Тобто система інформаційної безпеки повинна захищати інформацію, що забезпечує бізнес-завдання організації.

Таким чином, будь-яка система інформаційної безпеки, що захищає велику організацію з розподіленою інформаційною системою, або система, що представляє собою один міжмережевий екран, повинна бути розумно достатньою по відношенню до організації, вона не повинна заважати роботі працівників. Завжди повинен бути адекватний вибір рівня захисту, правильний вибір технологій і засобів захисту.

РОЗДІЛ 3 ПОРЯДОК ЗДІЙСНЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Технічний захист інформації здійснюється поетапно:

1 етап – визначення й аналіз загроз;

2 етап – розроблення системи захисту інформації;

3 етап – реалізація плану захисту інформації;

4 етап – контроль функціонування та керування системою захисту інформації.

3.1. Визначення й аналіз загроз

Говорити про безпеку об'єкта (системи) можна, лише маючи на увазі, що за допомогою цього об'єкта або над цим об'єктом відбуваються якісь дії. У цьому сенсі, якщо об'єкт не діє, а саме не функціонує (не використовується, не розвивається і т. д.), Або, кажучи іншими словами, не взаємодіє з зовнішнім середовищем, то і розглядати його безпеку безглуздо. Отже, об'єкт необхідно розглядати в динаміці і у взаємодії із зовнішнім середовищем.

У деяких випадках можна говорити про безпеку системи при її зберігання. Але навіть при зберігання системи взаємодія з зовнішнім середовищем неминуче.

При функціонуванні об'єкта завжди переслідуються певні цілі. Сукупність дій, що здійснюються об'єктом, для досягнення певної мети реалізується у вигляді результатів, які мають значення для самого об'єкта. Якщо мета операції або сукупності цілеспрямованих дій досягнута, то безпеку операції, а отже, інформації, що циркулює в системі, забезпечена.

Проблема дослідження критичних ситуацій і факторів, які можуть становити певну небезпеку для інформації, а також пошуку та обґрунтування комплексу заходів і засобів по їх виключення або зниження, характеризується наступними особливостями:

– великою кількістю чинників небезпечних ситуацій і необхідністю виявлення джерел і причин їх виникнення;

– необхідністю виявлення і вивчення повного спектру можливих заходів і засобів парирування небезпечних факторів з метою забезпечення безпеки.

У статті А. І. Алексєнцева «Поняття і структура загроз захищається Інформації» визначення загрози сформульовано таким чином: «Загроза захищається – сукупність явищ, факторів і умов, що створюють небезпеку порушення статусу інформації». Тобто загроза інформації обумовлена цілком певними факторами, сукупністю явищ і умов, які можуть скластися в конкретній ситуації.

По відношенню до інформаційної системи все безліч загроз можна розбити на дві групи: зовнішні і внутрішні, кожна з яких, в свою чергу, ділиться на умисні й випадкові загрози, які можуть бути явними і прихованими.

Виявлення та аналіз загроз, що захищається є відповідальним етапом при побудові системи захисту інформації на підприємстві. Більшість фахівців вживають термін «загрози безпеки інформації». Але безпека інформації – це стан захищеності інформації від впливів, що порушують її статус. Отже, безпека інформації означає, що інформація знаходиться в такому захищеному вигляді, який здатний протистояти будь-яким дестабілізуючим впливам.

Будь-яка загроза не зводиться до чогось однозначного, вона складається з певних взаємопов'язаних компонентів, кожен з яких сам по собі не створює загрозу, але є невід'ємною частиною її, загроза же виникає лише при сукупному їх взаємодії.

Загрози, що захищається пов'язані з її вразливістю, тобто нездатністю інформації самостійно протистояти дестабілізуючим впливам, таким, що порушує її статус. Реалізація загроз призводить, в залежності від їх характеру, до однієї або кількох форм прояву уразливості інформації. При цьому кожній з форм прояву уразливості (або декільком з них) притаманні певні, що мають відношення тільки до них загрози з набором відповідних компонентів. Структура конкретної загрози зумовлює конкретну форму. Однак повинна існувати і загальна, як би типова структура загроз, яка складає основу конкретних загроз. Ця загальна структура повинна базуватися на певних ознаках, характерних для загрози захищається.

Перш за все, загроза повинна мати якісь сутнісні прояви. А будь-який прояв, виявлення чогось прийнято називати явищем. Отже, одним з ознак і разом з тим однією зі складових загрози повинні бути явища.

Але в основі будь-якого явища лежать відповідні причини, які є його рушійною силою і які, в свою чергу, зумовлені певними обставинами або передумовами. Ці причини і обставини (причини) відносяться до чинників, що створює можливість дестабілізуючого впливу на інформацію. Таким чином, фактори є ще одним приймачем і другої складової загрози.

Разом з тим чинники можуть стати спонукальною силою для явищ, а останні можуть «спрацювати» лише при наявності певних умов (обставин) для цього. Наявність умов для дестабілізуючого впливу на інформацію є третім ознакою і ще однієї складової загрози.

Визначальною ознакою загрози є її спрямованість, результат, до якого може привести дестабілізуючий вплив на інформацію. Цим результатом у всіх випадках реалізацію загрози є порушення статусу інформації.

Таким чином, загроза захищається – це сукупність явищ, факторів і умов, що створюють небезпеку порушення статусу інформації.

До явищ сутнісним проявам загрози, відносяться:

– джерела дестабілізуючого впливу на інформацію (від кого або від чого виходить дестабілізуючий вплив);

– види дестабілізуючого впливу на інформацію (яким чином (за якими напрямами) відбувається дестабілізуючий вплив);

– способи дестабілізуючого впливу на інформацію (якими прийомами, діями здійснюються (реалізуються) види дестабілізуючого впливу).

До факторів, крім причин і обставин, слід віднести наявність каналів і методів несанкціонована доступу до конфіденційної інформації для впливу на інформацію з боку осіб, які не мають до неї дозволеного доступу.

Що стосується складу структурних частин загрози, то необхідно підкреслити: стрижневими, вихідними є джерела дестабілізуючого впливу на інформацію, від їх складу залежать і види, і способи, і кінцевий результат впливу. Хоча склад інших структурних частин загрози також грає істотну роль, він на відміну від джерел не носить визначального характеру і прямо залежить від джерел. Разом з тим ще раз слід зазначити, що джерела самі по собі не є загрозою, якщо від них не відбувається тих чи інших впливів.

Розглянемо джерела дестабілізуючого впливу на інформацію. До них відносяться:

– люди;

– технічні засоби відображення (фіксації), збереження, обробки, відтворення, передачі інформації, засоби зв`язку;

– системи забезпечення функціонування технічних засобів відображення, зберігання, обробки, відтворення і передачі інформації;

– технологічні процеси окремих категорій промислових об'єктів;

– природні явища.

Найпоширенішим, різноманітним і небезпечним джерелом дестабілізуючого впливу на захищає інформацію є люди, які діляться на наступні категорії:

– співробітники даного підприємства;

– особи, які не працюють на підприємстві, але мають доступ до інформації, що захищається підприємства в силу службового становища;

– співробітники державних органів розвідки інших країн і розвідувальних служб конкуруючих вітчизняних та зарубіжних підприємств;

– особи з кримінальних структур, хакери.

У частині співвідношення з видами і способами дестабілізуючого впливу на інформацію ці категорії людей поділяються на дві групи: мають доступ до носіїв даної інформації, що захищається, технічних засобів її відображення, зберігання, обробки, відтворення, передачі і системам забезпечення їх функціонування і не мають такого.

Відзнаки в конкретно застосовуваних видах і методах дестабілізуючий вплив на інформацію між названими групами людей (при однотипності видів і методів) обумовлені переслідуваними цілями. Основною метою

другий групи людей є несанкціоноване отримання (розкрадання) інформації, що є ІзОД. Знищення, перекручення, блокування інформації стоять на другому плані, а нерідко і не є метою. Дестабілізуючий вплив з боку цієї групи людей в переважній більшості випадків є навмисним (умисним, свідомим). До того ж, для того щоб здійснити дестабілізуючий вплив на конфіденційну інформацію, людям, що входять в цю групу, потрібно мати канал несанкціонованого доступу до неї.

Для першої групи людей несанкціоноване отримання ІзОД взагалі не є метою в силу наявності у них доступу до такої інформації. Цілями дестабілізуючого впливу з боку цієї групи є розголошення, несанкціоноване, знищення, блокування, спотворення інформації (перераховані в послідовності, відповідної ступеня інтенсивності впливу, від більшої до меншої). Розкрадання інформації також притаманне для даної групи, але воно є не метою, а засобом для здійснення знищення або розголошення інформації. Предметом впливу з боку цієї групи є не тільки конфіденційна інформація (хоча вона в першу чергу), але і захищається частина відкритої інформації. Вплив з боку людей, включених до цієї групи, може бути як навмисним, і ненавмисним (помилковим, випадковим). Слід, однак, домовитися про те, що по об'єктах доступу ця група неоднорідна по своєму складу. У неї входять люди, які мають доступ і до носіїв інформації, що захищається, і до засобів відображення, зберігання, обробки, відтворення і передачі інформації (до всіх або частини з них), і до систем забезпечення функціонування цих засобів, люди, які мають доступ тільки до інформації і (іноді або) до засобів її обробки (всім або окремим); люди, допущені тільки до системи забезпечення функціонування засобів.

Самим різноманітним це джерело є тому, що йому, в порівнянні з іншими джерелами, притаманне значно більшу кількість видів і способів дестабілізуючого впливу на інформацію.

Найнебезпечнішим це джерело є тому, що, по-перше, він наймасовіший, по-друге, вплив з боку носить не епізодичний, постійний характер, по-третє, як уже зазначалося, його вплив може бути не тільки ненавмисним, як з боку інших джерел, але і навмисним, і, по-четверте, який чиниться їм вплив може призвести до всіх форм прояву уразливості інформації (з боку інших джерел – до окремих форм).

Технічні засоби відображення, зберігання, обробки, відтворення, передачі інформації і засоби зв'язку є другим за значенням джерелом дестабілізуючого впливу на захищає інформацію в силу їхнього різноманіття, а також існуючих з їх боку способів дестабілізуючого впливу. До цього джерела відносяться:

– електронно-обчислювальна техніка;

– електричні та автоматичні друкарські машинки і копіювально-розмножувальна техніка;

– засоби відео- та звукозаписувальної та відтворювальної техніки;

– засоби телефонного, телеграфного, факсимільного, гучномовного передачі інформації;

– засоби радіомовлення і телебачення;

– засоби радіо і кабельного зв'язку.

Третє джерело дестабілізуючого впливу на інформацію включає системи електропостачання, водопостачання, теплопостачання, кондиціонування.

До четвертого джерела відносяться технологічні процеси об'єктів ядерної енергетики, хімічної промисловості, радіоелектроніки, а також об'єктів з виготовлення деяких видів озброєння і військової техніки, які змінюють природну структуру навколишнього об'єкт середовища.

П'яте джерело – природні явища – включає складові: стихійні лиха і атмосферні явища.

3.2 Методика виявлення способів впливу на інформацію

Залежно від джерела і виду впливу воно може бути безпосереднім на захищається інформацію або опосередкованим, через інше джерело впливу.

З боку людей можливі наступні види впливу:

1. Безпосередній вплив на носії інформації, що захищається;

2. несанкціоноване розповсюдження конфіденційної інформації;

3. висновок з ладу технічних засобів відображення, зберігання, обробки, відтворення, передачі інформації і засобів зв'язку;

4. порушення режиму роботи перерахованих коштів та технології обробки інформації;

5. висновок з ладу і порушення режиму роботи систем забезпечення функціонування названих засобів.

Способами безпосереднього впливу на носії інформації, що захищається можуть бути:

– фізичне руйнування носія (поломка, руйнування і ін.);

– створення аварійних ситуацій для носіїв (підпал, штучне затоплення, вибух і т. д.);

– видалення інформації з носіїв;

– створення штучних магнітних полів для розмагнічування носіїв;

– внесення фальсифікованої інформації у носії.

Цей вид дестабілізуючого впливу призводить до реалізації трьох форм прояву уразливості інформації: знищення, спотворення і блокування.

До безпосереднього впливу на носії інформації, що захищається можна з застереженням віднести і ненавмисне залишення їх в неохоронюваної зоні, найчастіше в громадському транспорті, магазині, на ринку, що призводить до втрати носіїв.

Несанкціоноване розповсюдження ІзОД може здійснюватися шляхом:

– словесної передачі (повідомлення) інформації;

– передачі копій (знімків) носіїв інформації;

– показу носіїв інформації;

– введення інформації в обчислювальні мережі;

– опублікування інформації в пресі;

– використання інформації у відкритих публічних виступах, в тому числі по радіо, телебаченню.

До розголошення може призвести і втрата носіїв інформації. Цей вид дестабілізуючого впливу призводить до розголошення ІзОД.

До способів виведення з ладу технічних засобів відображення, зберігання, обробки, відтворення, передачі інформації і засобів зв'язку можна віднести:

– неправильний монтаж засобів;

– поломку (руйнування) коштів, в тому числі розрив (пошкодження) кабельних ліній зв'язку;

– створення аварійних ситуацій для засобів (підпал, штучне затоплення, вибух та ін.);

– відключення засобів від систем;

– виведення з ладу або порушення режиму роботи систем забезпечення функціонування засобів;

– вмонтування в ЕОМ радіо- і програмних закладних пристроїв.

Цей вид дестабілізуючого впливу призводить до реалізації трьох форм прояву уразливості інформації: знищення, спотворення і блокування.

Способами порушення режиму роботи технічних засобів відображення, зберігання, обробки, відтворення, передачі інформації, засобів зв'язку і технології обробки інформації можуть бути:

– пошкодження окремих елементів засобів;

– порушення правил експлуатації засобів;

– внесення змін до порядку обробки інформації;

– зараження програм обробки інформації шкідливими програмами;

– видача неправильних програмних команд;

– перевищення розрахункового числа запитів;

– створення перешкод у радіоефірі за допомогою додаткового звукового або шумового фону, зміни (накладення) частот передачі інформації;

– передача хибних сигналів;

– порушення (зміна) режиму роботи систем забезпечення функціонування засобів.

Даний вид дестабілізуючого впливу також призводить до знищення, перекручення і блокування інформації.

До способів виведення з ладу і порушення режиму роботи систем забезпечення, функціонування технічних засобів відображення, зберігання, обробки, відтворення і передачі інформації слід віднести:

– неправильний монтаж систем;

– поломку (руйнування) систем або їх елементів;

– створення аварійних ситуацій для систем (підпал, штучне затоплення, вибух і т. д.);

– відключення систем від джерел живлення;

– порушення правил експлуатації систем.

Цей вид дестабілізуючого впливу призводить до тих же результатів, що і два попередні види.

До видів дестабілізуючого впливу на захищає інформацію з боку другого джерела впливу – технічних засобів відображення, зберігання, обробки, відтворення, передачі інформації і засобів зв'язку відносяться:

1. Виведення засобів з ладу;

2. Збої в роботі засобів;

3. Створення електромагнітних випромінювань.

Вихід засобів з ладу, що призводить до неможливості виконання операцій, може відбуватися шляхом:

– технічної поломки, аварії (без втручання людей);

– загоряння, затоплення (без втручання людей);

– виходу з ладу систем забезпечення функціонування засобів;

– впливу природних явищ;

– впливу зміненої структури навколишнього магнітного поля;

– зараження програм обробки інформації шкідливими програмами (шляхом розмноження останніх або з заражених дискет);

– руйнування або пошкодження носія інформації, в тому числі розмагнічування магнітного шару диска (стрічки) через осипання магнітного порошку.

Цей вид дестабілізуючого впливу призводить до реалізації трьох форм прояву уразливості інформації: знищення, перекручення, блокування.

Збої в роботі засобів, що призводять до неправильного виконання операцій (помилок), можуть здійснюватися за допомогою:

– виникнення технічних несправностей елементів засобів;

– зараження програм обробки інформації шкідливими програмами (шляхом розмноження останніх або з заражених дискет);

– впливу природних явищ;

– впливу навколишнього магнітного поля;

– часткового розмагнічування магнітного шару диска (стрічки) через осипання магнітного порошку;

– порушення режиму функціонування засобів.

Даний вид дестабілізуючого впливу призводить до реалізації чотирьох форм прояву уразливості інформації: знищення, перекручення, блокування, розголошенню (приклад останньої – з'єднання з номерів телефону, не тої абонента, який набирався або чутність розмови інших осіб через несправність в ланцюгах комунікації телефонної станції). Електромагнітні випромінювання, в тому числі побічні, що утворюються в процесі експлуатації засобів, призводять до розкрадання інформації.

Третє джерело дестабілізуючого впливу на інформацію – системи забезпечення функціонування технічних засобів відображення, зберігання, обробки, відтворення і передачі інформації – включає два види впливу:

1. Вихід систем з ладу.

2. Збої в роботі систем.

Вихід систем з ладу може відбуватися шляхом:

– поломки, аварії (без втручання людей);

– загоряння, затоплення (без втручання людей);

– виходу з ладу джерел живлення;

– впливу природних явищ.

Цей вид дестабілізуючого впливу призводить до реалізації трьох форм прояву уразливості інформації: знищення, блокування, викривлення.

Збої в роботі систем можуть здійснюватися за допомогою:

– появи технічних несправностей елементів систем;

– впливу природних явищ;

– порушення режиму роботи джерел живлення.

Результатом дестабілізуючого впливу також є знищення, блокування, спотворення інформації.

Видом дестабілізуючого впливу на інформацію з боку технологічних процесів окремих промислових об'єктів є зміна структури навколишнього середовища. Це вплив здійснюється шляхом:

– зміни природного радіаційного фону навколишнього середовища, що відбувається при функціонуванні об'єктів ядерної енергетики;

– зміни хімічного складу навколишнього середовища, що відбувається при функціонуванні об'єктів хімічної промисловості;

– зміни локальної структури магнітного поля, що відбувається внаслідок діяльності об'єктів радіоелектроніки і по виготовленню деяких видів озброєння і військової техніки.

Цей вид дестабілізуючого впливу в кінцевому підсумку призводить до розкрадання ІзОД.

П'яте джерело дестабілізуючого впливу на інформацію – природні явища, як уже зазначалося, включає стихійні лиха і атмосферні явища (коливання).

До стихійних лих і одночасно видам впливу слід віднести: землетрус, повінь, шторм, зсуви, лавини, виверження вулканів; до атмосферних явищ (видам впливу): грозу, дощ, сніг, перепади температури і вологості повітря, магнітні бурі.

Способами впливу з боку і стихійних лих, і атмосферних явищ можуть бути руйнування (поломка), землетрус, спалення носіїв інформації засобів відображення, зберігання, обробки, відтворення, передачі інформації і засобів зв'язку, систем забезпечення функціонування цих засобів, порушення режиму роботи засобів і систем , а також технології обробки інформації, створення паразитних наведень (грозові раз ряди).

Ці види впливу призводять до п'яти формами прояву уразливості інформації: втрати, знищення, перекручення, блокування і розкрадання.

При розгляді ознак і складових загрози захищається було сказано, що в основі будь-якого дестабілізуючого впливу лежать певні причини, спонукальні мотиви, які зумовлюють появу того чи іншого виду і способу впливу. Разом з тим і причини мають під собою підстави – обставини або передумови, які викликають ці чинники, сприяють їхній появі. Однак наявність джерел, видів, способів, причин і обставин (передумов) дестабілізуючого впливу на інформацію являє потенційно існуючу небезпеку, яка може бути реалізована тільки при наявності певних умов для цього.

3.2. Розроблення плану захисту інформації

На другому етапі розробляється план ТЗІ, що містить організаційні, первинні технічні та основні технічні заходи захисту ІзОД, визначити зони безпеки інформації.

Організаційні заходи регламентують порядок інформаційної діяльності з урахуванням норм і вимог ТЗІ для всіх періодів життєвого циклу ОІД.

Первинні технічні заходи передбачають захист інформації блокуванням загроз без використання засобів ТЗІ.

Основні технічні заходи передбачають захист інформації з використанням засобів забезпечення ТЗІ.

Заходи захисту інформації повинні:

• бути відповідними загрозам;

• бути розробленими з урахуванням можливої шкоди від їх реалізації і вартості захисних заходів та обмежень, що вносяться ними;

• забезпечувати задану ефективність захисту інформації на встановленому рівні протягом часу обмеження доступу до неї або можливості здійснення загроз.

Рівень захисту інформації означується системою кількісних та якісних показників, які забезпечують розв’язання завдання захисту інформації на основі норм та вимог ТЗІ.

Мінімально необхідний рівень захисту інформації забезпечують обмежувальними і фрагментарними заходами протидії найнебезпечнішій загрозі.

Підвищення рівня захисту інформації досягається нарощуванням технічних заходів протидії безлічі загроз.

Порядок розрахунку та інструментального визначення зон безпеки інформації, реалізації заходів ТЗІ, розрахунку ефективності захисту та порядок атестації технічних засобів забезпечення інформаційної діяльності, робочих місць (приміщень) установлюються нормативними документами системи ТЗІ.

