Секція: Юридичні науки

Тертичний Самір Сахільович
студент
Національного авіаційного університету
м. Київ, Україна

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ІМПЛЕМЕНТАЦІЇ ЗАКОРДОННОГО ДОСВІДУ ЗАХИСТУ ЕЛЕКТРОННОЇ ІНФОРМАЦІЇ

Оцінка проблем і перспектив імплементації іноземного досвіду захисту електронної інформації є вельми актуальним науковим питанням з огляду на такі фактори:

– Інформація та інформаційні системи організацій, мережеве оточення, у яких вони функціонують, є невід'ємними складовими сучасного ділового середовища. Їх доступність, цілісність і конфіденційність можуть мати вирішальне значення для забезпечення конкурентоспроможності підприємства, руху коштів, рентабельності, відповідності правовим нормам і стандартам.

– Водночас, унаслідок посилення залежності підприємств від інформаційних, комунікаційних систем і сервісів вони стають вразливішими до порушень режиму безпеки.

– Поширення інформаційних і комунікаційних систем надає все нові можливості несанкціонованого доступу до інформаційних ресурсів, а тенденція до переходу на розподілені обчислювальні системи обмежує можливості фахівців централізовано контролювати інформаційні системи та мережеве оточення.

Порушення режиму безпеки інформаційних систем може істотно ускладнити реалізацію виробничих завдань, тому вирішення проблеми формування ефективної системи захисту інформації набуває дуже

важливого значення. Це пояснюється тим, що у процесах розроблення й удосконалення систем ЗІ є чимало недостатньо вивчених і досліджених аспектів, які можуть негативно впливати на показники ефективності та надійності функціонування системи безпеки загалом.

Питанням розробки і функціонування систем захисту інформації присвячено значну кількість праць В. О. Хорошка [1], В.Б. Дудикевича [2; 3], О. С. Петрова [1] та ін. Проблематика сучасних загроз інформаційної безпеки для державних та приватних українських установ, міжнародні стандарти безпеки досліджені в роботах А. В. Платоненко, А.О. Аносова [4], О. В. Сєвєрінова, В. І. Черниша, М. Є. Молчанова [5-6] та ін.

Заходи із захисту 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.

Закордонний досвід захисту електронної інформації будується на певних стандартах і критеріях. Базовим міжнародним стандартом з інформаційної безпеки, розробленим спільно Міжнародною організацією зі стандартизації й Міжнародною електротехнічною комісією є ISO/IEC 27001. Підготовлений до випуску підкомітетом SC27 Об'єднаного технічного комітету JTC 1, стандарт містить вимоги у сфері інформаційної безпеки для створення, розвитку й підтримки Системи менеджменту інформаційної безпеки [8].

Відповідно до іноземного досвіду, організація може бути сертифікована акредитованими агентствами відповідно до цього стандарту. Процес сертифікації складається із трьох стадій:

– стадія 1 – вивчення аудитором ключових документів системи менеджменту інформаційної безпеки – положення про застосовність, план обробки ризиків тощо. Стадія може виконуватися як на території організації так і шляхом висилки цих документів зовнішньому аудиторові;

– стадія 2 – детальний, глибокий аудит, включаючи тестування впроваджених заходів і оцінка їх ефективності. Включає повне вивчення документів, які вимагає стандарт;

– стадія 3 – виконання інспекційного аудита для підтвердження, що сертифікована організація відповідає заявленим вимогам. Виконується на періодичній основі.

Процедура системи менеджменту за кожним із міжнародних стандартів або їх комбінації розподіляється на 4 етапи:

– підготовка до сертифікації;

– аудит 1-го щабля (перевірка готовності до сертифікації);

– аудит 2-го щабля (сертифікаційний аудит);

– видача сертифіката й нагляд.

Також закордоном активно розробляються й удосконалюються критерії оцінки інформаційної безпеки, які почали застосовуватися із розробки критеріїв оцінки довірених комп'ютерних систем у США (т. зв. «Помаранчева книга»).

