6) ідентифікація і аутентифікація при обміні для забезпечення взаємної достовірності між двома

Таким чином, ми проаналізували критерії захищеності інформаційного середовища, а саме:

- критерій захисту конфіденційності інформації;
- критерій збереження цілісності інформації;
- критерій збереження працездатності інформаційного середовища;
- критерій аудиту інформаційного середовища.

Експертна комісія, яка перевіряє рівень захищеності інформаційного середовища, визначає кількість і рівень реалізованих в інформаційній системі послуг безпеки і ступінь дотримання вимог перерахованих вище критеріїв.

Список використаних джерел

1. Нормативний документ системи технічного захисту інформації [Електронний ресурс] // Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. – 2002. – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article;jsessionid=81E66103A1845B5D12126F231FEBBD7D?showHidden=1&art_id=101885&cat_id=89734&ctime=1344501165427.

2. КЗЗ від НСД [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/term/34530.

3. Побудова раціонального захисту інформаційних ресурсів [Електронний ресурс] – Режим доступу до ресурсу: https://helpiks.org/6-9510.html.

УДК 004.056.5

АНАЛІЗ ІСНУЮЧИХ ПІДХОДІВ ДО ЗАХИСТУ ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА

Мальцева М.В., студ.гр. КБ-161,
Усов Я.Ю., викладач
Чернігівський національний технологічний університет

Для розвитку людського суспільства необхідні матеріальні, інструментальні, енергетичні та інші ресурси, в тому числі і інформаційні. Теперішній час характеризується небувалим зростанням обсягу інформаційних потоків. Це відноситься практично до будь-якій сфері діяльності людини.Інформація являє собою один з основних, вирішальних факторів, який визначає розвиток технології і ресурсів в цілому. Досліджування, що присвячені проблемі інформаційного суспільства та процесам інформатизації широко використовується поняття інформаційне середовище. Існує декілька визначень інформаційного середовища, а саме: інформаційне середовище — це світ інформації навколо людини і світ її інформаційної діяльності.Інформаційне середовище — це сукупність технічних і програмних засобів зберігання, обробки і передачі інформації, а також політичні, економічні і культурні умови реалізації процесів інформатизації. [1]. Однією з основних властивостей інформаційного середовища є, на думку І.А. Носкова, його відкритість [2, с.34]. Основними рівнями інформаційного середовища є глобальний, міжнародний, загальнодержавний, регіональний, локальний. Основною властивістю інформаційного середовища є наповнюваність інформацією, її зберігання триглавий час, варіативність та спрямованість. Тому важлива безпека інформаційного середовища та забезпечення цілісності, повноти, доступності та конфіденційності інформації яка в ній поширюється. Перед тим як аналізувати основні підходи розглянемо основні етапи захисту інформаційного середовища. По-перше, необхідно віднести секретну інформацію до категорії обмеженого доступу, по-друге, прогнозувати і своєчасно виявляти загрози безпеки інформаційних ресурсів, причин, умов, що сприяють нанесенню фінансового, матеріального збитку, порушення нормального функціонування і розвитку. Також необхідним є створення механізму і умов оперативного реагування на загрози інформаційної безпеки і прояву негативних тенденцій у функціонуванні, ефективне припинення зазіхань на ресурси на основі правових, організаційних, технічних заходів, а також інших засобів забезпечення безпеки. Важливим є створення умов максимального можливого відшкодування та локації збитку, що наноситься неправомірним діями фізичних і юридичних осіб, ослаблення негативного впливу наслідків порушення інформаційної безпеки на досягнення стратегічних цілей. Перед будуванням моделі захисту інформаційного середовища розглядується наступні фактори: загрози інформаційної безпеки, які характеризуються ймовірністю виникнення і реалізації; уразливості інформаційного середовища та ризики. Після побудови моделі відбувається безпосередньо етап захисту інформаційного середовища.

До основних підходів можна віднести: програмний, апаратний, апаратно-програмний, правовий. Також для більш повної захищеності інформаційного середовища слід використати організаційний, криптографічний, інженерний та технічний захист.