3.3. Реалізація плану захисту інформації

На третьому етапі слід реалізувати організаційні, первинні технічні та основні технічні заходи захисту ІзОД, установити необхідні зони безпеки інформації, провести атестацію технічних засобів забезпечення інформаційної діяльності, технічних засобів захисту інформації, робочих місць (приміщень) на відповідність вимогам безпеки інформації.

Технічний захист інформації забезпечується застосуванням захищених програм і технічних засобів забезпечення інформаційної діяльності, програмних і технічних засобів захисту інформації (далі – засоби ТЗІ) та контролю ефективності захисту, які мають сертифікат відповідності вимогам нормативних документів системи УкрСЕПРО або дозвіл на їх використання від уповноваженого Кабінетом Міністрів України органу, а також застосуванням спеціальних інженерно-технічних споруд, засобів і систем (далі – засоби забезпечення ТЗІ).

Засоби ТЗІ можуть функціонувати автономно або спільно з технічними засобами забезпечення інформаційної діяльності у вигляді самостійних пристроїв або вбудованих у них складових елементів.

Склад засобів забезпечення ТЗІ, перелік їх постачальників, а також послуг з установлення, монтажу, налагодження та обслуговування визначаються особами, що володіють, користуються і розпоряджаються ІзОД самостійно або за рекомендаціями спеціалістів з ТЗІ згідно з нормативними документами системи ТЗІ.

Надання послуг з ТЗІ, атестацію та сервісне обслуговування засобів забезпечення ТЗІ можуть здійснювати юридичні і фізичні особи, що мають ліцензію на право проведення цих робіт, видану Державною службою спеціального зв’язку та захисту інформації України.

3.4 Організація проведення обстеження об’єктів інформаційної діяльності

Метою обстеження об’єктів інформаційної діяльності є вивчення його ІД, визначення об`єктів захисту – ІзОД, виявлення загроз, їхній аналіз та побудова окремої моделі загроз.

Обстеження повинно бути проведено комісією, склад якої визначається відповідальною за ТЗІ особою і затверджується наказом Керівника підприємства.

У ході обстеження необхідно:

– провести аналіз умов функціонування ОІД підприємства, їх розташування на місцевості (ситуаційного плану) для визначення можливих джерел загроз;

– дослідити засоби забезпечення ІД, які мають вихід за межі контрольованої території;

– вивчити схеми засобів і систем життєзабезпечення ОІД (електроживлення, заземлення, автоматизації, пожежної та охоронної сигналізації), а також інженерних комунікацій та металоконструкцій;

– дослідити інформаційні потоки, технологічні процеси передачі, одержання, використання, розповсюдження і зберігання (далі – оброблення) інформації і провести необхідні вимірювання;

– визначити наявність та технічний стан засобів забезпечення ТЗІ;

– перевірити наявність на ОІД нормативних документів, які забезпечують функціонування системи захисту інформації, організацію проектування будівельних робіт з урахуванням вимог ТЗІ, а також нормативної та експлуатаційної документації, яка забезпечує ІД;

– виявити наявність транзитних, незадіяних (повітряних, настінних, зовнішніх та закладених у каналізацію) кабелів, кіл і проводів;

– визначити технічні засоби і системи, застосування яких не обґрунтовано службовою чи виробничою необхідністю і які підлягають демонтуванню;

– визначити технічні засоби, що потребують переобладнання (перемонтування) та встановлення засобів ТЗІ.

За результатами обстеження слід скласти акт, який повинен бути затверджений Керівником підприємства.

Матеріали обстеження необхідно використовувати під час розроблення окремої моделі загроз, яка повинна включати:

– генеральний та ситуаційний плани підприємства, схеми розташування засобів і систем забезпечення ІД, а також інженерних комунікацій, які виходять за межі контрольованої території;

– схеми та описи каналів витоку інформації, каналів спеціального впливу і шляхів несанкціонованого доступу до ІзОД;

– оцінку шкоди, яка передбачається від реалізації загроз.

3.5. Організація розроблення системи захисту інформації

На підставі матеріалів обстеження та окремої моделі загроз необхідно визначити головні задачі захисту інформації і скласти технічне завдання (ТЗ) на розроблення системи захисту інформації.

ТЗ повинно включати основні розділи:

– вимоги до системи захисту інформації;

– вимоги до складу проектної та експлуатаційної документації;

– етапи виконання робіт;

– порядок внесення змін і доповнень до розділів ТЗ;

– вимоги до порядку проведення випробування системи захисту.

Основою функціонування системи захисту інформації є план ТЗІ, що повинен містити такі документи:

– перелік розпорядчих, організаційно-методичних, нормативних документів з ТЗІ, а також вказівки щодо їхнього застосування;

– інструкції про порядок реалізації організаційних, первинних технічних та основних технічних заходів захисту;

– інструкції, що встановлюють обов`язки, права та відповідальність персоналу;

– календарний план ТЗІ.

ТЗ і план ТЗІ розробляють спеціалісти з ТЗІ, узгоджують із зацікавленими підрозділами (організаціями). Затверджує їх керівник підприємства.

3.6. Реалізація організаційних заходів захисту

Організаційні заходи захисту інформації – комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення задач захисту шляхом регламентації діяльності персоналу і порядку функціонування засобів (систем) забезпечення ІД та засобів (систем) забезпечення ТЗІ.

У процесі розроблення і реалізації організаційних заходів потрібно:

– визначити окремі задачі захисту ІзОД;

– обґрунтувати структуру і технологію функціонування системи захисту інформації;

– розробити і впровадити правила реалізації заходів ТЗІ;

– визначити і встановити права та обов`язки підрозділів та осіб, що беруть участь в обробленні ІзОД;

– придбати засоби забезпечення ТЗІ та нормативні документи і забезпечити ними ОІД підприємства;

– установити порядок упровадження захищених засобів оброблення інформації, програмних і технічних засобів захисту інформації, а також засобів контролю ТЗІ;

– установити порядок контролю функціонування системи захисту інформації та її якісних характеристик;

– визначити зони безпеки інформації;

– установити порядок проведення атестації системи захисту інформації, її елементів і розробити програми атестаційного випробування;

– забезпечити керування системою захисту інформації.

Оперативне вирішення задач ТЗІ досягається організацією керування системою захисту інформації, для чого необхідно:

– вивчати й аналізувати технологію проходження ІзОД у процесі ІД;

– оцінювати схильність ІзОД до впливу загроз у конкретний момент часу;

– оцінювати очікувану ефективність застосування засобів забезпечення ТЗІ;

– визначати (за необхідності) додаткову потребу в засобах забезпечення ТЗІ;

– здійснювати збирання, оброблення та реєстрацію даних, які відносяться до ТЗІ;

– розробляти і реалізовувати пропозиції щодо коригування плану ТЗІ в цілому або окремих його елементів.

3.7. Організаційно – правові заходи щодо охорони державної таємниці

З метою охорони державної таємниці впроваджуються:

- єдині вимоги до виготовлення, користування, збереження, передачі, транспортування та обліку матеріальних носіїв секретної інформації;
- дозвільний порядок провадження органами державної влади, діяльності, пов'язаної з державною таємницею;
- обмеження оприлюднення, передачі іншій державі або поширення іншим шляхом секретної інформації;
- обмеження щодо перебування та діяльності в Україні іноземців, осіб без громадянства та іноземних юридичних осіб, їх доступу до державної таємниці, а також розташування і переміщення об'єктів і технічних засобів, що їм належать;
- особливості здійснення органами державної влади їх функцій щодо органів державної влади, діяльність яких пов'язана з державною таємницею;
- режим обмеження доступу органів державної влади, органів місцевого самоврядування, підприємств, установ і організацій, що провадять діяльність, пов'язану з державною таємницею;
- спеціальний порядок допуску та доступу громадян до державної таємниці;
- технічний та криптографічний захисти секретної інформації.

3.8. Реалізація первинних технічних заходів захисту

У процесі реалізації первинних технічних заходів потрібно забезпечити:

– блокування каналів витоку інформації;

– блокування несанкціонованого доступу до інформації чи її носіїв;

– перевірку справності та працездатності технічних засобів забезпечення ІД.

Блокування каналів витоку інформації може здійснюватися:

– демонтуванням технічних засобів, ліній зв'язку, сигналізації та керування, енергетичних мереж, використання яких не пов'язано з життєзабезпеченням ОІД та обробленням ІзОД;

– видаленням окремих елементів технічних засобів, які є середовищем поширення полів та сигналів, з приміщень, де циркулює ІзОД;

– тимчасовим відключенням технічних засобів, які не беруть участі в обробленні ІзОД, від ліній зв'язку, сигналізації, керування та енергетичних мереж;

– застосуванням способів та схемних рішень із захисту інформації, що не порушують основних технічних характеристик засобів забезпечення ІД.

Блокування несанкціонованого доступу до інформації або її носіїв може здійснюватися:

– створенням умов роботи в межах установленого регламенту;

– унеможливленням використання програмних, програмно-апаратних засобів, що не пройшли перевірки (випробування).

Перевірку справності та працездатності технічних засобів і систем забезпечення ІД необхідно проводити відповідно до експлуатаційних документів.

Виявлені несправні блоки й елементи можуть сприяти витоку або порушенню цілісності інформації і підлягають негайній заміні (демонтуванню).

3.9. Реалізація основних технічних заходів захисту

У процесі реалізації основних технічних заходів захисту потрібно:

– установити засоби виявлення та індикації загроз і перевірити їхню працездатність;

– установити захищені засоби оброблення інформації, засоби ТЗІ та перевірити їхню працездатність;

– застосувати програмні засоби захисту в засобах обчислювальної техніки, автоматизованих системах, здійснити їхнє тестування і тестування на відповідність вимогам захищеності;

– застосувати спеціальні інженерно-технічні споруди, засоби (системи).

Вибір засобів забезпечення ТЗІ зумовлюється фрагментарним або комплексним способом захисту інформації.

Фрагментарний захист забезпечує протидію певній загрозі.

Комплексний захист забезпечує одночасну протидію безлічі загроз.

Засоби виявлення та індикації загроз застосовують для сигналізації та оповіщення власника (користувача, розпорядника) ІзОД про витік інформації чи порушення її цілісності.

Засоби ТЗІ застосовуються автономно або спільно з технічними засобами забезпечення ІД для пасивного або активного приховування ІзОД.

Для пасивного приховування застосовують фільтри-обмежувачі, лінійні фільтри, спеціальні абонентські пристрої захисту та електромагнітні екрани.

Для активного приховування застосовують вузькосмугові й широкосмугові генератори лінійного та просторового зашумлення.

Програмні засоби застосовуються для забезпечення:

– ідентифікації та автентифікації користувачів, персоналу і ресурсів системи оброблення інформації;

– розмежування доступу користувачів до інформації, засобів обчислювальної техніки і технічних засобів автоматизованих систем;

– цілісності інформації та конфігурації автоматизованих систем;

– реєстрації та обліку дій користувачів;

– маскування оброблюваної інформації;

– реагування (сигналізації, відключення, зупинення робіт, відмови у запиті) на спроби несанкціонованих дій.

Спеціальні інженерно-технічні споруди, засоби та системи застосовуються для оптичного, акустичного, електромагнітного та іншого екранування носіїв інформації.

До них належать спеціально обладнані світлопроникні, технологічні та санітарно-технічні отвори, а також спеціальні камери, перекриття, навіси, канали тощо.

Розміщення, монтування та прокладання спеціальних інженерно-технічних засобів і систем, серед них систем заземлення та електроживлення засобів забезпечення ІД, слід здійснювати відповідно до вимог нормативних документів з ТЗІ.

Технічні характеристики, порядок застосування та перевірки засобів забезпечення ТЗІ наводять у відповідній експлуатаційній документації.

3.10. Приймання, визначення повноти та якості робіт

За результатами виконання рекомендацій акта обстеження та реалізації заходів захисту ІзОД слід скласти у довільній формі акт приймання робіт з ТЗІ, який повинен підписати виконавець робіт, особа, відповідальна за ТЗІ, та затвердити Керівник підприємства.

Для визначення повноти та якості робіт з ТЗІ слід провести атестацію. Атестація виконується організаціями, які мають ліцензії на право діяльності в галузі ТЗІ.

Об`єктами атестації є системи забезпечення ІД та їхні окремі елементи, де циркулює інформація, що підлягає технічному захисту.

У ході атестації потрібно:

– установити відповідність об`єкта, що атестується, вимогам ТЗІ;

– оцінити якість та надійність заходів захисту інформації;

– оцінити повноту та достатність технічної документації для об`єкта атестації;

– визначити необхідність внесення змін і доповнень до організаційно-розпорядчих документів тощо.

РОЗДІЛ 4 АТЕСТАЦІЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Атестація комплексу ТЗІ (далі – атестація) здійснюється за відповідними програмою і методиками випробувань.

На підставі результатів випробувань складається висновок щодо відповідності стану ТЗІ, який забезпечується комплексом, вимогам нормативних документів з ТЗІ.

Атестація може бути первинною, черговою та позачерговою.

Первинна атестація здійснюється після (або під час) приймання робіт із створення комплексу ТЗІ.

Термін проведення чергової атестації визначається технічним паспортом на комплекс ТЗІ або актом попередньої атестації.

Позачергову атестацію проводять у разі змін умов функціонування ОІД, що приводять до змін загроз для інформації, та за висновками органів, які контролюють стан ТЗІ.

Етапи атестації:

– визначення організації-виконавця атестації та оформлення відповідних організаційних документів;

– аналіз умов функціонування ОІД, технічної документації на комплекс ТЗІ та розроблення і оформлення Програми і методик атестації (ПМА);

– проведення випробувань відповідно до ПМА та оформлення протоколів випробувань і підсумкового документа – акта атестації.

Суб'єкти атестації:

– Державна служба спеціального зв’язку та захисту інформації України (далі – Держспецзв’язок);

– організації-замовники атестації;

– організації-виконавці атестації.

Державна служба спеціального зв’язку та захисту інформації України:

– організує розроблення та удосконалення нормативних документів з атестації;

– контролює виконання вимог щодо атестації та розглядає апеляції;

– узгоджує вибір організації-виконавця атестації, ПМА та результати атестації на особливо важливих ОІД.

Витрати на проведення атестації включаються до кошторису на проектування, будівництво та експлуатацію (утримання) ОІД.

4.1 Порядок організації та проведення атестації

Організація-замовник на засадах, передбачених законодавством щодо закупівель послуг за рахунок державних коштів, визначає організацію-виконавця атестації.

Організацією-виконавцем атестації може бути підприємство, установа чи організація, які мають відповідну ліцензію або дозвіл на провадження

діяльності в галузі ТЗІ, одержані у встановленому законодавством порядку.

Відносини між організацією-замовником та організацією-виконавцем, яка є ліцензіатом, регламентуються укладеним між ними договором.

У разі проведення атестації на особливо важливих ОІД визначення організації-виконавця атестації узгоджується з Департаментом.

Організація-виконавець за результатами аналізу відомостей, наданих організацією-замовником, та, за необхідності, за результатами аналізу умов функціонування ОІД і загроз для інформації безпосередньо на ОІД, розробляє проект ПМА та подає його на узгодження організації-замовнику.

Узгоджений організацією-замовником проект ПМА затверджує організація-виконавець.

У разі атестації комплексу ТЗІ на особливо важливих ОІД проект ПМА узгоджується також з Департаментом.

Організація-замовник створює умови проведення атестації, передбачені договором та ПМА.

Організація-виконавець проводить випробування відповідно до ПМА та оформляє акт атестації за формою додатку 2 у 2–х примірниках (1й надається організації-замовнику, 2й – зберігається у організації-виконавця).

До акту атестації додаються протоколи випробувань, передбачених ПМА.

За результатами атестації заповнюється технічний паспорт на комплекс ТЗІ.

У разі проведення атестації на особливо важливих ОІД матеріали з атестації у 5–денний термін організація-виконавець надає Департаменту. Департамент у 2–тижневий термін розглядає результати атестації, приймає рішення щодо можливості їх узгодження, реєструє акт атестації та надсилає його організації-замовнику, одночасно інформуючи про це організацію-виконавця.

4.2 Контроль функціонування та керування системою захисту інформації

Контроль за функціонуванням системи ТЗІ на об’єктах інформаційної діяльності підприємства здійснюється з метою визначення й удосконалення стану ТЗІ в підрозділах підприємства, щодо яких здійснюється ТЗІ, виявлення та запобігання порушенням з ТЗІ в інформаційних системах та об'єктах.

Контроль стану ТЗІ в підрозділах підприємства організується відповідно до планів, затверджених керівниками зазначених органів, шляхом проведення перевірок.

Перевірки стану ТЗІ здійснюються безпосередньо комісіями, на які покладається забезпечення ТЗІ.

Організація проведення перевірок стану ТЗІ, заходи з ТЗІ, які підлягають контролю, висновки та рекомендації визначаються цим Положенням та іншими нормативно-правовими актами з питань ТЗІ.

Контрольно-інспекційна робота з питань ТЗІ включає планування та проведення перевірок стану ТЗІ в підрозділах підприємства, щодо яких здійснюється ТЗІ, проведення аналізу та надання рекомендацій щодо вдосконалення заходів з ТЗІ.

Перевірки поділяються на комплексні, цільові (тематичні) та контрольні.

При комплексній перевірці вивчається та оцінюється стан ТЗІ в підрозділах підприємства, щодо яких здійснюється ТЗІ.

При цільовій (тематичній) перевірці вивчаються окремі напрямки ТЗІ, перевіряється виконання рішень (розпоряджень, наказів, вказівок) органів державної влади з питань ТЗІ в підрозділах, щодо яких здійснюється ТЗІ, виконання завдань або провадження діяльності в галузі ТЗІ за відповідними дозволами та ліцензіями суб'єктами системи ТЗІ.

При контрольній перевірці перевіряється усунення недоліків, які були виявлені під час проведення попередньої комплексної або цільової перевірки.

Зазначені перевірки можуть бути планові та позапланові, з попередженням та раптові.

Позапланова перевірка здійснюється за вказівкою керівництва підприємства в разі виникнення потреби визначення повноти та достатності заходів з ТЗІ за наявності відомостей щодо порушень виконання вимог нормативно-правових актів з питань ТЗІ.

Перевірки здійснюються комісіями підприємства на які покладено виконання завдань щодо здійснення контролю за функціонуванням системи ТЗІ.

При проведенні перевірки стану ТЗІ контролю підлягають організаційні, організаційно-технічні, технічні заходи з ТЗІ в виділених приміщеннях, інформаційних системах і об'єктах, повнота та достатність робіт з атестації виділених приміщень.

Необхідно провести аналіз функціонування системи захисту інформації, перевірку виконання заходів ТЗІ, контроль ефективності захисту, підготувати та видати дані для керування системою захисту інформації.

Керування системою захисту інформації полягає у адаптації заходів ТЗІ до поточного завдання захисту інформації. За фактами зміни умов здійснення або виявлення нових загроз заходи ТЗІ реалізуються у найкоротший строк.

Контроль організаційних заходів з ТЗІ в підрозділах підприємства включає перевірку:

• переліку відомостей, що підлягають технічному захисту;

• окремої моделі загроз для інформаційної системи або об'єкта;

• плану контрольованої зони органу, щодо якого здійснюється ТЗІ;

• переліку виділених приміщень органу, щодо якого здійснюється ТЗІ, інформаційних систем та об'єктів;

• проведення категоріювання виділених приміщень та об'єктів.

Контроль організаційно-технічних і технічних заходів щодо ТЗІ у виділених приміщеннях, інформаційних системах та об'єктах, повноти та достатності робіт з атестації виділених приміщень включає перевірку відповідності виконання цих заходів до нормативно-правових актів з питань ТЗІ.

Організаційно-технічні й технічні заходи з ТЗІ у виділених приміщеннях, інформаційних системах та об'єктах, роботи з атестації виділених приміщень виконуються власними силами або суб'єктами підприємницької діяльності в галузі ТЗІ.

За результатами комплексної перевірки комісією складається акт перевірки стану та ефективності заходів з технічного захисту інформації, а цільової та контрольної перевірки – довідка за довільною формою. Ознайомлення керівника суб'єкта системи ТЗІ з актом (довідкою) здійснюється під розпис.

Керівник підрозділу зобов'язаний ужити невідкладних заходів щодо усунення недоліків і реалізації пропозицій комісії відповідно до вимог нормативно-правових актів з питань ТЗІ.

Порушення встановлених норм та вимог з ТЗІ, виявлені під час проведення перевірок, поділяються на три категорії:

• перша – невиконання норм та вимог з ТЗІ, внаслідок якого створюється реальна можливість порушення конфіденційності, цілісності й доступності інформації або її витоку технічними каналами;

• друга – невиконання норм та вимог з ТЗІ, внаслідок якого створюються передумови для порушення конфіденційності, цілісності і доступності інформації або її витоку технічними каналами;

• третя – невиконання інших вимог з ТЗІ.

