УДК 681.3

С.М. Головань

ЗАХИСТ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В ОРГАНІЗАЦІЇ

General approaches are expounded to the construction of plan of providing of technical defence of confidential information on all stages of its life cycle and the variant of form of plan is offered.

Вступ

Технічний захист конфіденційної інформації – діяльність спрямована на забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності (унеможливлення блокування) інформації [1].

Заходи по захист конфіденційної інформації можливо поділити на правові (законодавчі), організаційні (адміністративні), фізичні і технічні (апаратні і програмні), що реалізують функції і задачі комплексної системи захисту конфіденційної інформації в інформаційній системі, повинні забезпечувати:

– попередження появи загроз;
– виявлення появи загроз;
– попередження впливу загроз на інформаційну систему;
– локалізація впливу загроз на інформаційну систему;
– ліквідація наслідків впливу загроз на інформаційну систему;

Забезпечення безпеки конфіденційної інформації в інформаційній системі може бути ефективним тільки в тому випадку, коли її захист буде представляти собою безперервний і цілеспрямований процес, постійно здійснений на всіх етапах життєвого циклу конфіденційної інформації. Так комплексна система захисту конфіденційної інформації в інформаційній системі крім функцій, задач і засобів власне забезпечення захисту конфіденційної інформації повинна включати функції, задачі і засоби управління в якості одного із основних компонентів.

Комплексна система захист конфіденційної інформації інформаційної системи та її складових повинна реалізуватися на принципах:

– системності;
– комплектності;
– адекватності;
– функціональній самостійності;
– зручності користування;
– обмеження доступу до конфіденційної інформації;
– повний контроль за роботою інформаційної системи;
– своєчасне реагування на появу загроз;
– економічності.

В даній статті зупинимось на основному питанні – організація захисту конфіденційної інформації на всіх етапах її життєвого циклу.

План захисту конфіденційної інформації

План заходів щодо забезпечення технічного захисту конфіденційної інформації розробляється на підставі технології обробки конфіденційної інформації, аналізу ризиків, сформульованої політики її безпеки. План визначає основні завдання захисту, загальні правила обробки конфіденційної інформації в інформаційній системі, мету побудови та функціонування комплексної системи захисту конфіденційної інформації. План має фіксувати на певний момент часу виконавці які не мають допуску та доступу до конфіденційної інформації, але беруть участь в обслуговуванні системи, склад необхідної технічної документації тощо.

План забезпечення технічного захисту конфіденційної інформації на всіх етапах її життєвого циклу повинен регулярно переглядатися та при необхідності змінюватися. Зміни та доповнення до нього затверджуються на тому ж рівні та в тому порядку, що і основні документи.

Наведено зразок форми плану забезпечення технічного захисту конфіденційної інформації на всіх етапах її життєвого циклу.

Приклад

Гриф обмеження доступу
(при необхідності)

ПОГОДЖЕНО	**ЗАТВЕРДЖУЮ**
Найменування посади керівника організації (замовника)	Найменування посади керівника організації (виконавця)
Підпис Ініціал(и), прізвище	Підпис Ініціал(и), прізвище
Дата	Дата

ПЛАН

забезпечення технічного захисту конфіденційної інформації на всіх етапах її життєвого циклу

1. Найменування теми _____ шифр _____

Тема відноситься до _____ робіт, технічне завдання та документація до нього має гриф обмеження доступу _____ , технічні параметри _____ ,

Розробляються в підрозділі _____ організації _____ .

Строк виконання технічного захисту інформації з _____ до _____ .

Технічний захист конфіденційної інформації виконується на підставі _____

_____

(постанови, рішення, план-графік чи інші вказівки по виконанню, номер, дата)

Примітка. Керівник теми при складанні плану заходів необхідно керуватися стандартом організації: _____

2. Організація-замовник (адреса і найменування) _____

3. Адреса і найменування співвиконавця за темою (характер виконуваної роботи, керівник роботи, інформація про роботи, що виконуються за темою) _____

4. Виконавці які мають доступ до конфіденційної інформації

Посада	Прізвище, ініціал(и)	Місце роботи (відділ, цех тощо)	Форма допуску

5. Виконавці які не мають доступу до конфіденційної інформації і беруть участь в технічному обслуговуванні за темою

Посада	Прізвище, ініціал(и)	Місце роботи (відділ, цех тощо)	Форма допуску

6. Порядок користування матеріальними носіями конфіденційної інформації

Вказується:

– документація яка необхідна для роботи;

– з дозволу (керівника організації, начальника відділу тощо).

7. Порядок ознайомлення з матеріалами розробника:

– представника замовника _____

– представників сторонніх організацій _____

8. Порядок листування за темою _____

9. Порядок проведення нарад (приміщення, № кімнати, об'єм інформації) _____

10. Перелік документів з грифом обмеження доступу, необхідних при виконанні

Назва документу	Примітка

Примітка. Керівник теми при визначенні необхідного виду документації з грифом обмеження доступу, в залежності від характеру розробки, необхідно керуватися стандартом організації _____

11. Порядок опублікування та передачі документів стороннім організаціям _____

12. Заходи щодо технічного захисту інформації початок з _____ до _____ згідно з інструкціями щодо технічного захисту інформації інв. № _____

а) відомості, що підлягають захисту за допомогою технічних засобів _____

б) види та засоби технічного захисту інформації _____

13. ЗАБЕЗПЕЧЕННЯ ЗАХОДІВ ПО ТЕХНІЧНОМУ ЗАХИСТУ ІНФОРМАЦІЇ

Етапи побудови системи захисту конфіденційної інформації	Гриф обмеження доступу	Строк проведення робіт
Визначення та аналіз загроз		
Розроблення системи захисту конфіденційної інформації		
Реалізація плану захисту конфіденційної інформації		
Контроль функціонування та керування системою захисту конфіденційної інформації		

Примітка 1. На першому етапі необхідно здійснити аналіз об'єктів, ситуаційний план, умов функціонування організації, оцінити ймовірність прояву загроз та очікувану шкоду від їх реалізації, підготувати дані для побудови окремої моделі загроз.