Програмний захист – комплекс спеціальних програм програмного забезпечення, які реалізують захист інформації. Захисний програмний код може виступати в якості як окремо, в якості захисного програмного продукту (антивірус, міжмережевий екран як приклад), так и входити до складу інших, багатофункціональних програм, з метою захисту інформаційного середовища. При використані програмного захисту захищається лише інформація, а отже використанні лише цього способу недостатньо для повного захисту інформаційного середовища [3].

Програмно-апаратний захист – включають програми для ідентифікації користувачів, контролю доступу, шифрування інформації, видалення залишкової (робочої) інформації типу тимчасових файлів, тестового контролю системи захисту та ін.

Правовий захист – це захист інформації, який базується на використанні статей Конституції і законів держави, положень цивільного і кримінального кодексів та інших нормативно-правових документів в галузі інформатики, інформаційних відносин, правовий статус органів, технічних засобів і способів захисту інформації і є базою для створення морально-етичних норм в області захисту інформації [4]. Основними законодавчими актами, нормативно правових та нормативних актів щодо інформаційної безпеки в Україні входять:

1. Закони України:

Закон України «Про інформацію» від 02.10.1992 № 2657-XII, Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР, Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII, Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI

2. Постанови КМУ:

Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373, Постанова Кабінету міністрів України «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію» від 27 листопада 1998 р. №1893

3. Нормативні документи в галузі технічного захисту інформації (НД ТЗІ) та державні стандарти України (ДСТУ) стосовно створення і функціонування КСЗІ:

НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі , Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96,НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу, НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу, Автоматизовані системи. Вимоги до збереження документів РД 50-34.698

4. Галузеві стандарти:

ГСТУ СУІБ 1.0/ISO/IEC 27001:2010 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги. (ISO/IEC 27001:2005, MOD), ГСТУ СУІБ 2.0/ISO/IEC 27002:2010 Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою. (ISO/IEC 27002:2005, MOD)

Організаційні засоби захисту інформації складаються з організаційно-технічних (підготовка приміщень з комп'ютерами, прокладка кабельної системи з урахуванням вимог обмеження доступу до неї та ін.) і організаційно-правових (національні законодавства і правила роботи, що встановлюються керівництвом конкретного підприємства).Організаційна захист інформації - складова частина системи захисту інформації, яка визначає і виробляє порядок і правила функціонування об'єктів захисту і діяльності посадових осіб з метою забезпечення захисту інформації.Організаційна захист інформації на підприємстві - регламентація виробничої діяльності та взаємовідносин суб'єктів (працівників підприємства) на нормативно-правовій основі, що виключає або послаблює нанесення збитку даному підприємству.Перше з наведених визначень більшою мірою показує сутність організаційної захисту інформації. Друге - розкриває її структуру на рівні підприємства. Разом з тим обидва визначення підкреслюють важливість нормативно-правового регулювання питань захисту інформації поряд з комплексним підходом до використання в цих цілях наявних сил і засобів. Основні напрямки організаційної захисту інформації: організація роботи з персоналом, організація внутрішньооб'єктногоі пропускного режимів і охорони, організація роботи з носіями відомостей, комплексне планування заходів щодо захисту інформації, організація аналітичної роботи і контролю.

Отже можна зробити висновок, що для забезпечення надійного захисту інформаційного середовища необхідно комбінувати різні підходи. Комплексний захист інформаційних ресурсів підприємств забезпечує:захист інформації від різного роду вірусних і хакерських загроз;збереження даних при фізичної втрати і поломки інформаційних носіїв;безпеку доступу до збережених ресурсів;відновлення інформаційної системи в разі пошкоджень.

Список використаних джерел

1. Інформаційне середовище [Електронний ресурс] / а – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Інформаційне_середовище

2. Носков И.А. Проблема формирования информирования информационной образовательной среды/ И.А. Носков // Интернет и образование.-200.-№32.-С.32-35

3. Защитадоступа к информации [Електронний ресурс] – Режим доступу до ресурсу: http://rus.safensoft.com/security.phtml?c=882.

4. Домарев В.В. Безопасностьинформационихтехнологий. Методологиясоздания систем захиты / В.В. Домарев.-К.: ООО ТИД ДС, 2001. – С.650