У разі виявлення порушення першої категорії вживають такі заходи:

- голова комісії негайно доповідає керівництву підприємства для прийняття рішення про припинення робіт, які проводились з порушенням норм і вимог ТЗІ, та про факт порушення;
- здійснюються заходи з усунення порушень у терміни, погоджені з підрозділом, на який покладено забезпечення ТЗІ;
- організовується в установленому порядку розслідування причин, які призвели до порушень, з метою недопущення їх у подальшому і притягнення осіб, які припустили порушення нормативно-правових актів з питань ТЗІ, до відповідальності згідно із законодавством України.

Дозвіл на відновлення робіт, під час виконання яких були виявлені порушення норм і вимог ТЗІ першої категорії, дає керівник підприємства

за погодженням з підрозділом, на який покладено забезпечення ТЗІ після усунення порушень і перевірки достатності й ефективності вжитих заходів з ТЗІ.

Керівництво підприємства зобов'язано надавати комісії повну інформацію стосовно впроваджених заходів з ТЗІ та сприяти проведенню їх перевірки.

4.3 Порядок контролю за станом технічного захисту інформації

Метою контролю є виявлення можливих технічних каналів витоку інформативного (небезпечного) сигналу (проведення спецдосліджень), вироблення заходів, що забезпечують його приховування, оцінка достатності й ефективності вжитих заходів захисту, оперативний контроль за станом технічного захисту каналів витоку інформативного сигналу.

Технічний канал витоку вважається захищеним, якщо сигнал не перевищує встановленого нормативною документацією відношення "інформативний сигнал/шум".

Пристрої захисту і захищені технічні засоби вважаються справними, якщо їх параметри відповідають вимогам експлуатаційних документів.

Контроль за виконанням організаційних та підготовчих технічних заходів щодо захисту інформації здійснюється візуальним оглядом прокладки проводів і кабелів, що виходять за межі об`єкта захисту, а також технічних засобів захисту та захищеної техніки.

У ході перевірки визначаються:

– наявність електромагнітного зв`язку між лініями ОТЗ та ДТЗ (проходження в одному кабелі чи джгуті), між різними видами ОТЗ та ДТЗ (спільний пробіг проводів систем пожежно-охоронної сигналізації, часофікації, радіотрансляції);

– наявність виходів ліній зв`язку, сигналізації, часофікації, радіотрансляції за межі виділених приміщень;

– наявність незадіяних ОТЗ, ДТЗ, проводів, кабелів;

– можливість відключення ОТЗ на період проведення конфіденційних переговорів або важливих нарад;

– рознесення джерел електромагнітних та акустичних полів на максимально можливу відстань у межах виділених приміщень;

– виконання заземлення апаратури, яке виключає можливість утворення петель з проводів та екранів;

– рознесення кабелів електроживлення ОТЗ та ДТЗ з метою виключення наводок небезпечних сигналів;

– виконання розведення кіл електроживлення екранованим або крученим кабелем;

– наявність можливості відключення електроживлення ОТЗ під час знеструмлення мережі; відхилення параметрів електроживлення від норм, заданих в ТУ, під час появи несправностей у колах живлення.

У процесі проведення спецдосліджень, перевірки ефективності технічних заходів захисту підлягають інструментальному контролю ОТЗ і лінії зв`язку.

У ході контролю перевіряються електромагнітні поля інформативних (небезпечних) сигналів у широкому діапазоні частот навколо апаратури та кабельних з`єднань ОТЗ, наявність інформативних (небезпечних) сигналів у колах, проводах електроживлення та заземленні ОТЗ та ДТЗ.

Під час спецдосліджень визначається радіус, за межами якого відношення "інформативний сигнал/шум" менше гранично допустимої величини. Проводяться вимірювання і розрахунок параметрів інформативного (небезпечного) сигналу, виявляється можливість його витоку каналами ПЕМВН, визначаються фактичні значення його параметрів у каналах витоку, проводиться порівняння фактичних параметрів з нормованими.

У випадку перевищення допустимих значень розробляються захисні заходи, використовуються засоби захисту (екранування джерел випромінювання, встановлення фільтрів, стабілізаторів, засобів активного захисту).

Після проведення спецдосліджень, вироблення та впровадження засобів захисту проводиться контроль за ефективністю застосованих технічних засобів захисту.

У процесі роботи технічних засобів і захищеної техніки, у міру необхідності, проводиться оперативний контроль за ефективністю захисту каналів витоку інформативного (небезпечного) сигналу.

Результати контролю (спецдосліджень) оформляються актом, складеним у довільній формі, підписуються перевіряючим та затверджуються Керівником підприємства.

4.4 Визначення інформаційних і технічних ресурсів, а також об'єктів інформаційної діяльності в підприємстві що підлягають захисту

Об’єктом технічного захисту є інформація, що становить державну або іншу передбачену законодавством України таємницю, ІзОД, що є державною власністю чи передана державі у володіння, користування, розпорядження (далі – інформація з обмеженим доступом, ІзОД).

4.5 Категоріювання об'єктів інформаційної діяльності підприємства

Категоріюванню підлягають об'єкти, в яких обговорюється, мається, пересилається, приймається, перетворюється, накопичується, обробляється, відображається й зберігається (дали – циркулює) інформація з обмеженим доступом (ІзОД).

До об'єктив, що підлягають категоріюванню, відносяться:

- інформаційні системи (ІС) та засоби обчислювальною техніки (ЗОТ), що діють й проектуються;
- технічні засоби, яки призначені для роботи з ІзОД та не відносяться до ІС, за винятком тих, що засновані на криптографічних методах захисту;
- приміщення, призначені для проведення нарад, конференцій, обговорень тощо з використанням ІзОД;
- приміщення, в яких розміщені ІС, ЗОТ, інші технічні засоби, призначені для роботи з ІзОД, у тому числи й основані на криптографічних методах захисту.

Категоріювання проводиться з метою вживання обґрунтованих заходив щодо технічного захисту ІзОД, яка циркулює на об`єктах, вид витоку каналами побічних електромагнітних випромінювань й наводок, а також акустичних (віброакустичних) полів.

Установлюються чотири категорії об'єктів залежно вид правового режиму доступу до інформації, що циркулює в них:

- до першою категорії відносяться об'єкти, в яких циркулює інформація, що містить відомості, яки становлять державну таємницю, для якою встановлено гриф обмеження доступу "особливої важливості";
- до другою категорії відносяться об’єкти, в яких циркулює інформація, що містить відомості, яки становлять державну таємницю, для якою встановлено гриф секретності "цілком таємно";
- до третьою категорії відносяться об'єкти, в яких циркулює інформація, що містить відомості, яки становлять державну таємницю, для якою встановлено гриф секретності "таємно", а також інформація, що містить відомості, яки становлять іншу передбачену законом таємницю, розголошення якою завдає шкоди особи, суспільству й держави;
- до четвертою категорії відносяться об'єкти, в яких циркулює службова та ІзОД.

4.6 Порядок проведення робіт з категоріювання об'єктів

Для проведення робіт з категоріювання об`єктів інформаційної діяльності підприємства наказом керівника підприємства призначається комісія. У наказі визначається мета створення комісії, її склад, об'єкти, що підлягають категоріюванню, строки подання результатів.

Комісія з категоріювання визначає:

- вищий гриф обмеження доступу інформації, що циркулює на об'єкти;
- підставу для категоріювання (первинне, планове, у зв`язку зі змінами).

За результатами роботи комісію складається акт, в яких наводяться зазначені відомості, раніше встановлена категорія та прийняте рішення про категоріювання. Акти затверджуються керівником підприємства.

Під час проведення робіт з категоріювання об`єктів підприємства, на яких циркулює інформація, що містить державну таємницю, враховуються додаткові вимоги та складаються відповідні акти;

Повторне категоріювання об'єкта проводиться у випадку змини грифа секретності інформації, що циркулює на об'єкті, і (або) умов розміщення технічних засобів, але не рідше одного разу в 5 років.

4.7 Засекречування та розсекречування матеріальних носіїв інформації

Перелік посад, які дають право посадовим особам, що їх займають, надавати матеріальним носіям секретної інформації грифи обмеження доступу, затверджується керівником органу державної влади, що провадить діяльність, пов'язану з державною таємницею.

Засекречування матеріальних носіїв інформації здійснюється шляхом надання відповідному документу, виробу або іншому матеріальному носію інформації гриф обмеження доступу.

Реквізити кожного матеріального носія секретної інформації мають містити гриф обмеження доступу, який відповідає ступеню обмеження доступу інформації, встановленому рішенням державного експерта з питань таємниць, – "особливої важливості", "цілком таємно", "таємно", дату та строк засекречування матеріального носія секретної інформації, що встановлюється з урахуванням передбачених статтею 13 Закону України “Про державну таємницю” строків дії рішення про віднесення інформації до державної таємниці, підпис, його розшифрування та посаду особи, яка надала зазначений гриф, а також посилання на відповідний пункт (статтю) Зводу відомостей, що становлять державну таємницю.

Якщо реквізити, зазначені у частині другій цієї статті, неможливо нанести безпосередньо на матеріальний носій секретної інформації, вони мають бути зазначені у супровідних документах.

Забороняється надавати грифи обмеження доступу, передбачені цим Законом, матеріальним носіям іншої таємної інформації, яка не становить державної таємниці, або ІзОД.

Ступені обмеження доступу науково-дослідних, дослідно-конструкторських і проектних робіт, які виконуються в інтересах забезпечення національної безпеки та оборони держави, встановлюються державним експертом з питань таємниць, який виконує свої функції у сфері діяльності замовника, разом з підрядником.

Звід відомостей, що становлять державну таємницю, формує та публікує в офіційних виданнях Служба безпеки України на підставі рішень державних експертів з питань таємниць.

На підставі та в межах Зводу відомостей, що становлять державну таємницю, з метою конкретизації та систематизації даних про секретну інформацію в Підприємстві можуть створюватися розгорнуті переліки відомостей, що становлять державну таємницю.

Розгорнуті переліки відомостей, що становлять державну таємницю, не можуть суперечити Зводу відомостей, що становлять державну таємницю.

У разі включення до Зводу відомостей, що становлять державну таємницю, або до розгорнутих переліків цих відомостей інформації, яка не відповідає категоріям і вимогам, передбаченим статтею 8 Закону України “Про державну таємницю”, або порушення встановленого порядку віднесення інформації до державної таємниці заінтересовані громадяни та юридичні особи мають право оскаржити відповідні рішення до суду. З метою недопущення розголошення державної таємниці судовий розгляд скарг може проводитися в закритих засіданнях відповідно до Закону України “Про державну таємницю”.

РОЗДІЛ 5 ЗАХИСТ ІНФОРМАЦІЇ ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ

5.1 Основні положення

Об’єктом технічного захисту є інформація, що становить державну або іншу передбачену законодавством України таємницю, ІзОД, що є державною власністю чи передана державі у володіння, користування, розпорядження
(далі – інформація з обмеженим доступом, ІзОД).

Інформація з обмеженим доступом (ІзОД) в процесі інформаційної діяльності (ІД), основними видами якої є одержання, використання, поширення та зберігання ІзОД, може зазнавати впливу загроз її безпеці (далі – загроза), у результаті чого може відбутися її витік або порушення цілісності інформації.

Схильність ІзОД до впливу загроз визначає її вразливість.

Здатність системи захисту інформації протистояти впливу загроз визначає захищеність ІзОД.

Зміст та послідовність робіт з протидії загрозам або їхньої нейтралізації повинні відповідати зазначеним в ДСТУ 3396.0–96 етапам функціонування системи захисту інформації і полягає в:

– проведенні обстеження підприємства, установи, організації (далі – підприємство);

– розробленні і реалізації організаційних, первинних технічних, основних технічних заходів з використанням засобів забезпечення ТЗІ;

– прийманні робіт з ТЗІ;

– атестації засобів (систем) забезпечення ІД на відповідність вимогам нормативних документів з ТЗІ.

Порядок проведення робіт з ТЗІ або окремих їхніх етапів установлюється наказом (розпорядженням) керівника підприємства.

Роботи повинні виконуватися під керівництвом спеціалістів з ТЗІ.

Для участі в роботах, подання методичної допомоги, оцінювання повноти та якості реалізації заходів захисту можуть залучатися спеціалісти з ТЗІ інших організацій, які мають ліцензію органа, уповноваженого Кабінетом Міністрів України.

Об’єкт, мету і завдання ТЗІ визначають і встановлюють особи, які володіють, користуються, розпоряджаються ІзОД у межах прав і повноважень, наданих законами України, підзаконними актами та нормативними документами системи ТЗІ.

Середовищем поширення носіїв ІзОД можуть бути лінії зв’язку, сигналізації, керування, енергетичні мережі, прикінцеве і проміжне обладнання, інженерні комунікації і споруди, огороджувальні будівельні

конструкції, а також світлопроникні елементи будинків і споруд (отвори), повітряне, водне та інші середовища, грунт, рослинність тощо.

Витік або порушення цілісності ІзОД (спотворення, модифікація, руйнування, знищення) можуть бути результатом реалізації загроз безпеці інформації (далі – загроза).

Технічному захисту підлягає інформація з обмеженим доступом, носіями якої є поля і сигнали, що утворюються в результаті роботи технічних засобів пересилання, оброблення, зберігання, відображення інформації (ОТЗ), а також допоміжних технічних засобів і систем (ДТЗ).

До ОТЗ відносяться:

– засоби і системи телефонного, телеграфного (телетайпного), директорського, гучномовного, диспетчерського, внутрішнього, службового та технологічного зв`язку;

– засоби і системи звукопідсилення, звукозапису та звуковідтворення;

– пристрої, що утворюють дискретні канали зв`язку: абонентська апаратура із засобами відображення та сигналізації, апаратура підвищення достовірності пересилання, каналоутворююча тощо;

– апаратура перетворення, оброблення, пересилання і приймання відеоканалів, що містять факсимільну інформацію.

ОТЗ можуть бути захищеними і незахищеними.

До допоміжних технічних засобів і систем відносяться:

– засоби і системи спеціальної охоронної сигналізації (на відкриття дверей, вікон та проникнення до приміщення сторонніх осіб), пожежної сигналізації (з датчиками, що реагують на дим, світло, тепло, звук);

– система дзвінкової сигналізації (виклик секретаря, вхідна сигналізація);

– контрольно-вимірювальна апаратура (КВА);

– засоби і системи кондиціонування (датчики температури, вологості, кондиціонери);

– засоби і системи провідної радіотрансляційної мережі та приймання програм радіомовлення і телебачення (абонентські гучномовці системи радіомовлення та оповіщення, радіоприймачі та телевізори);

– засоби і системи часофікації (електронні годинники, вторинні електрогодинники);

– засоби і системи електроосвітлення та побутового електрообладнання (світильники, люстри, настільні і стаціонарні вентилятори, електронагрівальні прилади, холодильники, паперорізальні машини, провідна мережа електроосвітлення);

– електронна та електрична оргтехніка.

ДТЗ можуть бути захищеними і незахищеними.

Елементи ОТЗ та ДТЗ можуть являти собою зосереджені випадкові антени (апаратура та її блоки) або розподілені випадкові антени (кабельні лінії та проводи).

Зазначеними елементами можуть бути:

– кінцеві технічні засоби і прилади;

– кабельні мережі та розводки, що з`єднують пристрої та обладнання;

– комутаційні пристрої (комутатори, кроси, бокси тощо);

– елементи заземлення та електроживлення.

ОТЗ, застосовувані для оброблення інформації з обмеженим доступом, називаються основними технічними засобами (ОТЗ).

Роботи із захисту інформації з обмеженим доступом від витоку каналами ПЕМВН складаються з організаційних, підготовчих технічних, технічних заходів і контролю за виконанням заходів технічного захисту інформації (ТЗІ) та за ефективністю цього захисту.

Організаційні і підготовчі заходи щодо технічного захисту інформації проводяться одночасно і є першим етапом робіт, технічні заходи – наступним етапом робіт.

Заходи щодо ТЗІ і контролю за його ефективністю можуть виконуватись організаціями, що мають ліцензію Державної служби України з питань технічного захисту інформації (ДСТЗІ) на право надання послуг у галузі ТЗІ

5.2. Організаційні заходи

На етапі проведення організаційних заходів потрібно:

– визначити перелік відомостей з обмеженим доступом, що підлягають технічному захисту (визначає власник інформації згідно з чинним законодавством України);

– обґрунтувати необхідність розроблення і реалізації захисних заходів з урахуванням матеріальної або іншої шкоди, яка може бути завдана внаслідок можливого порушення цілісності ІзОД чи її витоку технічними каналами;

– установити перелік виділених приміщень, в яких не допускається реалізація загроз та витік інформації з обмеженим доступом;

– визначити перелік технічних засобів, що повинні використовуватися як ОТЗ;

– визначити технічні засоби, застосування яких не обґрунтовано службовою та виробничою необхідністю та які підлягають демонтажу;

– визначити наявність задіяних і незадіяних повітряних, наземних, настінних та закладених у приховану каналізацію кабелів, кіл і проводів, що уходять за межі виділених приміщень;

– визначити системи, що підлягають демонтажу, потребують переобладнання кабельних мереж, кіл живлення, заземлення або установлення в них захисних пристроїв.

За результатами обстеження складається акт довільної форми з переліком виконаних заходів і прикладанням (за необхідністю):

– переліку ОТЗ, розміщених у виділених приміщеннях;

– плану виділених приміщень із зазначенням місць установлення ОТЗ, а також схем прокладання кабелів, проводів, кіл;

– переліку технічних засобів, кабелів, кіл, проводів, що підлягають демонтажу.

Акт підписується виконавцем робіт і затверджується керівником організації (підприємства).

5.3. Підготовчі технічні заходи

Підготовчі технічні заходи включають у себе первинні заходи блокування електроакустичних перетворювачів і ліній зв`язку, які виходять за межі виділених приміщень.

Блокування ліній зв`язку може виконуватися такими способами:

– відключенням ліній зв`язку ОТЗ та ДТЗ або встановленням найпростіших схем захисту;

– демонтажем технічних засобів, кабелів, кіл, проводів, що уходять за межі виділених приміщень;

– видаленням за межі виділених приміщень окремих елементів технічних засобів, які можуть бути джерелом виникнення каналу витоку інформації.

Блокування каналів можливого витоку ІзОД у системах міського та відомчого телефонного зв`язку може здійснюватися:

– відключенням дзвінкових (викличних) ліній телефонного апарата;

– установленням у колі телефонного апарата безрозривної розетки для тимчасового відключення;

– установленням найпростіших пристроїв захисту.

Запобігання витоку ІзОД через діючі системи гучномовного диспетчерського та директорського зв`язку здійснюється застосуванням таких захисних заходів:

– установленням у викличних колах вимикачів для розриву кіл;

– установленням на вході гучномовців вимикачів (реле), які дають можливість розривати кола по двох проводах;

– забезпеченням можливості відключення живлення мікрофонних підсилювачів;

– установленням найпростіших пристроїв захисту.

Захист ІзОД від витоку через радіотрансляційну мережу, що виходить за межі виділеного приміщення, може бути забезпечений:

– відключенням гучномовців по двох проводах;

– вмиканням найпростіших пристроїв захисту.

Для служби оповіщення слід виділити чергові абонентські пристрої поза виділеними приміщеннями; кола до цих пристроїв повинні бути прокладені окремим кабелем.

Блокування каналів витоку ІзОД через кола вторинних електрогодинників системи електрочасофікації здійснюється відключенням їх на період проведення закритих заходів.

Запобігання витоку ІзОД через системи пожежної та охоронної сигналізацій здійснюється відключенням датчиків пожежної та охоронної сигналізації на період проведення важливих заходів, що містять ІзОД, або застосуванням датчиків, які не потребують спеціальних заходів захисту.

З метою виключення можливості витоку ІзОД під час роботи незахищених технічними засобами телевізорів, радіоприймачів, звукопідсилювальної та звуковідтворювальної апаратури необхідно на період проведення важливих заходів зазначені пристрої відключати від мережі електроживлення по двох проводах.

Блокування витоку ІзОД через системи електронної оргтехніки та кондиціонування може бути забезпечене такими заходами:

– розташуванням зазначених систем усередині контрольованої території без винесення окремих компонентів за її межі;

– електроживленням систем від трансформаторної підстанції, що знаходиться всередині контрольованої території.

При невиконанні зазначених вище умов системи повинні відключатися від мережі електроживлення по двох проводах.

Захист ІзОД від витоку через кола електроосвітлення та електроживлення побутової техніки повинен здійснюватися підключенням зазначених кіл до окремого фідера трансформаторної підстанції, до якого не допускається підключення сторонніх користувачів.

У випадку невиконання зазначеної вимоги електропобутові прилади на період проведення закритих заходів повинні відключатися від кіл електроживлення.

5.4. Технічні заходи

Технічні заходи є основним етапом робіт з технічного захисту ІзОД і полягають у встановленні ОТЗ, забезпеченні ОТЗ та ДТЗ пристроями ТЗІ.