Примітка 2. На другому етапі слід розробити план технічного захисту конфіденційної інформації, що містить організаційні, первині технічні та основні технічні заходи захисту конфіденційної інформації, визначити зони безпеки інформації.

Примітка 3. На третьому етапі слід реалізувати організаційні, первині технічні та основні технічні заходи захисту конфіденційної інформації, установити необхідні зони безпеки інформації, провести атестацію технічних засобів забезпечення інформаційної діяльності, робочих місць (приміщень) на відповідність вимогам безпеки інформації.

Примітка 4. На четвертому етапі слід провести аналіз функціонування системи захисту конфіденційної інформації, перевірку виконання заходів технічного захисту конфіденційної інформації, контроль ефективності захисту, підготувати та видати дані для керування системою захисту конфіденційною інформацією.

14. ПОЕТАПНО НА ВЕСЬ ПЕРІОД РОБОТИ

Відділ, цех, номер кімнати, в яких проводиться розробка, складання, монтаж, випробування	Виконавці, (прізвище, ініціал(и), підрозділ)	Забезпечення заходів режиму на період робіт (при наявності охоронної сигналізації, шифр-замка, списку осіб які мають доступ до приміщення тощо)	Примітка

15. Коли закінчена робота за темою. Які підсумкові документи видані, їх облікові номери. Список осіб, яким дозволено користуватися матеріалами роботи _____

Від замовника

Керівник робіт
Підпис Ініціал(и), прізвище

Начальник підрозділу
Підпис Ініціал(и), прізвище

Від виконавця

Керівник робіт
Підпис Ініціал(и), прізвище

Начальник підрозділу
Підпис Ініціал(и), прізвище

При виконанні робіт забороняється:

– ознайомлення із конфіденційної інформації представникам інших організацій і співробітників не працюючих за цією темою;

– залучати інших організацій для виконання робіт;

– використовувати матеріали, отримані при виконанні робіт в статтях, дисертаціях, виступах на симпозіумах, конференціях тощо.

Для технічного захисту конфіденційної інформації слід застосовувати заходи приховування або заходи технічної дезінформації.

Заходи захисту конфіденційної 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 конфіденційної інформації на встановленому рівні протягом часу обмеження доступу до неї або можливостям здійснення загроз.

Рівень захисту конфіденційної інформації визначається системою кількісних та якісних показників, які забезпечують розв'язання завдання захисту конфіденційної інформації на основі норм і вимог технічного захисту інформації.

Мінімально необхідний рівень захисту конфіденційної інформації забезпечують обмежувальними і фрагмент ними заходами протидії найнебезпечнішій загрозі.

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

Порядок розрахунку та інструментального визначення зон безпеки конфіденційної інформації, реалізація заходів технічного захисту конфіденційної інформації, розрахунку ефективності захисту та порядку атестації технічних засобів забезпечення інформаційної діяльності, робочих місць (приміщень) установлюються нормативними документами з технічного захисту інформації.

Технічне завдання на створення комплексної системи захисту конфіденційної інформації в інформаційній системі є організаційно-технічним документом для виконання робіт щодо забезпечення захисту конфіденційної інформації в системі.

Технічне завдання на комплексну систему захисту конфіденційної інформації розробляється у разі необхідності розробки або модернізації комплексної системи захисту конфіденційної інформації існуючої (що функціонує) інформаційної системи. В разі розробки комплексної системи захисту конфіденційної інформації в процесі проектування інформаційної системи допускається оформлення вимог захисту конфіденційної інформації в інформаційній системі у вигляді окремого (часткового) технічного завдання, доповнення до загального технічного завдання на інформаційну систему або розділу загального технічного завдання на інформаційну систему.

В технічному завданні на комплексну систему захисту конфіденційної інформації викладаються вимоги до функціонального складу і порядку розробки та впровадження технічних засобів, що забезпечують безпеку інформації в процесі її оброблення в інформаційній системі. Додатково треба викласти вимоги до організаційних, фізичних та інших заходів захисту, що реалізуються поза інформаційною системою у доповнення до комплексу програмно-технічних засобів захисту конфіденційної інформації.

Перелік вимог з захисту конфіденційної інформації, які включаються в технічне завдання на комплексну систему захисту конфіденційної інформації, може бути для кожної конкретної інформаційної системи як розширений так і скорочений.

Вимоги повинні передбачати розроблення та використання сучасних ефективних засобів і методів захисту, які дають можливість забезпечення виконання цих вимог з найменшими матеріальними затратами.

Висновки

Викладені загальні підходи до побудови плану забезпечення технічного захисту конфіденційної інформації на всіх етапах її життєвого циклу та запропоновано варіант форми плану.

1. *Термінологія* в галузі інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 1.1-003-99, ДСТЗІ СБ України, К.: 1999.

2. *Закон України* „Про електронні документи та електронний документообіг ": Закон України від 22.05.93 № 851-IV // Відомості Верховної Ради України. – 2003. – № 36. – Ст. 275.