В 1995 році Європейським Союзом була прийнята Директива щодо захисту особистості з дотриманням режиму персональних даних та вільного руху таких даних. Директива спрямована на впорядкування практики захисту інформації в межах Європейського Союзу. Однією з вимог, адресованих державам-учасникам, є вимога прийняти закони щодо захисту персональної інформації, як в публічному, так і в приватному секторі.

Зазначені закони мають також включати тимчасове блокування переміщення інформації до державне членів Європейського Союзу, які не встановили «адекватного» рівня захисту інформації.

Відповідно до загальних принципів Акту захисту інформації в телекомунікаціях, збирання, обробка та використання інформації дозволяється лише у випадках, коли воно дозволене законом або здійснюється за наявності згоди користувача обслуговування. Інформація може бути лише зібрана, оброблена або використана окремо для різних послуг, яких потребує один і той самий користувач. Згода користувача не може виступати в якості умов для надання послуг. Інформація за договором може бути зібрана, оброблена та використана в тому обсязі, який є необхідним для виконання договору. Дані використання та бухгалтерського обліку не повинні передаватися третім особам. Однак деякі з зазначених вище типів даних можуть бути передані для певної мети обслуговування постачальників від постачальників, через яких здійснений доступ до послуг [4, с. 90].

Загалом, як свідчить іноземний досвід, проведення роботи в галузі захисту інформації дозволяє оцінити або переоцінити рівень поточного стану інформаційної безпеки організації, виробити рекомендації щодо забезпечення (підвищенню) інформаційної безпеки організації, знизити потенційні втрати підприємства чи організації через підвищення стійкості функціонування корпоративної мережі, розробити концепцію та політику безпеки установи, а також запропонувати плани захисту конфіденційної інформації організації, що передається по відкритих каналах зв'язку, захисту інформації закладу від навмисного спотворення (руйнування), несанкціонованого доступу до неї, її копіювання чи використання.

Діяльнісний аспект захисту інформації здійснюється у рамках організаційної системи захисту інформації. Діяльність має певні властивості, а саме: ефективність, зрілість, адекватність, прийнятність,

гнучкість, здійсненність та простоту в адміністративному забезпеченні. Ефективність є досить широкою властивістю, що дозволяє досліджувати її на більш глибокому рівні. Ефективність захисту інформації можна розглядати з точки зору результативності, економічності та оперативності

Література

1. Нормативне забезпечення інформаційної безпеки / С.М. Головань, О.С. Петров, В.О. Хорошко, Д.В. Чирков, Л.М. Щербак; За ред. проф. В.О. Хорошка. – К. : ДУІКТ, 2008. – 533 с.
2. Гарасимчук О. І. Комплексні системи санкціонованого доступу / О. І. Гарасимчук, В. Б. Дудикевич, В. А. Ромака. – Львів : Львівська політехніка, 2010. – 212 с.
3. Системи менеджменту інформаційної безпеки / В. А. Ромака, В. Б. Дудикевич, Ю. Р. Гарасим, П. І. Гаранюк, І. О. Козлюк. – Львів: Львівська політехніка, 2012. – 232 с.
4. Аносов А. О. Модель перехоплення та захист інформації в бездротових мережах / А. О. Аносов, А. В. Платоненко // Сучасний захист інформації. – 2017. – № 2. – С. 90-94.
5. Северинов А. В. Анализ угроз и рисков безопасности информации в беспроводных сетях / А. В. Северинов, В. И. Черныш // Системи управління, навігації та зв'язку. – Вип. 1. – К. : ЦНДІ НіУ, 2011. – С. 229-232.
6. Сєвєрінов О. В. Управління інформаційною безпекою згідно міжнародних стандартів / О. В. Сєвєрінов, В. І. Черниш, М. Є. Молчанова // Системи управління, навігації та зв'язку. – Вип. 4. – К. : ЦНДІ НіУ, 2011. – С. 250-253.
7. Термінологічний словник з питань технічного захисту інформації /за ред. проф. В. О. Хорошка – 3-є видання. – К. : Поліграф Колсалтинг, 2012. – 268 с.

8. ISO 27001 Британского института стандартов. URL: http://www.standardsdirect.org/iso17799.htm.