Під час вибору, встановлення, заміни технічних засобів слід керуватися паспортами, технічними описами, інструкціями з експлуатації, рекомендаціями з установлення, монтажу та експлуатації, що додаються до цих засобів.

ОТЗ повинні розміщуватися, по можливості, ближче до центру будинку або в бік найбільшої частини контрольованої території. Складові елементи ОТЗ повинні розміщуватися в одному приміщенні або в суміжних.

Якщо зазначені вимоги невиконувані, слід вжити додаткових заходів захисту:

– установити високочастотні ОТЗ в екрановане приміщення (камеру);

– установити в незахищені канали зв`язку, лінії, проводи і кабелі спеціальні фільтри та пристрої.

– прокласти проводи і кабелі в екранувальних конструкціях;

– зменшити довжину паралельного пробігу кабелів і проводів різних систем з проводами та кабелями, що несуть ІзОД;

– виконати технічні заходи щодо захисту ІзОД від витоку колами заземлення та електроживлення.

До засобів технічного захисту відносяться:

– фільтри-обмежувачі та спеціальні абонентські пристрої захисту для блокування витоку мовної ІзОД через двопровідні лінії телефонного зв`язку, системи директорського та диспетчерського зв`язку;

– пристрої захисту абонентських однопрограмних гучномовців для блокування витоку мовної ІзОД через радіотрансляційні лінії;

– фільтри мережеві для блокування витоку мовної ІзОД колами електроживлення змінного (постійного) струму;

– фільтри захисту лінійні (високочастотні) для встановлення в лініях апаратів телеграфного (телекодового) зв`язку;

– генератори лінійного зашумлення;

– генератори просторового зашумлення;

– екрановані камери спеціальної розробки.

Для телефонного зв`язку, не призначеного для пересилання ІзОД, рекомендується застосовувати апарати вітчизняного виробництва, сумісні з пристроями захисту. Телефонні апарати іноземного виробництва можуть застосовуватися за умови проходження спецдосліджень і позитивного висновку компетентних організацій системи ТЗІ про їх сумісність з пристроями захисту.

Вибір методів і способів захисту елементів ОТЗ та ДТЗ, що мають мікрофонний ефект, залежить від величини їх вхідного опору на частоті 1 кГц.

Елементи з вхідним опором менше 600 Ом (головки гучномовців, електродвигуни вентиляторів, трансформатори тощо) рекомендується відключати по двох проводах або встановлювати у розрив кіл пристрої захисту з високим вихідним опором для зниження до мінімальної величини інформативної складової струму.

Елементи з високим вхідним опором (електричні дзвінки, телефонні капсулі, електромагнітні реле) рекомендується не тільки відключати від кіл, а й замикати на низький опір або закорочувати, щоб зменшити електричне поле від цих елементів, зумовлене напругою, наведеною під час впливу акустичного поля. При цьому слід враховувати, що обраний спосіб захисту не повинен порушувати працездатність технічного засобу і погіршувати його технічні параметри.

Високочастотні автогенератори, підсилювачі (мікрофонні, приймання, пересилання, гучномовного зв`язку) та інші пристрої, що містять активні

елементи, рекомендується відключати від ліній електроживлення у "черговому режимі" або "режимі чекання виклику".

Підключення пристроїв захисту слід проводити без порушення або зміни електричної схеми і ОТЗ, і ДТЗ.

Захист ІзОД від витоку кабелями та проводами рекомендується здійснювати шляхом:

– застосування екранувальних конструкцій;

– роздільного прокладання кабелів ОТЗ та ДТЗ.

При неможливості виконання вимог щодо рознесення кабелів електроживлення ОТЗ та ДТЗ електроживлення останніх слід здійснювати або екранованими кабелями, або від розділових систем, або через мережеві фільтри.

Не допускається утворення петель та контурів кабельними лініями. Перехрещення кабельних трас різного призначення рекомендується здійснювати під прямим кутом одна до одної.

Електроживлення ОТЗ повинно бути стабілізованим за напругою та струмом для нормальних умов функціонування ОТЗ і забезпечення норм захищеності.

У колах випрямного пристрою джерела живлення необхідно встановлювати фільтри нижніх частот. Фільтри повинні мати фільтрацію по симетричних і несиметричних шляхах поширення.

Необхідно передбачити відключення електромережі від джерела живлення ОТЗ під час зникнення напруги в мережі, під час відхилення параметрів електроживлення від норм, заданих в ТУ, та під час появи несправностей у колах електроживлення.

Усі металеві конструкції ОТЗ (шафи, пульти, корпуси розподільних пристроїв та металеві оболонки кабелів) повинні бути заземлені.

Заземлення ОТЗ слід здійснювати від загального контуру заземлення, розміщеного в межах контрольованої території, з опором заземлення за постійним струмом відповідно до вимог стандартів.

Система заземлення повинна бути єдиною для всіх елементів ОТЗ і будуватися за радіальною схемою.

Утворення петель і контурів у системі заземлення не допускається.

Екрани кабельних ліній ОТЗ, що виходять за межі контрольованої території, повинні заземлятися в кросах від загального контуру заземлення в одній точці для виключення можливості утворення петель по екрану та корпусах.

У кожному пристрої повинна виконуватися умова безперервності екрана від входу до виходу. Екрани слід заземляти тільки з одного боку. Екрани кабелів не повинні використовуватися як другий провід сигнального кола або кола живлення.

Екрани кабелів не повинні мати електричного контакту з металоконструкціями. Для монтажу слід застосовувати екрановані кабелі з ізоляцією або одягати на екрани ізоляційну трубку.

У довгих екранованих лініях (мікрофонних, лінійних, звукопідсилювальних) рекомендується ділити екран на ділянки для одержання малих опорів для високочастотних струмів і кожну ділянку заземляти тільки з одного боку.

Результати виконання технічних заходів оформляються актом приймання робіт, складеним у довільній формі, підписуються виконавцем робіт і затверджуються Керівником підприємства.

РОЗДІЛ 6 ЗАХИСТ ІНФОРМАЦІЇ ПІД ЧАС ВИКОРИСТАННЯ ЗАСОБІВ КОПІЮВАЛЬНО–РОЗМНОЖУВАЛЬНОЇ ТЕХНІКИ

6.1 Основні положення

Під час оброблення документів засобами КРТ електричні струми інформативних сигналів спричиняють виникнення побічного електромагнітного випромінення (ПЕМВ), яке може бути носієм ІзОД і реєструватися технічними засобами розвідки за межами контрольованої зони (КЗ) об'єкта. Крім того, ПЕМВ може наводити електрорушійну силу (ЕРС) в розташованих поряд з джерелом випромінення колах електроживлення, заземлення, лініях зв'язку тощо. В разі виходу таких кіл і ліній за межі КЗ наводи інформативних сигналів можуть реєструватися технічними засобами розвідки.

Згідно з "Класифікатором засобів копіювально-розмножувальної техніки" засоби КРТ поділяються на два класи:

клас А – засоби КРТ, що у процесі роботи не створюють інформативні ПЕМВН; до цього класу віднесено світлокопіювальні, фотокопіювальні, термокопіювальні, мікрографічні, електрофотографічні аналогові апарати з оптичним перенесенням зображення з оригіналу на копію;

клас Б – електрофотографічні цифрові апарати з оптично-дискретним перенесенням зображення з оригіналу на копію.

Клас Б поділяється на два підкласи:

підклас І – засоби КРТ з циклічним інформативним сигналом (цифрові електрофотографічні апарати);

підклас ІІ – засоби КРТ з одноразовим інформативним сигналом (ризографи).

Інформативна складова в електромагнітному випроміненні присутня лише в цифрових КРА (клас Б), які реалізують оптичне сканування зображення оригіналу з його наступним цифровим розкладанням, подальшою передачею цифрового електричного сигналу та лазерною розгорткою інформативного сигналу при створенні копії. В цифрових КРА існує реальна загроза витоку ІзОД. Під час роботи таких апаратів можливий витік інформації каналами ПЕМВН.

6.2 Вимоги до захисту інформації

Захист інформації забезпечується, якщо задовольняється одна з таких вимог:

– використовуються КРА класу А;

– у разі використання КРА класу Б здійснено заходи ТЗІ, які забезпечують виконання відповідних норм захисту згідно з НД ТЗІ.

6.3 Організація технічного захисту інформації

Захист інформації здійснюється в порядку, встановленому нормативними документами системи ТЗІ (НД ТЗІ) з розроблення та впровадження заходів ТЗІ на об'єктах інформаційної діяльності з уточненнями, які визначаються особливостями використання технічних засобів:

– у приміщенні не циркулює інша інформація, крім тієї, що обробляється засобами КРТ;

– у приміщенні, разом з ІзОД, що обробляється КРТ, циркулює також інша інформація.

Якщо у приміщенні не циркулює інша інформація, крім тієї, що обробляється засобами КРТ, то в разі використання КРА класу А під час розроблення та впровадження заходів ТЗІ слід виходити з того, що технічні канали витоку інформації (ТКВІ) можуть створювати закладні пристрої з оптичними перетворювачами.

У разі використання КРА класу Б, слід виходити з можливості існування ТКВІ шляхом ПЕМВН та закладних пристроїв з оптичними та електромагнітними перетворювачами.

Якщо у приміщенні, разом з ІзОД, що обробляється КРТ, циркулює також інша інформація, то необхідно проводити повний обсяг робіт, передбачених загальним порядком розроблення заходів з ТЗІ, що враховує загрози витоку технічними каналами інформації, що обробляється засобами КРТ, а також іншої інформації, що циркулює в цьому ж приміщенні.

У разі використання КРА класу Б в процесі розроблення заходів з ТЗІ необхідно враховувати вимоги НД ТЗІ.

При цьому слід передбачати:

– встановлення КЗ, за межами якої виконуються норми захисту;

– вилучення незадіяних (задіяних) допоміжних технічних засобів, застосування яких не обгрунтовано виробничою необхідністю, а також вилучення з КЗ незадіяних (задіяних) кабелів та проводів, що виходять за межі КЗ, на які можливе наведення ЕРС інформативними ПЕМВ;

– застосування захищених засобів КРТ;

– блокування ТКВІ за допомогою засобів ТЗІ (пасивних, активних тощо).

Технічні засоби, що використовуються з метою забезпечення технічного захисту інформації, охорона якої забезпечується державою, повинні мати дозвіл уповноваженого органу і міститися у відповідних переліках.

Контроль ефективності захисту інформації здійснюється згідно з чинними НД ТЗІ.

Заходи з ТЗІ доцільно виконувати одночасно з захистом іншої інформації, що циркулює на об'єкті, де використовуються засоби КРТ.

Оброблення ІзОД можливе лише після атестації комплексу ТЗІ на відповідність вимогам НД ТЗІ.

6.4 Рекомендації з захисту інформації, що обробляється засобами КРТ класу Б

З метою ТЗІ від витоку мережами електроживлення трансформаторну підстанцію низької напруги, кабелі електроживлення, усі елементи заземлення та засоби ТЗІ, що підключаються до мережі живлення, рекомендується розміщувати в межах КЗ.

Забороняється підключення до низької сторони трансформаторної підстанції споживачів електроенергії, що розміщуються за межами КЗ. Якщо ця вимога не виконується, то необхідно вживати додаткові заходи із захисту (пасивні та активні), які визначаються за результатами обстеження згідно з ДСТУ 3396.1–96 та спецдосліджень.

Кола електроживлення КРТ на ділянці від технічних засобів до розподільної системи чи захисних мережевих фільтрів рекомендується прокладати в жорстких екранованих конструкціях, кабелі прокладати окремими пакетами, без утворення петель, перетинання здійснювати під прямим кутом без електричного контакту екрануючих оболонок кабелів. У разі неможливості виконання вимог щодо рознесення кабелів, електроживлення засобів КРТ повинно забезпечуватися екранованими кабелями від розділювальних систем або через мережеві фільтри.

Опір контуру заземлення не повинен перевищувати 4 Ом, заземлюючі провідники повинні мати перехідний опір з`єднання не більше 600 мкОм та розміщуватися в межах КЗ (можливе використання глибинного заземлювача). Забороняється використовувати для заземлення металеві конструкції водопостачання, опалення, газофікації тощо. Якщо заземлення виконати утруднено, то допускається виконати занулення КРТ.

Екрануючі конструкції засобів КРТ та кабелів повинні створювати екранований замкнутий об`єм.

У разі недостатності пасивних заходів ТЗІ вживаються заходи активного захисту – просторове чи лінійне зашумлення.

6.5 Класифікатор засобів копіювально-розмножувальної техніки

Об`єктом класифікації є технічні засоби оргтехніки, що грунтуються на неполіграфічних методах оперативного копіювання та розмноження документації.

Ознаки, за якими проводиться класифікація засобів КРТ, визначаються загрозами для оброблюваної інформації, що спричиняються роботою таких засобів, зокрема фізичними процесами перенесення зображення – методами копіювання.

Загрозою для інформації, що обробляється засобом КРТ, є її витік технічними каналами (ДСТУ 3396.2–97) через:

– побічні електромагнітні випромінення,

– електромагнітні наводи в мережі живлення, заземлення та інші загрози.

Засоби копіювально-розмножувальної техніки – світлокопіювальні, фотокопіювальні, термокопіювальні та мікрографічні апарати у процесі роботи не створюють інформативні побічні електромагнітні випромінення і наводи (ПЕМВН).

Електрофотографічні копіювальні апарати поділяються на аналогові – з оптичним перенесенням зображення з оригіналу на копію, та цифрові – з оптично–дискретним перенесенням зображення.

Електрофотографічні копіювальні апарати аналогового типу у процесі роботи не створюють інформативні ПЕМВН. Цифрові електрофотографічні копіювальні апарати створюють інформативні ПЕМВН, що можуть бути носіями інформації, яка обробляється. Під час роботи таких апаратів можливий витік інформації, що обробляється КРТ, каналами побічних електромагнітних випромінень (ПЕМВ) і наведень у мережі живлення та заземлення, а також інші загрози.

РОЗДІЛ 7 ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНІЙ СИСТЕМІ ПІДПРИЄМСТВА

7.1 Загальні положення

Інформаційні ресурси держави або суспільства в цілому, а також окремих організацій і фізичних осіб являють собою певну цінність, мають відповідне матеріальне вираження і вимагають захисту від різноманітних за своєю сутністю впливів, які можуть призвести до зниження цінності інформаційних ресурсів.

Впливи, які призводять до зниження цінності інформаційних ресурсів, називаються несприятливими. Потенційно можливий несприятливий вплив називається загрозою.

Захист інформації, що обробляється в комп’ютерних системах (КС), полягає в створенні і підтримці в дієздатному стані системи заходів, як технічних (інженерних, програмно-апаратних), так і нетехнічних (правових, організаційних), що дозволяють запобігти або ускладнити можливість реалізації загроз, а також знизити потенційні збитки. Іншими словами, захист інформації спрямовано на забезпечення безпеки оброблюваної інформації і КС в цілому, тобто такого стану, який забезпечує збереження заданих властивостей інформації і КС, що її обробляє. Система зазначених заходів, що забезпечує захист інформації в КС, називається комплексною системою захисту інформації.

Істотна частина проблем забезпечення захисту інформації в КС може бути вирішена організаційними заходами. Проте, з розвитком інформаційних технологій спостерігається тенденція зростання потреби застосування технічних заходів і засобів захисту.

Правовою основою забезпечення технічного захисту інформації в Україні є Конституція України, Закони України "Про інформацію", "Про захист інформації в комп’ютерних системах", "Про державну таємницю", "Про науково-технічну інформацію", Концепція (основи державної політики) національної безпеки України, Концепція технічного захисту інформації в Україні, інші нормативно-правові акти, а також міжнародні договори України, що стосуються сфери інформаційних відносин.

До КС підприємства, згідно з встановленою НД ТЗІ 2.5–005 класифікацією, відносяться комп’ютерні системи, створені на базі локалізованого багатомашинного багатокористувачевого комплексу.

До складу КС підприємства входять обчислювальна система, фізичне середовище, в якому вона знаходиться і функціонує, користувачі КС та оброблювана інформація, у тому числі й технологія її оброблення. Під час забезпечення захисту інформації необхідно враховувати всі

характеристики зазначених складових частин, які мають вплив на реалізацію політики безпеки.

7.2 Основні загрози інформації в КС підприємства

Інформація в КС існує у вигляді даних, тобто представляється в формалізованому вигляді, придатному для обробки. Тут і далі під обробкою слід розуміти як власне обробку, так і введення, виведення, зберігання, передачу і т. ін. (ДСТУ 2226–93). Далі терміни “інформація” і “дані” використовуються як синоніми.

Інформація для свого існування завжди вимагає наявності носія. Як носій інформації може виступати поле або речовина. В деяких випадках у вигляді носія інформації може розглядатися людина. Втрата інформацією своєї цінності (порушення безпеки інформації) може статися внаслідок переміщення інформації або зміни фізичних властивостей носія.

При аналізі проблеми захисту від НСД інформації, яка може циркулювати в КС, як правило, розглядаються лише інформаційні об'єкти, що служать приймальниками/джерелами інформації, і інформаційні потоки (порції інформації, що пересилаються між об'єктами) безвідносно до фізичних характеристик їх носіїв.

Загрози оброблюваної в КС інформації залежать від характеристик ОС, фізичного середовища, персоналу і оброблюваної інформації. Загрози можуть мати або об'єктивну природу, наприклад, зміна умов фізичного середовища (пожежі, повені і т. і.) чи відмова елементів ОС, або суб'єктивну, наприклад, помилки персоналу чи дії зловмисника. Загрози, що мають суб'єктивну природу, можуть бути випадковими або навмисними. Спроба реалізації загрози називається атакою.

Із всієї множини способів класифікації загроз найпридатнішою для аналізу є класифікація загроз за результатом їх впливу на інформацію, тобто порушення конфіденційності, цілісності і доступності інформації.

Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею.

Інформація зберігає цілісність, якщо дотримуються встановлені правила її модифікації (видалення).

Інформація зберігає доступність, якщо зберігається можливість ознайомлення з нею або її модифікації відповідно до встановлених правил упродовж будь-якого певного (малого) проміжку часу.

Загрози, реалізація яких призводить до втрати інформацією якої-небудь з названих властивостей, відповідно є загрозами конфіденційності, цілісності або доступності інформації.

Загрози можуть впливати на інформацію не безпосередньо, а опосередковано. Наприклад, втрата КС керованості може призвести до нездатності КС забезпечувати захист інформації і, як результат, до втрати певних властивостей оброблюваної інформації.

7.3 Визначення несанкціонованого доступу

Під несанкціонованим доступом (НСД) слід розуміти доступ до інформації з використанням засобів, включених до складу КС, що порушує встановлені ПРД.

Несанкціонований доступ може здійснюватись як з використанням штатних засобів, тобто сукупності програмно-апаратного забезпечення, включеного до складу КС розробником під час розробки або системним адміністратором в процесі експлуатації, що входять у затверджену конфігурацію КС, так і з використанням програмно-апаратних засобів, включених до складу КС зловмисником.

До основних способів НСД відносяться:

• безпосереднє звертання до об'єктів з метою одержання певного виду доступу;

• створення програмно-апаратних засобів, що виконують звертання до об'єктів в обхід засобів захисту;

• модифікація засобів захисту, що дозволяє здійснити НСД;

• впровадження в КС програмних або апаратних механізмів, що порушують структуру і функції КС і дозволяють здійснити НСД.

Під захистом від НСД, слід розуміти діяльність, спрямовану на забезпечення додержання правил розмежування доступу (ПРД) шляхом створення і підтримки в дієздатному стані системи заходів із захисту інформації.

7.4 Основні напрями захисту

Комп’ютерна система являє собою організаційно-технічну систему, що об'єднує обчислювальну систему, фізичне середовище, персонал і оброблювану інформацію (малюнок). Прийнято розрізняти два основних напрями ТЗІ в КС — це захист КС і оброблюваної інформації від несанкціонованого доступу і захист інформації від витоку технічними каналами (оптичними, акустичними, захист від витоку каналами побічних електромагнітних випромінювань і наведень).

Кінцевою метою всіх заходів щодо захисту інформації, які реалізуються, є забезпечення безпеки інформації під час її обробки в АС. Захист інформації повинен забезпечуватись на всіх стадіях життєвого циклу КС, на всіх технологічних етапах обробки інформації і в усіх

режимах функціонування. Життєвий цикл КС включає розробку, впровадження, експлуатацію та виведення з експлуатації.

У випадку, якщо в КС планується обробка інформації, порядок обробки і захисту якої регламентується законами України або іншими нормативно-правовими актами (наприклад, інформація, що становить державну таємницю), то для обробки такої інформації в цій КС необхідно мати дозвіл відповідного уповноваженого державного органу. Підставою для видачі такого дозволу є висновок експертизи КС, тобто перевірки відповідності реалізованої КСЗІ встановленим нормам.

В процесі експертизи оцінюється КСЗІ КС в цілому. В тому числі виконується і оцінка реалізованих в ОС КС засобів захисту. Засоби захисту від НСД, реалізовані в обчислювальній системі, слід розглядати як підсистему захисту від НСД у складі КСЗІ. Характеристики фізичного середовища, персоналу, оброблюваної інформації, організаційної підсистеми істотно впливають на вимоги до функцій захисту, що реалізуються ОС.

Обчислювальна система комп’ютерної системи являє собою сукупність апаратних засобів, програмних засобів (в тому числі програм ПЗП), призначених для обробки інформації. Кожний з компонентів ОС може розроблятись і надходити на ринок як незалежний продукт.

Кожний з цих компонентів може реалізовувати певні функції захисту інформації, оцінка яких може виконуватись незалежно від процесу експертизи КС і має характер сертифікації. За підсумками сертифікації видається сертифікат відповідності реалізованих засобів захисту певним вимогам (критеріям). Наявність сертифіката на обчислювальну систему КС або її окремі компоненти може полегшити процес експертизи КС.

Як в процесі експертизи, так і сертифікації оцінка реалізованих функцій захисту інформації виконується відповідно до встановлених критеріїв. Ці критерії встановлюються НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу " (далі – Критерії).

Як КС можуть виступати:

- ЕОМ загального призначення або персональна ЕОМ;
- операційна система; прикладна або інструментальна програма (пакет програм);
- КЗЗ, що окремо поставляється, або підсистема захисту від НСД, наприклад, мережа, яка являє собою надбудову над ОС; локальна обчислювальна мережа, як сукупність апаратних засобів, ПЗ, що реалізує протоколи взаємодій, мережевої операційної системи і т. ін.;
- ОС комп’ютерної системи, яка реально функціонує;
- в найбільш загальному випадку – сама КС або її частина.

Коли для побудови КС використовуються компоненти, кожний або деякі з них мають сертифікат, що підтверджує, що ці компоненти

реалізують певні функції захисту інформації. Це, однак, не означає, що КС, яка складається з таких компонентів, буде реалізовувати всі ці функції.

Для гарантії останнього має бути виконано проектування КС з метою інтеграції засобів захисту, що надаються кожним компонентом, в єдиний комплекс засобів захисту. Таким чином, наявність сертифіката слід розглядати як потенційну можливість КС реалізовувати певні функції захисту оброблюваної інформації від певних загроз.

7.5 Політика безпеки інформації

Під політикою безпеки інформації слід розуміти набір законів, правил, обмежень, рекомендацій і т. ін., які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз. Термін "політика безпеки" може бути застосовано щодо організації, КС, ОС, послуги, що реалізується системою (набору функцій), і т. ін.

Політика безпеки інформації в КС є частиною загальної політики безпеки організації і може успадковувати, зокрема, положення державної політики у галузі захисту інформації.

Для кожної КС політика безпеки інформації може бути індивідуальною і може залежати від технології обробки інформації, що реалізується, особливостей ОС, фізичного середовища і від багатьох інших чинників.

КС може реалізовувати декілька різноманітних технологій обробки інформації. Тоді і політика безпеки інформації в такій КС буде складеною і її частини, що відповідають різним технологіям, можуть істотно відрізнятись.

Політика безпеки повинна визначати ресурси КС, що потребують захисту, зокрема установлювати категорії інформації, оброблюваної в КС. Мають бути сформульовані основні загрози для ОС, персоналу, інформації різних категорій і вимоги до захисту від цих загроз.

Як складові частини загальної політики безпеки інформації в КС мають існувати політики забезпечення конфіденційності, цілісності і доступності оброблюваної інформації.

Відповідальність персоналу за виконання положень політики безпеки має бути персоніфікована.

7.6 Характеристика обчислювальної підсистеми КС

Метою створення комп’ютерних систем підприємства є надання будь-якому користувачеві, у відповідності із захищеною технологією обробки інформації, потенційної можливості доступу до інформаційних ресурсів усіх комп’ютерів, що об’єднані в обчислювальну мережу.

Узагальнена функціонально–логічна структура обчислювальної системи КС підприємства включає:

– підсистему обробки інформації;

– підсистему взаємодії користувачів з КС;

– підсистему обміну даними.

Підсистема обробки інформації реалізує головну цільову функцію КС і складається із засобів обробки інформації, які утворюють основу інформаційно-обчислювальних ресурсів КС, що надаються користувачам (обчислення, пошук, зберігання та оброблення інформації). Принциповими її особливостями є багатофункціональність і можливість доступу до неї для будь-яких робочих станцій КС. Можливі обмеження визначаються тільки специфікою технологій, технічними й організаційними особливостями функціонування КС.

Як компоненти підсистеми можуть використовуватися універсальні високопродуктивні ЕОМ (у тому числі й ПЕОМ), спеціалізовані сервери обробки даних або надання послуг (сервери баз даних, друку тощо).

Підсистема взаємодії користувачів з КС забезпечує користувачам доступ до засобів підсистеми обробки інформації і подання отриманого від них ресурсу у вигляді результату обчислення, інформаційного масиву або графічного зображення у зручній та зрозумілій для користувача формі.

Компоненти підсистеми у функціональному відношенні є автономно замкненими та, як правило, не передбачається доступ до їх внутрішніх обчислювальних ресурсів зі сторони інших компонентів КС.

Як компоненти підсистеми можуть використовуватися ПЕОМ, що укомплектовані засобами введення та відображення інформації (робочі станції), дисплейні станції.

Підсистема обміну даними забезпечує взаємодію робочих станцій із засобами підсистеми обробки інформації, а також робочих станцій між собою на основі визначених правил, процедур обміну даними з реалізацією фаз встановлення, підтримання та завершення з’єднання. Підсистема забезпечує інформаційну взаємодію різних компонентів КС і об’єднує їх в єдине ціле як у структурному, так і у функціональному відношенні.

Підсистема обміну даними складається з пасивної мережі для обміну даними (кабельна мережа), активного мережевого обладнання (комутаторів, концентраторів, маршрутизаторів, шлюзів тощо), що об’єднує в єдине ціле пасивну мережу з обладнанням інших підсистем для забезпечення інформаційної взаємодії.

Як різновид підсистеми обміну даними можна розглядати структуровану кабельну систему – набір стандартних комутаційних елементів (кабелів, з’єднувачів, коннекторів, кросових панелей і спеціальних шаф та ін.), які дозволяють створювати регулярні структури передачі даних, що відносно легко розширюються.

Обчислювальні системи, за допомогою яких реалізуються підсистема обробки інформації та підсистема взаємодії користувачів з КС, укомплектовані:

засобами обчислювальної техніки;

периферійним обладнанням – пристроями друку, зберігання інформації тощо;

• комплексом програмного забезпечення обчислювальної системи;

• комплексом програмно-апаратних засобів захисту інформації.

У разі необхідності засоби обчислювальної техніки додатково можуть комплектуватися сумісними периферійними пристроями і відповідними модулями системного програмного забезпечення.

Комплекс програмного забезпечення обчислювальної системи складають:

- операційні системи серверів;
- операційні системи універсальних високопродуктивних ЕОМ;
- операційні системи робочих станцій;
- операційні системи, що забезпечують виконання мережевих функцій;
- програмні засоби, що підтримують реалізацію протоколів передачі даних обчислювальної мережі;
- програмні засоби активних компонентів мережі, що реалізують спеціальні алгоритми управління мережею;
- системи керування базами даних серверів, високопродуктивних універсальних ЕОМ, робочих станцій;
- програмні засоби забезпечення КЗЗ;
- функціональне програмне забезпечення.

Наведена функціонально-логічна структура КС може розглядатися як універсальна, в той час як фізична структура комп'ютерної системи може мати значно більшу кількість модифікацій в залежності від цілей та завдань, які вона повинна вирішувати, способу розподілу функцій між окремими технічними засобами, видів та можливостей технічних засобів, що застосовуються, інших специфічних особливостей, які враховуються під час проектування конкретної обчислювальної мережі.

7.7 Типові адміністративні та організаційні вимоги до КС підприємства стосовно питань ТЗІ

Типові адміністративні та організаційні вимоги до обчислювальної системи КС, умов її функціонування і забезпечення захисту інформації визначаються наступним.

Для КС в цілому та (або) для окремих (усіх) її компонентів у відповідності до вимог із захисту інформації від НСД повинен бути сформований перелік необхідних функціональних послуг захисту і визначено рівень гарантій їх реалізації.

Сервери, робочі станції, периферійні пристрої, інші технічні засоби обробки ІзОД повинні бути категорійовані згідно з вимогами нормативних документів із технічного захисту інформації, якщо це вимагається цими документами .

Засоби захисту інформації, інші технічні засоби та програмне забезпечення КС, що задіяні в КСЗІ, повинні мати підтвердження їхньої відповідності нормативним документам із захисту інформації (атестат, сертифікат відповідності, експертний висновок) і використовуватись згідно з вимогами, визначеними цими документами. Інших обмежень щодо типів технічних засобів обробки інформації та обладнання, видів програмного забезпечення не запроваджується.

Технічна та експлуатаційна документація на засоби захисту та обробки інформації, системне та функціональне програмне забезпечення належним чином класифіковані і для кожної категорії користувачів визначено перелік документації, до якої вони можуть отримати доступ. Доступ до документації фіксується у відповідних реєстрах. Порядок ведення реєстрів визначає СЗІ.

Сервери і робочі станції, що здійснюють зберігання та обробку ІзОД, повинні розташовуватися в приміщеннях, доступ до яких обслуговуючого персоналу та користувачів різних категорій здійснюється в порядку, що визначений СЗІ та затверджений керівником установи (організації).

Повинен здійснюватися контроль за доступом користувачів та обслуговуючого персоналу до робочих станцій, серверів КС і компонентів підсистеми обміну даними на всіх етапах життєвого циклу КС, а також періодичний контроль за цілісністю компонентів підсистеми обміну даними (з метою виявлення несанкціонованих відводів від компонентів підсистеми).

З метою забезпечення безперервного функціонування під час оброблення, зберігання та передачі ІзОД КС повинна мати можливість оперативного, без припинення її функціонування, проведення регламентного обслуговування, модернізації обчислювальної системи в цілому або окремих її компонентів. Порядок введення в експлуатацію нових компонентів, якщо це впливає на захист інформації в КС, визначається СЗІ.

Програмно–апаратні засоби захисту, що входять до складу КЗЗ, разом з організаційними заходами повинні забезпечувати СЗІ інформацією про користувачів, які працюють в системі, з локалізацією точки їхнього входу в систему і переліком технічних засобів і процесів, до яких вони отримали доступ.

Має бути визначено порядок організації та проведення СЗІ процедур періодичного та/або динамічного тестування комплексу засобів захисту інформації під час функціонування КС.

7.8 Характеристика фізичного середовища КС

У загальному випадку КС є територіально розосередженою системою, фізичне розташування компонентів якої можна представити як ієрархію, що включає:

– територію, на якій вона знаходиться;
– будівлю, яка знаходиться на території;
– окреме приміщення в межах будівлі.

КС комплектується необхідними засобами енергозабезпечення, сигналізації, зв'язку, допоміжними технічними засобами, іншими системами життєзабезпечення.

Типові адміністративні та організаційні вимоги щодо умов розміщення компонентів КС наступні.

Усі будівлі повинні бути розміщені в межах контрольованої території, що має пропускний та внутрішній режими, які відповідають режимним вимогам, що визначено чинними в організації нормативними та розпорядчими документами.

Контроль за доступом до приміщень, де знаходяться критичні з точки зору безпеки інформації компоненти КС, повинен забезпечуватись на всіх етапах її життєвого циклу. Порядок доступу до приміщень із визначенням категорій користувачів, які мають право це здійснювати, визначається СЗІ і затверджується керівником організації.

Для приміщень, в яких розташовані категорійовані компоненти КС, повинні бути вжиті відповідні заходи із захисту інформації від витоку технічними каналами, достатність і ефективність яких засвідчується актами атестації комплексів технічного захисту інформації для кожного такого приміщення.

7.9 Характеристика користувачів КС

За рівнем повноважень щодо доступу до інформації, характером та складом робіт, які виконуються в процесі функціонування комп'ютерних систем, особи, що мають доступ до КС, поділяються на наступні категорії:

- користувачі, яким надано повноваження розробляти й супроводжувати КСЗІ (адміністратор безпеки, співробітники ПЗІ);
- користувачі, яким надано повноваження забезпечувати управління КС (адміністратори операційних систем, СКБД, мережевого обладнання, сервісів та ін.);
- користувачі, яким надано право доступу до ІзОД одного або декількох класифікаційних рівнів;
- користувачі, яким надано право доступу тільки до відкритої інформації;
- технічний обслуговуючий персонал, що забезпечує належні умови функціонування КС;
- розробники та проектувальники апаратних засобів КС, що забезпечують її модернізацію та розвиток;
- розробники програмного забезпечення, які здійснюють розробку та впровадження нових функціональних процесів, а також супроводження вже діючих;

- постачальники обладнання і технічних засобів КС та фахівці, що здійснюють його монтаж, поточне гарантійне й післягарантійне обслуговування;
- технічний персонал, що здійснює повсякденне підтримання життєдіяльності фізичного середовища КС (електрики, технічний персонал з обслуговування будівель, ліній зв'язку тощо).

Усі користувачі та персонал КС повинні пройти підготовку щодо умов та правил використання технічних та програмних засобів, які застосовуються ними під час виконання своїх службових та функціональних обов'язків.

Доступ осіб всіх категорій до ІзОД та її носіїв здійснюється на підставі дозволу, що надається наказом (розпорядженням) керівника організації. Дозвіл надається лише для виконання ними службових та функціональних обов'язків і на термін не більший, ніж той, що цими обов'язками передбачений.

Якщо в КС встановлено декілька класифікаційних рівнів ІзОД, кожній особі з допущених до роботи в КС мають бути визначені її повноваження щодо доступу до інформації певного класифікаційного рівня.

Дозвіл на доступ до ІзОД, що обробляється в КС, може надаватися лише користувачам. Як виключення, в окремих випадках (наприклад, аварії або інші непередбачені ситуації) дозвіл може надаватися іншим категоріям осіб на час ліквідації негативних наслідків і поновлення працездатності КС.

Персонал КС, розробники програмного забезпечення, розробники та проектувальники апаратних засобів, постачальники обладнання та фахівці, що здійснюють монтаж і обслуговування технічних засобів КС, і не мають дозволу на доступ до ІзОД, можуть мати доступ до програмних та апаратних засобів КС лише під час робіт із тестування й інсталяції програмного забезпечення, встановлення і регламентного обслуговування обладнання тощо, за умови обмеження їх доступу до даних конфіденційного характеру.

Зазначені категорії осіб повинні мати дозвіл на доступ тільки до конфіденційних відомостей, які містяться в програмній і технічній документації на КС або на окремі її компоненти, і необхідні їм для виконання функціональних обов'язків.

Порядок та механізми доступу до ІзОД та компонентів КС особами різних категорій розробляються ПЗІ та затверджуються керівником організації.

Для організації управління доступом до ІзОД та компонентів КС необхідно:

– розробити та впровадити посадові інструкції користувачів та персоналу КС, а також інструкції, якими регламентується порядок виконання робіт іншими особами з числа тих, що мають доступ до КС;

– розробити та впровадити розпорядчі документи щодо правил перепусткового режиму на територію, в будівлі та приміщення, де розташована КС або її компоненти;

– визначити правила адміністрування окремих компонентів КС та процесів, використання ресурсів КС, а також забезпечити їх розмежування між різними категоріями адміністраторів;

– визначити правила обліку, зберігання, розмноження, знищення носіїв ІзОД;

– розробити та впровадити правила ідентифікації користувачів та осіб інших категорій, що мають доступ до КС.

7.10 Характеристика оброблюваної в КС інформації

В КС обробляється ІзОД, володіти, користуватися чи розпоряджатися якою можуть окремі фізичні та/або юридичні особи, що мають доступ до неї у відповідності до правил, встановлених власником цієї інформації.

В КС може зберігатися і циркулювати відкрита інформація, яка не потребує захисту, або захист якої забезпечувати недоцільно, а також відкрита інформація, яка у відповідності до рішень її власника може потребувати захисту.

Конфіденційна й відкрита інформація можуть циркулювати та оброблятися в КС як різними процесами для кожної з категорій інформації, так і в межах одного процесу.

У загальному випадку в КС, безвідносно до ступеню обмеження доступу, інформація за рівнем інтеграції характеризується як:

– сукупність сильнозв’язаних об’єктів, що вимагають забезпечення своєї цілісності як сукупність;

– окремі слабозв’язані об’єкти, що мають широкий спектр способів свого подання, зберігання й передачі і вимагають забезпечення своєї цілісності кожний окремо.

Незалежно від способу подання об’єкти можуть бути структурованими або неструктурованими.

КСЗІ повинна реалізувати механізми, що забезпечують фізичну цілісність слабозв’язаних об’єктів, окремих складових сильнозв’язаних об’єктів, та підтримку логічної цілісності сильнозв’язаних об’єктів, що розосереджені в різних компонентах КС.

В КС присутня інформація, яка за часом існування та функціонування:

– є швидкозмінюваною з відносно коротким терміном її актуальності;

– має відносно тривалий час існування при високому ступені інтеграції і гарантуванні стану її незруйнованості за умови приналежності різним користувачам, в рамках сильно- або слабозв’язаних об’єктів.

КСЗІ повинна забезпечити доступність зазначених видів інформації у відповідності до особливостей процесів, що реалізують інформаційну модель конкретного фізичного об’єкта.

КС повинна забезпечувати підтримку окремих класів сукупностей сильнозв’язаних об’єктів стандартними для галузі системами керування базами даних, іншими функціональними чи системними процесами, які надають можливість здійснення паралельної обробки запитів і мають засоби, що в тій чи іншій мірі гарантують конфіденційність і цілісність інформації на рівні таблиць, стовпців таблиці, записів таблиці.

КС повинна забезпечувати підтримку окремих класів сукупностей слабозв’язаних об’єктів стандартними для галузі операційними системами, які мають засоби, що в тій чи іншій мірі гарантують конфіденційність і цілісність інформації на рівні сукупності файлів, окремих файлів.

КСЗІ повинна гарантувати забезпечення цілісності, конфіденційності й доступності інформації, яка міститься в сильно- або слабозв’язаних об’єктах і має ступінь обмеження ДСК, згідно з визначеними у цьому документі вимогами до відповідного функціонального профілю захищеності.

7.11 Характеристика технологій оброблення інформації в КС підприємства

Технологічні особливості функціонування КС підприємства визначаються особливістю архітектури КС, способами застосування засобів обчислювальної техніки для виконання функцій збору, зберігання, оброблення, передавання та використання даних, вимогами до забезпечення властивостей інформації.

КС за структурою технічних та програмних засобів, що використовуються, може бути однорідною або гетерогенною структурою, мати різну топологію, що, відповідно, визначає різні підходи до забезпечення режимів циркулювання інформації в КС та способів доступу до неї.

КСЗІ повинна гарантувати користувачам стійкість комп’ютерної системи до відмов та можливість проведення заміни окремих її компонентів з одночасним збереженням доступності до окремих компонентів КС або до КС в цілому.

В КС під час зберігання, оброблення та передавання ІзОД має забезпечуватися реєстрація дій користувачів способом, що дозволяє однозначно ідентифікувати користувача, адресу робочого місця, з якого здійснено доступ до об’єктів та час, протягом якого здійснювався доступ.

Засоби КЗЗ повинні забезпечити необхідний рівень цілісності та конфіденційності інформації в журналах реєстрації КС із можливим виділенням одного чи декількох серверів аудиту. Статистика роботи користувачів повинна бути спостереженою й доступною для адміністратора безпеки та/або співробітників СЗІ.

Журнали реєстрації системи повинні мати захист від несанкціонованого доступу, модифікації або руйнування.

У загальному випадку кожен користувач КС, що має дозвіл на роботу з конфіденційною інформацією, повинен мати можливість доступу до неї з будь-якої робочої станції комп'ютерної системи.

У разі необхідності можуть вводитися обмеження щодо цього. За певних адміністративно-організаційних заходів та відповідних програмно-технічних рішень в КС, де одночасно циркулює інформація різних ступенів доступу, для роботи з інформацією, що має ступінь обмеження ДСК, можуть бути виділені окремі робочі станції. Робота інших робочих станцій, що не віднесені до переліку зазначених вище, повинна блокуватися за умови намагання користувачем будь-якої з категорій отримати доступ до ІзОД.

КСЗІ повинна забезпечити ідентифікацію користувача з визначенням точки його входу в КС, однозначно автентифікувати його і зареєструвати результат (успішний чи невдалий) цих подій у системному журналі. У випадку виявлення неавторизованого користувача повинна блокуватися можливість його роботи в КС.

КСЗІ повинна забезпечувати можливість двох режимів роботи користувача – із конфіденційною інформацією та з відкритою інформацією, гарантуючи в першому випадку доступ до відповідних об'єктів і процесів як з обмеженим доступом, так і до загальнодоступних, а в останньому – тільки до відкритої інформації й блокування будь-якого доступу до об'єктів і процесів з обмеженим доступу.

В обох режимах повинна забезпечуватися можливість визначення власниками об'єктів конкретних користувачів або їх групи, яким надається право мати доступ до цих об'єктів.

ІзОД може зберігатися як на окремих виділених для цього (однорівневих) пристроях – серверах, робочих станціях, запам'ятовуючих пристроях та ін., так і на пристроях, що одночасно зберігають інформацію загального призначення (багаторівневих).

КСЗІ повинна забезпечити розмежування доступу користувачів різних категорій до інформації незалежно від способу її групування на однорівневих чи багаторівневих пристроях.

В КС повинна надаватись можливість формування робочих груп з використанням засобів адміністрування:

– за ознакою належності до того чи іншого компонента комп'ютерної системи;

– відповідно до функцій, що необхідно виконувати конкретному користувачеві або групі користувачів.

Крайній випадок – вся КС призначена для забезпечення виконання усіх функцій усіма користувачами або групами користувачів.

Під час цього засоби адміністрування комп'ютерної системи повинні забезпечувати контроль за можливостями встановлення, перегляду, модифікації стратегій управління (наприклад, реалізація управління

віртуальними мережами), а засоби КЗЗ – гарантувати забезпечення контролю за цілісністю засобів адміністрування КС.

Копіювання об’єктів, що містять конфіденційну інформацію, із сервера на робочу станцію користувача дозволяється тільки у випадках, коли це передбачено технологічними процесами обробки інформації. КЗЗ повинен гарантувати, що зазначені процеси перед завершенням своєї роботи забезпечують копіювання цих об’єктів на сервер (якщо в цьому є потреба) і знищують їх на робочій станції способом, що унеможливлює відновлення або відтворення.

Під час обробки ІзОД повинна забезпечуватися можливість відміни окремої операції або певної їх послідовності до стану, що визначено користувачем або передбачено технологією реалізації певних процедур функціональним або системним програмним забезпеченням.

Виведення інформації у текстовому вигляді повинно здійснюватися на зареєстровані в установленому порядку паперові носії на спеціально виділених для цього пристроях друку. КСЗІ повинна забезпечити контроль за процесом виконання друку інформації з фіксацією в системному журналі: імені користувача, об’єкта, робочої станції та часу, коли здійснюється друк. У разі необхідності можлива фіксація додаткової інформації, що характеризує процес друку і дозволяє його однозначно ідентифікувати.

Реалізація функцій копіювання інформації в електронному вигляді на зйомні носії інформації та створення резервних копій може здійснюватися тільки уповноваженими користувачами або за дозволом адміністратора безпеки.

КСЗІ повинна контролювати зазначені процеси шляхом реєстрації в журналі системи: імені користувача, об’єкта копіювання, робочої станції та часу, коли здійснюється процес копіювання або створення резервної копії. Допускається фіксація додаткової інформації, що характеризує ці процеси і дозволяє їх однозначно ідентифікувати.

Повинна бути реалізована можливість виявлення фактів несанкціонованого доступу до об’єктів та (або) процесів, що потенційно можуть призвести до виникнення загроз для інформації, і забезпечена фіксація в журналі системи: імені користувача, об’єкта та (або) процесу, до якого була спроба доступу, місця та часу, коли виникла загроза. Допускається фіксація додаткової інформації, яка дозволяє однозначно ідентифікувати процеси, що створили загрозу. КСЗІ повинна забезпечити блокування роботи робочих станцій, з яких була здійснена загроза інформації.

З урахуванням характеристик і особливостей подання оброблюваної інформації, особливостей процесів, що застосовуються для її оброблення, а також порядку роботи користувачів та вимог до забезпечення захисту інформації в КС підприємства визначаються такі технології обробки інформації:

– обробка без активного діалогу зі сторони користувача слабозв’язаних об’єктів, що вимагають конфіденційності оброблюваної інформації, або конфіденційності й цілісності оброблюваної інформації;

– обробка без активного діалогу зі сторони користувача сильнозв’язаних об’єктів, що вимагають конфіденційності та цілісності оброблюваної інформації;

– обробка в активному діалоговому режимі зі сторони користувача слабозв’язаних об’єктів, що вимагають конфіденційності та доступності оброблюваної інформації, або конфіденційності та цілісності оброблюваної інформації;

– обробка в активному діалоговому режимі зі сторони користувача сильнозв’язаних об’єктів, що вимагають конфіденційності, цілісності та доступності оброблюваної інформації.

Визначені вище технології обробки інформації можуть бути застосовані як до КС в цілому, так і до окремих її компонентів або процесів, що використовуються в КС. Одночасно в КС можуть застосовуватись декілька технологій.

Обробка без активного діалогу зі сторони користувача слабозв’язаних об’єктів у загальному випадку представляє собою обробку окремого набору даних (або певної їх множини, але послідовно одне за одним) у фоновому режимі, який забезпечується операційними системами (за виключенням однокористувацьких однозадачних), що використовуються на робочих станціях та серверах комп’ютерної системи.

Обробка без активного діалогу зі сторони користувача сильнозв’язаних об’єктів являє собою вирішення в фоновому режимі комплексів функціональних задач, які взаємодіють із базами даних, що підтримуються стандартними для галузі СКБД, а також реалізацію будь-яких інших процесів, які здійснюють одночасну обробку певної множини наборів даних, що мають між собою логічні зв’язки.

Обробка в активному діалоговому режимі зі сторони користувача слабозв’язаних об’єктів являє собою обробку окремого набору даних у режимі реального часу в діалозі між користувачем та прикладним процесом, що цю обробку здійснює (наприклад, створення та редагування текстів, і тому подібне).

Обробка в активному діалоговому режимі зі сторони користувача сильнозв’язаних об’єктів являє собою процеси реалізації в режимі реального часу взаємодії між користувачем та базою даних або сильнозв’язаними об’єктами (наприклад, будь-які інформаційні системи, що побудовані з використанням баз даних та СКБД і працюють у реальному часі; будь-які системи комп’ютерного проектування тощо).

7.12 Модель порушника

Як порушник розглядається особа, яка може одержати доступ до роботи з включеними до складу КС засобами.

Порушники класифікуються за рівнем можливостей, що надаються їм штатними засобами КС.

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 КС — 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 КС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;

• четвертий рівень визначається всім обсягом можливостей осіб, що здійснюють проектування, реалізацію і ремонт апаратних компонентів КС, аж до включення до складу КС власних засобів з новими функціями обробки інформації.

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

Така класифікація порушників є корисною для використання в процесі оцінки ризиків, аналізу вразливості системи, ефективності існуючих і планових заходів захисту.

7.13 Політика реалізації послуг безпеки інформації в КС підприємства

Політика безпеки інформації в КС повинна поширюватися на об’єкти комп’ютерної системи, які безпосередньо чи опосередковано впливають на безпеку ІзОД.

До таких об’єктів належать:

– адміністратор безпеки та співробітники СЗІ;

– користувачі, яким надано повноваження інших адміністраторів;

– користувачі, яким надано право доступу до ІзОД або до інших видів інформації;

– слабо- та сильнозв’язані об’єкти, які містять конфіденційну інформацію або інші види інформації, що підлягають захисту;

– системне та функціональне програмне забезпечення, яке використовується в КС для оброблення інформації або для забезпечення КЗЗ;

– технологічна інформація КСЗІ (дані щодо персональних ідентифікаторів та паролів користувачів, їхніх повноважень та прав доступу до об’єктів, встановлених робочих параметрів окремих механізмів або засобів захисту, інша інформація баз даних захисту, інформація журналів реєстрації дій користувачів тощо);

– засоби адміністрування та управління обчислювальною системою КС та технологічна інформація, яка при цьому використовується;

– окремі периферійні пристрої, які задіяні у технологічному процесі обробки ІзОД;

– обчислювальні ресурси КС (наприклад, дисковий простір, тривалість сеансу користувача із засобами КС, час використання центрального процесора і т. ін.), безконтрольне використання яких або захоплення окремим користувачем може призвести до блокування роботи інших користувачів, компонентів КС або КС в цілому.

7.14 Комплекс засобів захисту і об'єкти комп’ютерної системи

Комплекс засобів захисту (КЗЗ) – це сукупність всіх програмно-апаратних засобів, в тому числі програм ПЗП, задіяних під час реалізації політики безпеки. Частина КС, що складає КЗЗ, визначається розробником.

Будь-який компонент КС, який внаслідок якого-небудь впливу здатний спричинити порушення політики безпеки, повинен розглядатись як частина КЗЗ.

Комплекс засобів захисту розглядає ресурси КС як об'єкти і керує взаємодією цих об'єктів відповідно до політики безпеки інформації, що реалізується.

Як об'єкти ресурси характеризуються двома аспектами: логічне подання (зміст, семантика, значення) і фізичне (форма, синтаксис).

Об'єкт характеризується своїм станом, що в свою чергу характеризується атрибутами і поводженням, яке визначає способи зміни стану.

Для різних КС об'єкти можуть бути різні. Наприклад, для СУБД в якості об'єктів можна розглядати записи БД, а для операційної системи — процеси, файли, кластери, сектори дисків, сегменти пам'яті і т. ін. Все, що підлягає захисту відповідно до політики безпеки, має бути визначено як об'єкт.

При розгляді взаємодії двох об'єктів КС, що виступають як приймальники або джерела інформації, слід виділити пасивний об'єкт, над яким виконується операція, і активний об'єкт, який виконує або ініціює цю операцію.

Далі розглядаються такі типи об'єктів КС:

• об'єкти-користувачі;

• об'єкти-процеси і пасивні об'єкти.

Прийнятий у деяких зарубіжних документах термін "суб'єкт" є суперпозицією об'єкта-користувача і об'єкта-процеса.

Об'єкти-користувачі і об'єкти-процеси є такими тільки всередині конкретного домену – ізольованої логічної області, всередині якої об'єкти володіють певними властивостями, повноваженнями і зберігають певні відносини.

7.15 Планування захисту і керування системою захисту

Для забезпечення безпеки інформації під час її обробки в КС підприємства створюється комплексна система захисту інформації (КСЗІ), процес управління якою повинен підтримуватись протягом всього життєвого циклу КС.

На стадії розробки метою процесу управління КСЗІ є створення засобів захисту, які могли б ефективно протистояти ймовірним загрозам і забезпечували б надалі дотримання політики безпеки під час обробки інформації.

На стадії експлуатації КС метою процесу управління КСЗІ є оцінка ефективності створеної КСЗІ і вироблення додаткових (уточнюючих) вимог для доробки КСЗІ з метою забезпечення її адекватності при зміні початкових умов (характеристик ОС, оброблюваної інформації, фізичного середовища, персоналу, призначення КС, політики безпеки і т. ін.).

На кожному етапі мають бути виконані збирання і підготовка даних, їх аналіз і прийняття рішення. При цьому результати виконаного на певному етапі аналізу і прийняті на їх підставі рішення нарівні з уточненими вимогами слугують вихідними даними для аналізу на наступному етапі.

На будь-якій стадії або будь-якому етапі може постати необхідність уточнення початкових умов і повернення на попередні етапи.

Створення КСЗІ має починатись з аналізу об'єкта захисту і можливих загроз. Передусім мають бути визначені ресурси КС, що підлягають захисту.

Загрози мають бути визначені в термінах ймовірності їх реалізації і величини можливих збитків.

На підставі аналізу загроз, існуючих в системі вразливостей, ефективності вже реалізованих заходів захисту для всіх ресурсів, що підлягають захисту, мають бути оцінені ризики.

Ризик являє собою функцію ймовірності реалізації певної загрози, виду і величини завданих збитків. Величина ризику може бути виражена в грошовому вимірі або у вигляді формальної оцінки (високий, низький і т. ін.).

На підставі виконаної роботи мають бути вироблені заходи захисту, перетворення яких в життя дозволило б знизити рівень остаточного ризику

до прийнятного рівня. Підсумком даного етапу робіт повинна стати сформульована або скоригована політика безпеки.

На підставі проведеного аналізу ризиків сформульованої політики безпеки розробляється план захисту, який включає в себе опис послідовності і змісту всіх стадій і етапів життєвого циклу КСЗІ, що мають відповідати стадіям і етапам життєвого циклу КС. Вартість заходів щодо захисту інформації має бути адекватною розміру можливих збитків.

7.16 Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу

Згідно з Положенням про технічний захист інформації в Україні в КС, де обробляється інформація, яка є власністю держави або захист якої гарантується державою, повинні використовуватись засоби ТЗІ, які мають документ, що засвідчує їх відповідність вимогам нормативних документів з питань технічного захисту інформації (експертний висновок та/або сертифікат відповідності).

Склад засобів ТЗІ, що використовуються під час створення комплексу засобів захисту (КЗЗ) інформації, визначають власники КС, де обробляється інформація, яка підлягає захисту, або уповноважені ними суб'єкти системи ТЗІ, з урахуванням того, що ці засоби повинні мати рівень гарантій коректності реалізації послуг безпеки (НД ТЗІ 2.5-004-99) не нижчий від рівня гарантій створюваного КЗЗ.

Дозволяється в КС класів "1" та "2" (НД ТЗІ 2.5-005-99) використання засобів ТЗІ з рівнем гарантій на один нижче від рівня гарантій створюваного КЗЗ, за умов реалізації в цих КС необхідного обсягу організаційних заходів. Обсяг цих заходів визначається моделями загроз та порушника, умовами експлуатації КС тощо.

Засоби криптографічних перетворень, які є складовою частиною засобів ТЗІ, повинні відповідати вимогам нормативних документів з питань криптографічного захисту інформації.

Створення та впровадження засобів ТЗІ здійснюють підприємства, установи та організації всіх форм власності, за умови наявності у них відповідної ліцензії на право провадження господарської діяльності в галузі ТЗІ.

Виробництво та впровадження апаратних та програмно-апаратних засобів ТЗІ здійснюється за наявності технічних умов (ТУ), які розробляються, оформляються та реєструються відповідно до вимог ДСТУ 1.3-98, ГОСТ 2.114-95.

Створення програмних засобів ТЗІ здійснюється з урахуванням вимог ДСТУ 3918–99, ГОСТ 19.101–77.

Впровадження програмних засобів ТЗІ здійснюється за наявності Формуляру, який розробляється відповідно до вимог ГОСТ 19.501–78.

З метою досягнення певного рівня гарантій реалізації функціональних послуг безпеки інформації розробники (впроваджувальні організації) засобів ТЗІ повинні взаємодіяти з Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України (далі – Департамент).

Експертне оцінювання засобів ТЗІ на відповідність нормативних документів з питань ТЗІ, здійснюється в порядку, визначеному Положенням про державну експертизу в сфері технічного захисту інформації.

Рівень гарантії реалізації функціональних послуг безпеки визначається в процесі експертного оцінювання з урахуванням вимог цього НД ТЗІ.

Для забезпечення можливості досягнення 3–7 рівня гарантій реалізації функціональних послуг безпеки розробник (впроваджувальна організація) повинен здійснювати супроводження засобу ТЗІ. Для цього розробник (впроваджувальна організація) укладає з користувачем договір на супроводження засобу ТЗІ.

Модернізація засобів ТЗІ в комп’ютерних системах здійснюється у відповідності з окремим ТЗ або доповненням до основного ТЗ на створення засобу ТЗІ. ТЗ (доповнення до основного ТЗ) розробляється та оформляється відповідно до чинних ДСТУ з урахуванням вимог НД ТЗІ 3.7–001–99.

7.17 Організація захисту інформації в КС від витоку каналами ПЕМВН

Роботи з технічного захисту інформації (ТЗІ) в ІС і ЗОТ передбачають:

– категоріювання об'єктів електронно-обчислювальної техніки (ЕОТ);

– включення до технічних завдань на монтаж ІС і ЗОТ розділу з ТЗІ;

– монтаж ІС і ЗОТ відповідно до рекомендацій цього документа;

– обстеження (в тому числі технічний контроль) об'єктів ЕОТ;

– установлення (при необхідності) атестованих засобів захисту;

– технічний контроль за ефективністю вжитих заходів.

Для об'єктів ЕОТ, що обробляють ІзОД, проводиться обов'язкове категоріювання згідно з чинним Положенням про категоріювання. Обсяг і зміст робіт із захисту цієї інформації визначаються присвоєною категорією.

Обстеження ІС і ЗОТ відповідно до рекомендацій цього документа проводиться структурними підрозділами ТЗІ, у віданні яких знаходиться об'єкт, або підприємствами, установами, організаціями і громадянами, що одержали в установленому порядку відповідні ліцензії Державної служби України з питань технічного захисту інформації.

Рекомендований алгоритм обстеження містить такі процедури:

– аналіз у технічних засобах (ТЗ) ЕОТ потоків інформації з обмеженим доступом;

– визначення складу ОТЗ і ДТЗ на ОІД;

– визначення складу кабельних ліній, що виходять за межі КТ і мають паралельний пробіг з кабелями ІС і ЗОТ;

– виявлення комунікацій, що проходять через територію ОІД і мають вихід за межі КЗ;

– інструментальне вимірювання інформативних побічних електромагнітних випромінювань та наводок;

– оцінку відповідності рівнів сигналів і параметрів полів, які є носіями ІзОД, нормам ефективності захисту.

За результатами обстеження складається акт, в якому відбиваються:

– категорія ОІД;

– перелік ОТЗ (найменування, тип, заводський номер);

– перелік ДТЗ і комунікацій, що знаходяться на ОІД;

– оцінка відповідності монтажу цим рекомендаціям;

– пропозиції щодо застосування додаткових заходів захисту (при необхідності).

До акта додаються:

– схема розміщення технічних засобів ОІД і проходження комунікацій на ньому;

– протоколи вимірювань.

7.18 Рекомендації із захисту інформації від перехоплення випромінювань технічних засобів ОІД

Навколо ОТЗ повинна забезпечуватися контрольована територія, за межами якої відношення "інформативний сигнал/шум" не перевищує Норм. З цією метою ОТЗ рекомендується розташовувати у внутрішніх приміщеннях об'єкта, бажано, на нижніх поверхах.

У випадку неможливості забезпечення цієї умови необхідно:

– замінити ОТЗ на захищені;

– провести часткове або повне екранування приміщень чи ОТЗ;

– установити системи просторового зашумлення;

– замінити незахищені ТЗ на захищені;

– застосувати завадозаглушувальні фільтри.

В екранованих приміщеннях (капсулах) рекомендується розміщувати високочастотні (ВЧ) ОТЗ. Як правило, до них відносяться процесори, запам'ятовувальні пристрої, дисплеї тощо.

7.19 Рекомендації із захисту інформації від перехоплення наводок на незахищені технічні засоби та ДТЗ, що мають вихід за межі КТ

У незахищених каналах зв'язку, лініях, проводах та кабелях ОТЗ і ДТЗ, що мають вихід за межі КТ, установлюються завадозаглушувальні фільтри.

Проводи і кабелі прокладаються в екранованих конструкціях.

Монтаж кіл ТЗ, що мають вихід за межі КТ, рекомендується проводити екранованим або прокладеним в екранувальних конструкціях симетричним кабелем.

Кабелі ОТЗ прокладаються окремим пакетом і не повинні утворювати петлі. Перехрещення кабелів ОТЗ і ДТЗ, що мають вихід за межі КТ, рекомендується проводити під прямим кутом, забезпечуючи відсутність електричного контакту екранувальних оболонок кабелів у місці їх перехрещення.

Незадіяні проводи і кабелі демонтуються або закорочуються та заземляються.

7.20 Рекомендації із захисту інформації від витоку колами заземлення

Система заземлення технічних засобів ОІД не повинна мати вихід за межі КТ і повинна розміщуватися на відстані не менше 10 – 15 м від них.

Заземлювальні проводи повинні бути виконані з мідного дроту (кабеля) з перехідним опором з'єднань не більше 600 мкОм. Опір заземлення не повинен перевищувати 4 Ом.

Не рекомендується використовувати для системи заземлення ТЗ ОІД природні заземлювачі (металеві трубопроводи, залізобетонні конструкції будинків тощо), які мають вихід за межі КТ.

Для усунення небезпеки витоку інформації металевими трубопроводами, що виходять за межі КТ, рекомендується використовувати струмонепровідні вставки (муфти) довжиною не менше 1 м.

За наявності в ТЗ ОІД "схемної землі" окреме заземлення для них створювати не потрібно. Шина "схемна земля" повинна бути ізольованою від захисного заземлення та металоконструкцій і не повинна утворювати замкнену петлю.

При неможливості провести заземлення ТЗ ОІД допускається їх "занулення".

7.21 Рекомендації із захисту інформації від витоку колами електроживлення

Найбільш ефективно гальванічну та електромагнітну розв'язку кабелів електроживлення ТЗ ОІД від промислової мережі забезпечує їх розділова система типу "електродвигун-генератор". Електроживлення допускається також здійснювати через завадозаглушувальні фільтри.

Електроживлення повинно здійснюватись екранованим (броньованим) кабелем.

Кола електроживлення ТЗ ОІД на ділянці від ОТЗ до розділових систем чи завадозаглушувальних фільтрів рекомендується прокладати у жорстких екранувальних конструкціях.

Не допускається прокладання в одній екранувальній конструкції кабелів електроживлення, розв`язаних від промислової мережі, з будь-якими кабелями, що мають вихід за межі КТ.

Забороняється здійснювати електроживлення технічних засобів, що мають вихід за межі КТ, від захищених джерел електропостачання без установлення завадозаглушувальних фільтрів.

Для об'єктів 2 – 4 категорій допускається не проводити роботи із захисту кіл електроживлення, якщо всі пристрої і кабелі електропостачання ОІД, включаючи трансформаторну підстанцію низької напруги із заземлювальним пристроєм, розміщені у межах КТ.

7.22 Рекомендації із застосування системи просторового зашумлення ОІД

Пристрої просторового зашумлення застосовуються у випадках, коли пасивні заходи не забезпечують необхідної ефективності захисту ОІД.

Установленню підлягають тільки сертифіковані Державною службою України з питань технічного захисту інформації (ДСТЗІ) засоби просторового зашумлення, до складу яких входять:

– надширокосмугові генератори електромагнітного поля шуму (гене–ратор шуму);

– система рамкових антен;

– пульт сигналізації справності роботи системи.

Установлення генераторів шуму, монтаж антен, а також їх обслуговування в процесі експлуатації здійснюють підприємства, установи й організації, що мають відповідну ліцензію ДСТЗІ.

Живлення генераторів шуму повинно здійснюватися від того ж джерела, що і живлення ТЗ ОІД. Антени рекомендується розташовувати поза екранованим приміщенням.

7.23 Основні рекомендації з обладнання та застосування екранувальних конструкцій

Екранувальні кабельні конструкції разом з екранувальними конструкціями ТЗ ОІД повинні створювати екранувальний замкнений об'єм.

Виведення кабелів з екранувальних конструкцій і введення в них необхідно здійснювати через завадозаглушувальні фільтри.

Екранувальні кабельні конструкції можуть бути жорсткими і гнучкими. Основу жорстких конструкцій становлять труби, короби та коробки; основу гнучких конструкцій – металорукави, взяті в обплетення, і сітчасті рукави.

Для екранування проводів і кабелів застосовуються водогазопровідні труби. Рекомендується застосовувати сталеві тонкостінні оцинковані труби або сталеві електрозварені.

З'єднання нероз'ємних труб здійснюється зварюванням, роз'ємних – за допомогою муфти та контргайки.

Для екранування проводів і кабелів застосовуються короби прямокутного перерізу. Їх переваги у порівнянні з трубами – можливість прокладання кабеля з роздільними роз'ємами.

Короби виготовляються з листової сталі. На кінцях секцій короба повинні бути фланці для з'єднання коробів між собою та з іншими екранувальними конструкціями. Для одержання надійного електричного контакту поверхня фланців повинна мати антикорозійне струмопровідне покриття.

Остаточний висновок про ефективність заходів щодо тех–нічного захисту інформації дається за результатами інструментального контролю

РОЗДІЛ 8 ЗАХИСТ ІзОД В КС ПІДПРИЄМСТВА

Засади щодо захисту ІзОД визначаються Законами України “Про інформацію” і “Про захист інформації в комп’ютерних системах”, іншими нормативно-правовими актами, виданими у відповідності з цими законами, а також “Інструкцією про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять ІзОД”.

Обробка в комп’ютерній системі ІзОД здійснюється з використанням захищеної технології.

Технологія обробки інформації є захищеною, якщо вона містить програмно-технічні засоби захисту та організаційні заходи, що забезпечують виконання загальних вимог із захисту інформації. Загальні вимоги передбачають:

– наявність переліку ІзОД, яка підлягає комп’ютерній обробці; у разі необхідності можлива її класифікація в межах категорії за цільовим призначенням, ступенем обмеження доступу окремих категорій користувачів та іншими класифікаційними ознаками;

– наявність визначеного (створеного) відповідального підрозділу, якому надані повноваження щодо організації і впровадження технології захисту інформації, контролю за станом захищеності інформації;

– створення комплексної системи захисту інформації (далі – КСЗІ), яка являє собою сукупність організаційних і інженерно-технічних заходів, програмно-апаратних засобів, спрямованих на забезпечення захисту інформації під час функціонування КС;

– розроблення плану захисту інформації в КС, зміст якого визначено в додатку до НД ТЗІ 1.4-001;

– наявність атестата відповідності КСЗІ в КС нормативним документам із захисту інформації;

– можливість визначення засобами КСЗІ декількох ієрархічних рівнів повноважень користувачів та декількох класифікаційних рівнів інформації;

– обов’язковість реєстрації в КС усіх користувачів та їхніх дій щодо ІзОД;

– можливість надання користувачам тільки за умови службової необхідності санкціонованого та контрольованого доступу до ІзОД, що обробляється в КС;

– заборону несанкціонованої та неконтрольованої модифікації ІзОД в КС;

– здійснення СЗІ обліку вихідних даних, отриманих під час вирішення функціональних задач у формі віддрукованих документів, що містять конфіденційну інформацію, у відповідності з “Інструкцією про порядок обліку, зберігання й використання документів, справ, видань та інших матеріальних носіїв інформації, які містять ІзОД”;

– заборону несанкціонованого копіювання, розмноження, розповсюдження ІзОД в електронному вигляді;

– забезпечення СЗІ контролю за санкціонованим копіюванням, розмноженням, розповсюдженням ІзОД в електронному вигляді;

– можливість здійснення однозначної ідентифікації та автентифікації кожного зареєстрованого користувача;

– забезпечення КСЗІ можливості своєчасного доступу зареєстрованих користувачів КС до ІзОД.

РОЗДІЛ 9 ЗАХИСТ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ В ІНФОРМАЦІЙНО–ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Захист державних інформаційних ресурсів в комп'ютерних системах, що входять до складу інформаційно-телекомунікаційних систем (ІТС) повинен забезпечуватися впровадженням комплексу технічних, криптографічних, організаційних та інших заходів і засобів комплексної системи захисту інформації (далі – КСЗІ), спрямованих на недопущення блокування інформації, несанкціонованого ознайомлення з нею та/або її модифікації.

Порядок створення та вимоги щодо КСЗІ в комп'ютерних системах під час їх створення, експлуатації та модернізації визначаються Законом України "Про захист інформації в комп'ютерних системах", Положенням про технічний захист інформації в Україні, затвердженим Указом Президента України від 27 вересня 1999 р. №1229, Положенням про порядок здійснення криптографічного захисту інформації в Україні, затвердженим Указом Президента України від 22 травня 1998 р. №505/98, нормативно-правовими актами та нормативними документами систем технічного та криптографічного захисту інформації.

В КС повинен забезпечуватися захист від несанкціонованого доступу до державних інформаційних ресурсів з боку мереж передачі даних, зокрема глобальних мереж.

Конфіденційність інформації, яка є державними інформаційними ресурсами, під час передавання мережею передачі даних забезпечує власник КС з використанням засобів та заходів з криптографічного захисту інформації або оператор ІТС за договором з власником КС.

Оброблення державних інформаційних ресурсів в комп'ютерній системі, у тому числі їх передавання з використанням ІТС, дозволяється тільки після отримання атестата відповідності КСЗІ вимогам із захисту інформації, який надається в установленому порядку Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України згідно з Положенням про державну експертизу в сфері технічного захисту інформації, затвердженим наказом ДСТСЗІ СБ України від 29 грудня 1999 р. N 62 і зареєстрованим в Міністерстві юстиції України 24 січня 2000 р. за N 40/4261.

Дозвіл на оброблення державних інформаційних ресурсів дається наказом керівника установи (підприємства, організації), яка є власником КС.

9.1 Забезпечення захисту державних інформаційних ресурсів в мережах передачі даних

Захист державних інформаційних ресурсів у ІТС повинен забезпечуватися впровадженням на кожному з її вузлів комутації комплексу технічних, криптографічних, організаційних та інших заходів і засобів захисту інформації, спрямованих на недопущення її блокування та/або модифікації.

Засоби захисту інформації, які використовуються в ІТС для забезпечення безпеки державних інформаційних ресурсів, повинні мати сертифікат відповідності або експертний висновок, отримані в установленому порядку.

Сертифікат відповідності надається згідно з Порядком проведення робіт із сертифікації засобів забезпечення технічного захисту інформації загального призначення, затвердженим наказом Держстандарту України та ДСТСЗІ СБ України від 9 липня 2001 р. N 329/32 і зареєстрованим у Міністерстві юстиції України 26 липня 2001 р. за N 640/5831, а експертний висновок – згідно з Положенням про державну експертизу в сфері технічного захисту інформації, затвердженим наказом ДСТСЗІ СБ України від 29 грудня 1999 р. N 62 і зареєстрованим у Міністерстві юстиції України 24 січня 2000 р. за N 40/4261.

У разі відсутності на час створення КСЗІ таких документів сертифікація або державна експертиза зазначених засобів на відповідність вимогам із захисту інформації здійснюється під час проведення державної експертизи КСЗІ.

Передавання державних інформаційних ресурсів дозволяється тільки через вузли комутації, що мають атестат відповідності КСЗІ вимогам із захисту інформації, який надається в такому порядку, як і на КСЗІ в КС.

Особи, винні в порушенні порядку захисту державних інформаційних ресурсів у ІТС, несуть відповідальність згідно з чинним законодавством України.

9.2 Контроль за забезпеченням захисту державних інформаційних ресурсів в ІТС

Контроль за забезпеченням захисту державних інформаційних ресурсів в ІТС здійснюється Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України і полягає у перевірці виконання власниками КС та операторами ІТС вимог нормативно-правових актів і нормативних документів з технічного та криптографічного захисту інформації.

У разі виявлення в ІТС порушень вимог із захисту державних інформаційних ресурсів ДСТСЗІ СБ України порушує у встановленому

порядку питання про припинення функціонування КС або використання ІТС.

Власники КС та оператори ІТС повинні створювати необхідні умови для здійснення державного контролю за забезпеченням захисту державних інформаційних ресурсів.

Власники КС та оператори ІТС повинні повідомляти ДСТСЗІ СБ України про виявлені ними спроби та факти здійснення несанкціонованих дій щодо державних інформаційних ресурсів.

Оператори ІТС повинні надавати власнику КС відомості про виявлені ними спроби та факти здійснення несанкціонованих дій в мережах передачі даних щодо інформації, яка йому належить.

Порядок організації та здійснення контролю за забезпеченням захисту державних інформаційних ресурсів в ІТС визначається відповідними нормативно-правовими актами.

РОЗДІЛ 10 ЗАХИСТ ІНФОРМАЦІЇ WEB-СТОРІНКИ ПІДПРИЄМСТВА ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Підприємство, під час створення WEB-сторінки та визначення операторів, вузли яких будуть використовуватися для підключення до мережі Інтернет, повинен керуватися законами України, іншими нормативно-правовими актами, що встановлюють вимоги з технічного захисту інформації.

WEB-сторінка підприємства установи може бути розміщена на власному сервері або на сервері, що є власністю оператора. Власник сервера зобов'язаний гарантувати власнику інформації рівень захисту у відповідності до вимог цього НД ТЗІ.

Функціонування WEB-сторінки забезпечується КС Підприємство, за допомогою якої здійснюється актуалізація розміщених на WEB-сторінці інформаційних ресурсів та керування доступом до них.

Для забезпечення захисту інформації WEB-сторінки в цій КС створюється КСЗІ, що є сукупністю організаційних і інженерно-технічних заходів, а також програмно-апаратних засобів, які забезпечують захист інформації.

Створення КСЗІ здійснюється відповідно до технічного завдання, розробленого згідно з НД ТЗІ 3.7–001.

КСЗІ підлягає державній експертизі у порядку, передбаченому Положенням про державну експертизу в сфері технічного захисту інформації.

Захист інформації на всіх етапах створення та експлуатації WEB-сторінки здійснюється відповідно до розробленого установою плану захисту інформації, зміст якого визначено НД ТЗІ 1.4–001. План захисту затверджується керівником установи, а у випадку використання сервера оператора – погоджується з власником сервера.

Перелік інформації, призначеної для публічного розміщення на WEB-сторінці, визначається з урахуванням вимог діючого законодавства та затверджується керівником установи, що є власником WEB-сторінки.

Організація робіт із захисту інформації та забезпечення контролю за станом її захищеності на WEB-сторінці Підприємство здійснюється відповідальним підрозділом або відповідальною особою.

У випадку користування послугами оператора щодо розміщення, експлуатації та адміністрування WEB-сторінки власник інформації укладає з оператором договір (угоду), яким визначаються права і обов'язки сторін, умови підключення, розміщення інформації та забезпечення доступу до неї, інші питання, що вимагають урегулювання між власником інформації WEB-сторінки та оператором, виходячи з вимог законодавства у сфері захисту інформації та цього НД ТЗІ.

Окремі питання із захисту інформації можуть оформлятися у вигляді додатків, які є невід'ємною частиною договору.

10.1 Характеристика типових умов функціонування та вимоги до захисту інформації WEB-сторінки підприємство

До складу КС, яка забезпечує функціонування WEB-сторінки, підприємства входять: ОС, фізичне середовище, в якому вона знаходиться і функціонує, середовище користувачів, оброблювана інформація, у тому числі й технологія її оброблення.

Під час забезпечення захисту інформації мають бути враховані всі характеристики зазначених складових частин, які впливають на реалізацію політики безпеки WEB-сторінки.

У випадку, якщо WEB-сторінка підприємства містить посилання на інформаційні ресурси іншої WEB-сторінки, умови функціонування останньої не повинні порушувати встановлену для даної WEB-сторінки політику безпеки.

10.2 Вимоги із захисту WEB-сторінки підприємства.

КСЗІ повинна забезпечувати реалізацію вимог із захисту цілісності та доступності розміщеної на WEB-сторінці загальнодоступної інформації, а також конфіденційності та цілісності технологічної інформації WEB-сторінки.

Технологія оброблення інформації повинна відповідати вимогам політики безпеки інформації, визначеної для КС, що забезпечує функціонування
WEB-сторінки.

Вимоги щодо забезпечення цілісності загальнодоступної інформації WEB-сторінки та конфіденційності й цілісності технологічної інформації вимагають застосування технологій, що забезпечують реалізацію контрольованого і санкціонованого доступу до інформації та заборону неконтрольованої й несанкціонованої її модифікації.

Технологія оброблення інформації повинна бути здатною реалізовувати можливість виявлення спроб несанкціонованого доступу до інформації WEB-сторінки та процесів, які з цією інформацією пов'язані, а також забезпечити реєстрацію в системному журналі визначених політикою відповідної послуги безпеки подій (як НСД, так і авторизованих звернень).

Для користувачів, які порушили встановлені правила розмежування доступу до WEB-сторінки, засоби КСЗІ на період сеансу роботи повинні забезпечити блокування доступу до WEB-сторінки.

Технологічними процесами повинна бути реалізована можливість створення резервних копій інформації WEB-сторінки та процедури їх відновлення з використанням резервних копій.

Технологія оброблення інформації повинна передбачати можливість аналізу використання користувачами і процесами обчислювальних ресурсів КС і забезпечувати керування ресурсами.

10.3 Інформаційно-телекомунікаційна система підприємства

Узагальнена функціонально-логічна структура інформаційно-телекомунікаційної системи підприємства включає:

- підсистему обробки інформації;
- підсистему взаємодії з користувачами КС;
- підсистему обміну даними.

Підсистема обробки інформації забезпечує створення, зберігання, актуалізацію інформації WEB-сторінки і складається із засобів обробки інформації, системного та функціонального ПЗ.

До засобів обробки інформації належать WEB-сервер та необхідна кількість робочих станцій (або терміналів) для забезпечення всіх функцій щодо супроводження WEB-сторінки та захисту інформації.

Підсистема взаємодії з користувачами КС забезпечує за запитами користувачів надання доступу до загальнодоступної інформації WEB-сторінки, яка має вигляд HTLM-документу, з використанням мереж передачі даних та стандартних Інтернет-протоколів.

Підсистема складається, як мінімум, з програмно-апаратного комплексу, який дозволяє здійснювати маршрутизацію запитів користувачів, забезпечувати пошук необхідних користувачу інформаційних ресурсів і доступ до них.

Підсистема обміну даними забезпечує підготовку та безпосередньо імпорт/експорт інформації в/із КС, а також внутрішньосистемний обмін інформацією між WEB-сервером та робочими станціями з реалізацією фаз встановлення, підтримання та завершення з’єднання.

Відповідно до політики безпеки інформації в КС підсистеми комплектуються засобами захисту інформації (можуть використовуватися штатні засоби захисту системного і функціонального ПЗ та/або спеціалізовані засоби), які складають компоненти КЗЗ.

Програмно-апаратні засоби захисту, що входять до складу КЗЗ, повинні мати належним чином оформлені документи (експертні висновки, сертифікати), які засвідчують відповідність цих засобів вимогам нормативних документів системи ТЗІ.

Встановлення на ОС нових (додаткових) компонентів, ПЗ (системного та/або функціонального), сервісів та розміщення будь-яких інших мережевих ресурсів, які не належать до категорії WEB-сторінки установи, не повинно порушувати політику безпеки інформації в КС, що забезпечує функціонування WEB-сторінки.

Вимоги до робочих станцій фізичних і юридичних осіб, які є користувачами загальнодоступної інформації WEB-сторінки, та їхнього ПЗ не висуваються.

10.4 Середовище користувачів інформаційно-телекомунікаційної системи підприємства

За рівнем повноважень щодо доступу до інформації, характером та складом робіт, які виконуються в процесі функціонування КС, користувачі поділяються на такі категорії:

а) користувачі, яким надано право доступу тільки до загальнодоступної інформації WEB-сторінки;

б) користувачі, яким надано повноваження супроводжувати КСЗІ та забезпечувати керування КС (адміністратор безпеки, інші співробітники СЗІ, користувачі з функціональними обов’язками WEB-майстрів, адміністраторів сервісів, адміністраторів мережевого обладнання, адміністраторів ресурсів DNS (Domain Name System), PROXY, FTP (File Transfer Protocol) та ін., якщо передбачається їх взаємодія з WEB-сторінкою, тощо);

в) технічний обслуговуючий персонал, що забезпечує належні умови функціонування КС, повсякденну підтримку життєдіяльності фізичного середовища (електрики, технічний персонал з обслуговування приміщень будівель, ліній зв’язку тощо);

г) розробники ПЗ, які здійснюють розробку та впровадження нових функціональних процесів, а також супроводження вже діючого функціонального ПЗ сервера, розробники та проектанти фізичної структури КС;

д) постачальники обладнання і технічних засобів та фахівці, що здійснюють його монтаж, поточне гарантійне й післягарантійне обслуговування.

Користувачі, що належать до категорії "в" повинні мати належний рівень кваліфікації для виконання своїх службових та функціональних обов’язків у відповідності до визначених в установі технологічних процесів та режимів експлуатації обладнання.

Доступ до інформації WEB-сторінки повинен надаватися користувачам у відповідності до положень політики безпеки інформації, визначеної для КС, що забезпечує функціонування WEB-сторінки.

Для встановлення правил та регламентації доступу цих користувачів до інформації WEB-сторінки розробляються та впроваджуються нормативні та розпорядчі документи, передбачені планом захисту інформації.

Користувачі, що належать до категорій "в" – "д" можуть мати доступ до програмних та апаратних засобів КС лише під час робіт із тестування й інсталяції ПЗ, встановлення і регламентного обслуговування обладнання тощо, за умови обмеження їхнього доступу до технологічної інформації КСЗІ.

Зазначені категорії осіб повинні мати дозвіл на доступ до відомостей, які містяться в програмній і технічній документації на КС або окремі її компоненти, і необхідні їм для виконання функціональних обов'язків.

Користувачі загальнодоступної інформації одержують доступ до WEB-сторінки у відповідності до діючих у мережі Інтернет правил та регламенту.

10.5 Фізичне середовище інформаційно-телекомунікаційної системи підприємства

Фізичне середовище, що призначене для розміщення, експлуатації, адміністрування WEB-сторінки установи, включає:

– приміщення, в яких розташовані сервер і робочі станції з усіма компонентами (ОС, сховища для носіїв інформації та документації, робочі місця обслуговуючого персоналу і т. д.);

– засоби енергопостачання, заземлення, життєзабезпечення та сигналізації приміщення;

– допоміжні технічні засоби та засоби зв'язку.

Приміщення, де розміщуються компоненти ОС, повинні знаходитися на контрольованій території і мати охорону.

Доступ здійснюється у порядку, визначеному СЗІ та затвердженому власником WEB-сторінки, або у відповідності до умов, передбачених договором (угодою) між власником WEB-сторінки та оператором (провайдером).

Вимоги до засобів енергопостачання, заземлення, життєзабезпечення, сигналізації приміщення та допоміжних технічних засобів і засобів зв'язку не висуваються.

10.6 Політика безпеки інформації WEB-сторінки підприємства

Політика безпеки інформації в КС повинна поширюватися на об'єкти комп'ютерної системи, які безпосередньо чи опосередковано впливають на безпеку інформації.

До таких об'єктів належать:

– адміністратор безпеки та співробітники СЗІ;

– користувачі, яким надано повноваження забезпечувати управління КС;

– користувачі, яким надано право доступу до загальнодоступної інформації;

– інформаційні об’єкти, що містять загальнодоступну інформацію;

– системне та функціональне ПЗ, яке використовується в КС для оброблення інформації або для забезпечення функцій КЗЗ;

– технологічна інформація КСЗІ (дані про мережеві адреси, імена, персональні ідентифікатори та паролі користувачів, їхні повноваження та права доступу до об’єктів, встановлені робочі параметри окремих механізмів або засобів захисту, інша інформація баз даних захисту, інформація журналів реєстрації дій користувачів тощо);

– засоби адміністрування і управління обчислювальною системою КС та технологічна інформація, яка при цьому використовується;

– обчислювальні ресурси КС (наприклад, дисковий простір, тривалість сеансу роботи користувача із засобами КС, час використання центрального процесора і т. ін.), безконтрольне використання або захоплення яких окремим користувачем може призвести до блокування роботи інших користувачів, компонентів КС або КС в цілому.

З урахуванням особливостей надання доступу до інформації WEB-сторінки, типових характеристик середовищ функціонування та особливостей технологічних процесів оброблення інформації визначаються наступні мінімально необхідні рівні послуг безпеки для забезпечення захисту інформації від загроз:

– за умови, коли WEB-сервер і робочі станції розміщуються на території установи-власника WEB-сторінки або на території оператора (технологія Т1), мінімально необхідний функціональний профіль визначається:

КА–2, ЦА–1, ЦО–1, ДВ–1, ДР–1, НР–2, НИ–2, НК–1, НО–1, НЦ–1, НТ–1;

– за умови, коли WEB-сервер розміщується у оператора, а робочі станції – на території власника WEB-сторінки, взаємодія яких з WEB-сервером здійснюється з використанням мереж передачі даних (технологія Т2), мінімально необхідний функціональний профіль визначається:

КА–2, КВ–1, ЦА–1, ЦО–1, ЦВ–1, ДВ–1, ДР–1, НР–2, НИ–2, НК–1, НО–1,НЦ–1, НТ–1, НВ–1.

Технологія Т1 різниться від технології Т2 способом передачі інформації від робочої станції до WEB-сервера, а саме: наявністю у другому випадку незахищеного середовища, яке не контролюється, і додатковими вимогами щодо ідентифікації та автентифікації між КЗЗ робочої станції й КЗЗ WEB-сервера під час спроби розпочати обмін інформацією та забезпечення цілісності інформації при обміні.

РОЗДІЛ 11 ПІДРОЗДІЛ ЗАХИСТУ ІНФОРМАЦІЇ В ПІДПРИЄМСТВІ

11.1 Мета створення підрозділу захисту інформації

Метою створення підрозділу захисту інформації (ПЗІ) є організаційне забезпечення завдань керування комплексною системою захисту інформації (КСЗІ) в Підприємстві та здійснення контролю за її функціонуванням.

На ПЗІ покладається виконання робіт з визначення вимог з захисту інформації в автоматизованій інформаційній системі підприємства (КС), проектування, розроблення і модернізації КСЗІ, а також з експлуатації, обслуговування, підтримки працездатності КСЗІ, контролю за станом захищеності інформації в КС.

Правову основу для створення і діяльності ПЗІ становлять Закон України “Про державну таємницю”, Закон України “Про захист інформації в автоматизованих системах”, Положення про технічний захист інформації в Україні, Положення про забезпечення режиму обмеження доступу під час обробки інформації, що становить державну таємницю, в автоматизованих системах, інші нормативно-правові акти з питань захисту інформації, державні і галузевими стандарти, розпорядчі та інші документи.

ПЗІ здійснює діяльність відповідно до “Плану захисту інформації”, календарних, перспективних та інших планів робіт, затверджених керівником (заступником керівника) підприємства.

Для проведення окремих заходів з захисту інформації в КС, які пов’язані з напрямком діяльності інших підрозділів підприємства, керівник підприємства своїм наказом визначає перелік, строки виконання та підрозділи для виконання цих робіт.

У своїй роботі ПЗІ взаємодіє з підрозділами підприємства (РСО, службою охорони, та ін.), а також з державними органами, установами та організаціями, що займаються питаннями захисту інформації.

У разі потреби, до виконання робіт можуть залучатися зовнішні організації, що мають ліцензії на відповідний вид діяльності у сфері захисту інформації.

11.2 Завдання підрозділу захисту інформації

Завданнями ПЗІ є:

– забезпечення безпеки інформації структурних підрозділів та персоналу підприємства в процесі інформаційної діяльності та взаємодії між собою, а також у взаємовідносинах з зовнішніми вітчизняними і закордонними організаціями;

– дослідження технології обробки інформації з метою виявлення можливих каналів витоку та інших загроз для безпеки інформації, формування моделі загроз, розроблення політики безпеки інформації, визначення заходів, спрямованих на її реалізацію;

– організація та координація робіт, пов’язаних з захистом інформації в Підприємстві, необхідність захисту якої визначається чинним законодавством, підтримка необхідного рівня захищеності інформації, ресурсів і технологій;

– розроблення проектів нормативних і розпорядчих документів, чинних у межах організації, згідно з якими повинен забезпечуватися захист інформації в Підприємстві;

– організація робіт зі створення і використання КСЗІ на всіх етапах життєвого циклу КС;

– участь в організації професійної підготовки і підвищенні кваліфікації персоналу та користувачів КС з питань захисту інформації;

– формування у персоналу і користувачів підприємства розуміння необхідності виконання вимог нормативно-правових актів, нормативних і розпорядчих документів, що стосуються сфери захисту інформації;

– організація забезпечення виконання персоналом і користувачами вимог нормативно-правових актів, нормативних і розпорядчих документів з захисту інформації Підприємстві та проведення контрольних перевірок їх виконання

– забезпечення визначених політикою безпеки властивостей інформації (конфіденційності, цілісності, доступності) під час створення та експлуатації КС;

– своєчасне виявлення та знешкодження загроз для ресурсів КС, причин та умов, які спричиняють (можуть привести до) порушення її функціонування та розвитку;

– створення механізму та умов оперативного реагування на загрози для безпеки інформації, інші прояви негативних тенденцій у функціонуванні КС;

– ефективне знешкодження (попередження) загроз для ресурсів КС шляхом комплексного впровадження правових, морально-етичних, фізичних, організаційних, технічних та інших заходів забезпечення безпеки;

– керування засобами захисту інформації, керування доступом користувачів до ресурсів КС, контроль за їхньою роботою з боку персоналу ПЗІ, оперативне сповіщення про спроби НСД до ресурсів КС підприємства;

– реєстрація, збір, зберігання, обробка даних про всі події в системі, які мають відношення до безпеки інформації;

– створення умов для максимально можливого відшкодування та локалізації збитків, що завдаються неправомірними (несанкціонованими)

діями фізичних та юридичних осіб, впливом зовнішнього середовища та іншими чинниками, зменшення негативного впливу наслідків порушення безпеки на функціонування КС.

11.3 Функції ПЗІ під час створення комплексної системи захисту інформації

До функцій ПЗІ під час створення КСЗІ підприємства належать:

– визначення переліків відомостей, які підлягають захисту в процесі обробки, інших об'єктів захисту в КС, класифікація інформації за вимогами до її конфіденційності або важливості для організації, необхідних рівнів захищеності інформації, визначення порядку введення (виведення), використання та розпорядження інформацією в КС;

– розробка та коригування моделі загроз і моделі захисту інформації в КС, політики безпеки інформації в КС;

– визначення і формування вимог до КСЗІ;

– організація і координація робіт з проектування та розробки КСЗІ, безпосередня участь у проектних роботах з створення КСЗІ;

– підготовка технічних пропозицій, рекомендацій щодо запобігання витоку інформації технічними каналами та попередження спроб несанкціонованого доступу до інформації під час створення КСЗІ;

– організація робіт і участь у випробуваннях КСЗІ, проведенні її експертизи;

– вибір організацій-виконавців робіт з створення КСЗІ, здійснення контролю за дотриманням встановленого порядку проведення робіт з захисту інформації, у взаємодії з РСО, службою охорони підприємства погодження основних технічних і розпорядчих документів, що супроводжують процес створення КСЗІ (технічне завдання, технічний і робочий проекти, програма і методика випробувань, плани робіт та ін.);

– участь у розробці нормативних документів, чинних у межах підприємства і КС, які встановлюють дисциплінарну відповідальність за порушення вимог з безпеки інформації та встановлених правил експлуатації КСЗІ;

– участь у розробці нормативних документів, чинних у межах підприємства і КС, які встановлюють правила доступу користувачів до ресурсів КС, визначають порядок, норми, правила з захисту інформації та здійснення контролю за їх дотриманням (інструкцій, положень, наказів, рекомендацій та ін.).

11.4 Функції ПЗІ під час експлуатації комплексної системи захисту інформації

До функцій ПЗІ під час експлуатації КСЗІ підприємства належать:

– організація процесу керування КСЗІ;

– розслідування випадків порушення політики безпеки, небезпечних та непередбачених подій, здійснення аналізу причин, що призвели до них, супроводження банку даних таких подій;

– вжиття заходів у разі виявлення спроб НСД до ресурсів КС, порушенні правил експлуатації засобів захисту інформації або інших дестабілізуючих факторів;

– забезпечення контролю цілісності засобів захисту інформації та швидке реагування на їх вихід з ладу або порушення режимів функціонування;

– організація керування доступом до ресурсів КС (розподілення між користувачами необхідних реквізитів захисту інформації – паролів, привілеїв, ключів та ін.);

– супроводження і актуалізація бази даних захисту інформації (матриці доступу, класифікаційні мітки об’єктів, ідентифікатори користувачів тощо);

– спостереження (реєстрація і аудит подій в КС, моніторинг подій тощо) за функціонуванням КСЗІ та її компонентів;

– підготовка пропозицій щодо удосконалення порядку забезпечення захисту інформації в КС, впровадження нових технологій захисту і модернізації КСЗІ;

– організація та проведення заходів з модернізації, тестування, оперативного відновлення функціонування КСЗІ після збоїв, відмов, аварій КС або КСЗІ;

– участь в роботах з модернізації КС – узгодженні пропозицій з введення до складу КС нових компонентів, нових функціональних завдань і режимів обробки інформації, заміни засобів обробки інформації тощо;

– забезпечення супроводження і актуалізації еталонних, архівних і резервних копій програмних компонентів КСЗІ, забезпечення їхнього зберігання і тестування;

– проведення аналітичної оцінки поточного стану безпеки інформації в КС (прогнозування виникнення нових загроз і їх врахування в моделі загроз, визначення необхідності її коригування, аналіз відповідності технології обробки інформації і реалізованої політики безпеки поточній моделі загроз та ін.);

– інформування власників інформації про технічні можливості захисту інформації в КС і типові правила, встановлені для персоналу і користувачів КС;

– негайне втручання в процес роботи КС у разі виявлення атаки на КСЗІ, проведення у таких випадках робіт з викриття порушника;

– регулярне подання звітів керівництву підприємства–власника (розпорядника) КС про виконання користувачами КС вимог з захисту інформації;

– аналіз відомостей щодо технічних засобів захисту інформації нового покоління, обґрунтування пропозицій щодо придбання засобів для підприємства;

– контроль за виконанням персоналом і користувачами КС вимог, норм, правил, інструкцій з захисту інформації відповідно до визначеної політики безпеки інформації, у тому числі контроль за забезпеченням режиму обмеження доступу у разі обробки в КС інформації, що становить державну таємницю;

– контроль за забезпеченням охорони і порядку зберігання документів (носіїв інформації), які містять відомості, що підлягають захисту;

– розробка і реалізація спільно з РСО підприємства комплексних заходів з безпеки інформації під час проведення заходів з науково-технічного, економічного, інформаційного співробітництва з іноземними фірмами, а також під час проведення нарад, переговорів та ін., здійснення їхнього технічного та інформаційного забезпечення.

11.5 Повноваження та відповідальність підрозділу захисту інформації

ПЗІ має право:

– здійснювати контроль за діяльністю будь-якого структурного підрозділу підприємства (КС) щодо виконання ним вимог нормативно-правових актів і нормативних документів з захисту інформації;

– подавати керівництву підприємства пропозиції щодо призупинення процесу обробки інформації, заборони обробки, зміни режимів обробки, тощо у випадку виявлення порушень політики безпеки або у випадку виникнення реальної загрози порушення безпеки;

– складати і подавати керівництву підприємства акти щодо виявлених порушень політики безпеки, готувати рекомендації щодо їхнього усунення;

– проводити службові розслідування у випадках виявлення порушень;

– отримувати доступ до робіт та документів структурних підрозділів підприємства (КС), необхідних для оцінки вжитих заходів з захисту інформації та підготовки пропозицій щодо їхнього подальшого удосконалення;

– готувати пропозиції щодо залучення на договірній основі до виконання робіт з захисту інформації інших організацій, які мають ліцензії на відповідний вид діяльності;

– готувати пропозиції щодо забезпечення КС (КСЗІ) необхідними технічними і програмними засобами захисту інформації та іншою

спеціальною технікою, які дозволені для використання в Україні з метою забезпечення захисту інформації;

– виходити до керівництва підприємства з пропозиціями щодо подання заяв до відповідних державних органів на проведення державної експертизи КСЗІ або сертифікації окремих засобів захисту інформації;

– узгоджувати умови включення до складу КС нових компонентів та подавати керівництву пропозиції щодо заборони їхнього включення, якщо вони порушують прийняту політику безпеки або рівень захищеності ресурсів КС;

– надавати висновки з питань, що належать до компетенції ПЗІ, які необхідні для здійснення інформаційної діяльності підприємства, особливо технологій, доступ до яких обмежено, інших проектів, що потребують технічної підтримки з боку співробітників ПЗІ;

– виходити до керівництва підприємства з пропозиціями щодо узгодження планів і регламенту відвідування КС сторонніми особами;

– інші права, які надані ПЗІ у відповідності з специфікою та особливостями діяльності підприємства щодо КС.

ПЗІ зобов'язаний:

– організовувати забезпечення повноти та якісного виконання організаційно-технічних заходів з захисту інформації в КС;

– вчасно і в повному обсязі доводити до користувачів і персоналу КС інформацію про зміни в галузі захисту інформації, які їх стосуються;

– перевіряти відповідність прийнятих в підприємства правил, інструкцій щодо обробки інформації, здійснювати контроль за виконанням цих вимог;

– здійснювати контрольні перевірки стану захищеності інформації в КС;

– забезпечувати конфіденційність робіт з монтажу, експлуатації та технічного обслуговування засобів захисту інформації, встановлених в Підприємстві;

– сприяти і, у разі необхідності, брати безпосередню участь у проведенні вищими органами перевірок стану захищеності інформації в КС;

– сприяти (технічними та організаційними заходами) створенню і дотриманню умов збереження інформації, отриманої організацією на договірних, контрактних або інших підставах від організацій-партнерів, постачальників, клієнтів та приватних осіб;

– періодично, не рідше одного разу на місяць (інший термін), подавати керівництву підприємства звіт про стан захищеності інформації в КС і дотримання користувачами та персоналом КС встановленого порядку і правил захисту інформації;

– негайно повідомляти керівництво КС (підприємства) про виявлені атаки та викритих порушників;

– Інші обов’язки, покладені на керівника та співробітників ПЗІ у відповідності з специфікою та особливостями діяльності КС підприємства.

11.6 Відповідальність ПЗІ

Керівництво та співробітники ПЗІ за невиконання або неналежне виконання службових обов’язків, допущені ними порушення встановленого порядку захисту інформації в КС несуть дисциплінарну, адміністративну, цивільно-правову, кримінальну відповідальність згідно з законодавством України.

Персональна відповідальність керівника та співробітників ПЗІ визначається посадовими (функціональними) інструкціями.

Відповідальність за діяльність ПЗІ покладається на її керівника.

Керівник ПЗІ відповідає за:

– організацію робіт з захисту інформації в КС, ефективність захисту інформації відповідно до діючих нормативно-правових актів;

– своєчасне розроблення і виконання “Плану захисту інформації в автоматизованій системі”;

– якісне виконання співробітниками ПЗІ завдань, функцій та обов'язків, зазначених у цьому Положенні, посадових інструкціях, а також планових заходів з захисту інформації, затверджених керівником підприємства;

– координацію планів діяльності підрозділів та служб КС (підприємства) з питань захисту інформації;

– створення системи навчання співробітників, користувачів, персоналу КС з питань захисту інформації;

– виконання особисто та співробітниками ПЗІ розпоряджень керівника підприємства, правил внутрішнього трудового розпорядку, встановленого режиму, правил охорони праці та протипожежної охорони.

Співробітники ПЗІ відповідають за:

– додержання вимог нормативних документів, що визначають порядок організації робіт з захисту інформації, інформаційних ресурсів та технологій;

– повноту та якість розроблення і впровадження організаційно-технічних заходів з захисту інформації в КС, точність та достовірність отриманих результатів і висновків з питань, що належать до компетенції ПЗІ;

– дотримання термінів проведення контрольних, інспекційних, перевірочних та інших заходів з оцінки стану захищеності інформації в КС, які включені до плану робіт ПЗІ;

– якість та правомірність документального оформлення результатів робіт окремих етапів створення КСЗІ, документального оформлення результатів перевірок;

– інші питання персональної відповідальності, які покладені на керівника та співробітників ПЗІ у відповідності з специфікою та особливостями діяльності підприємства.

11.7 Взаємодія підрозділу захисту інформації з іншими підрозділами підприємства та зовнішніми організаціями

ПЗІ здійснює свою діяльність у взаємодії з науковими, виробничими та іншими організаціями, державними органами і установами, що займаються питаннями захисту інформації.

Заходи з захисту інформації в КС повинні бути узгоджені ПЗІ з заходами охоронної та режимно-секретної діяльності інших підрозділів підприємства.

ПЗІ взаємодіє, узгоджує свою діяльність та встановлює зв'язки з:

– РСО підприємства;

– адміністрацією КС та іншими підрозділами підприємства, діяльність яких пов'язана з захистом інформації або її автоматизованою обробкою;

– службою охорони підприємства;

– зовнішніми організаціями, які є партнерами, користувачами, постачальниками, виконавцями робіт;

– підрозділами служб безпеки іноземних фірм (що є для підприємства партнерами, користувачами, постачальниками, виконавцями робіт), їхніми представництвами (на договірних або інших засадах);

– іншими суб'єктами діяльності у сфері захисту інформації.

Керівники відповідних підрозділів підприємства повинні своєчасно інформувати ПЗІ про пересування та зміни в складі технічних засобів ОІД де обробляться ІзОД.

Взаємодію з іншими підрозділами підприємства з питань, що безпосередньо не пов'язані з захистом інформації, ПЗІ здійснює у відповідності з наказами та (або) розпорядженнями керівника підприємства.

11.8. Штатний розклад та структура підрозділу захисту інформації

ПЗІ є штатним підрозділом підприємства безпосередньо підпорядкованим з питань ТЗІ Керівнику підприємства або його заступнику, що відповідає за забезпечення безпеки інформації.

Штатність чи позаштатність ПЗІ в підприємства визначається керівництвом підприємства.

Структура ПЗІ, її склад і чисельність визначається фактичними потребами підприємства для виконання вимог політики безпеки інформації та затверджується керівництвом підприємства.

Чисельність і склад ПЗІ мають бути достатніми для виконання усіх завдань з захисту інформації.

З метою ефективного функціонування і керування захистом інформації ПЗІ має штатний розклад, який включає перелік функціональних обов'язків усіх співробітників, необхідних вимог до рівня їхніх знань та навичок.

Штат ПЗІ комплектується спеціалістами, які мають спеціальну технічну освіту (вищу, середню спеціальну, спеціальні курси підвищення кваліфікації у галузі ТЗІ тощо) та практичний досвід роботи, володіють навичками з розробки, впровадження, експлуатації КСЗІ і засобів захисту інформації, а також реалізації організаційних, технічних та інших заходів з захисту інформації, знаннями і вмінням застосовувати нормативно-правові документи у сфері захисту інформації.

Функціональні обов'язки співробітників визначаються переліком і характером завдань, які покладаються на ПЗІ керівництвом підприємства.

В залежності від обсягів і особливостей завдань ПЗІ до її складу можуть входити спеціалісти (групи спеціалістів, підрозділи та ін.) різного фаху:

– спеціалісти з питань захисту інформації від витоку технічними каналами;

– спеціалісти з питань захисту каналів зв'язку і комутаційного обладнання, налагодження і керування активним мережевим обладнанням;

– спеціалісти з питань адміністрування та контролю засобів захисту, керування системами доступу та базами даних захисту;

– спеціалісти з питань захищених технологій обробки інформації.

За посадами співробітники ПЗІ можуть поділятися на такі категорії (за рівнем ієрархії):

– керівник ПЗІ;

– адміністратори захисту КС (безпеки баз даних, безпеки системи тощо);

– спеціалісти служби захисту.