УДК 004.681 **Чирков Д.В., Сєрєнко В.Є.**

ПРАВОВІ АСПЕКТИ СТВОРЕННЯ ТА ВВЕДЕННЯ В ЕКСПЛУАТАЦІЮ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ В КОНТЕКСТІ ЗАХИСТУ ІНФОРМАЦІЇ

Вступ

Дана стаття присвячена висвітленню основних питань при створені та введенню в експлуатацію інформаційно-телекомунікаційної системи в контексті захисту інформації. Проведення аналізу вимог нормативно-правових документів України щодо захисту інформації в інформаційно-телекомунікаційних системах в державних та не державних підприємствах, установах, організаціях, повинно сприяти своєчасному, грамотному виконанню службою захисту інформації своїх функцій.

Інформаційно-телекомунікаційна система (ІТС) представляє собою сукупність фізичного середовища, програмних, апаратних, апаратно-програмних засобів, каналів зв'язку, інформаційних ресурсів, яка створюється з метою вирішення інформаційних потреб персоналу і діє як єдине ціле при залучені нормативно-правових, організаційно-розпорядчих, інженерно-технічних заходів.

Зміст та об'єм вимог щодо захисту інформації залежить в першу чергу від виду інформації яка обробляється в ІТС. Масштаби ІТС визначають об'єм вимог, менша за масштабами ІТС буде містити більш адекватно-реалізовані вимоги.

На сьогодні в державних та недержавних підприємствах, установах, організаціях є проблемним питання створення адекватної вимогам нормативних документів України системи захисту інформації в ІТС при залученні комплексного підходу. Пов'язано це з наступним:

- наявність недостатньої взаємодії функціональних підсистем підприємства, установи, організації щодо захисту інформації в ІТС на всіх стадіях її функціонування, а саме, при проектуванні телекомунікаційної системи не враховуються питання із захисту інформації, до робіт проектування не залучаються спеціалісти із захисту інформації, при виборі технічних, програмних засобів, як складових частин системи, переваги віддаються стандартним, найпоширенішим засобам, які не відповідають вимогам захисту;
- відсутність формального визначення інформаційних потоків, що призводить до відсутності формально визначеної логічної, фізичної структури телекомунікаційної системи;
- майже на всіх етапах створення комплексної системи захисту інформації, навіть обстеження функціонального середовища, залучаються зовнішні виконавці;
- і таке інше.

Для вирішення визначених проблемних питань є доцільним використання етапності при створенні та введенні в дію ІТС. Виходячи із змісту нормативно-правових актів України в галузі захисту інформації в інформаційно-телекомунікаційних системах, а також системах, які є складовими частинами ІТС, в основному вимоги висуваються до захисту державних інформаційних ресурсів.

Тому, виходячи з вище зазначеного, визначимо процедуру введення в дію ІТС в першу чергу для державних підприємств, організацій, установ, та визначимо відмінності при введені в дію ІТС недержавних структур, де обробляється лише інформація власного, користувачевого характеру.

Введення в дію ІТС в державних підприємствах, організаціях, установах

Етап 1. Телекомунікаційна система. Згідно з визначеннями Закону України „Про захист інформації в інформаційно-телекомунікаційних системах", Телекомунікаційна система - сукупність технічних і програмних засобів, призначених для обміну інформацією

шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб. Виходячи із визначення телекомунікаційної системи, та змісту „Положення про Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління" затвердженого постановою Кабінету Міністрів України від 3 серпня 2005 року № 688, „Порядку формування й користування інформаційним фондом Реєстру інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління", затвердженого наказом ДСТСЗІ СБ України від 20.01.2006 № 9, сформулюємо вимоги до даного етапу.

Визначити структуру, телекомунікаційної системи:

- Фізична структура
  - o вид комп'ютерної техніки;
  - o кількість одиниць комп'ютерної техніки;
  - o вид комутаційного та телекомутаційного обладнання;
  - o кількість одиниць комутаційного та телекомутаційного обладнання в залежності від їх виду;
  - o спосіб об'єднання комп'ютерної техніки у системі;
  - o об'єкт до якого система має підключення;
  - o тип зв'язку, що використовується у системі, а також для з'єднання з об'єктами;
  - o тип каналу зв'язку;
  - o швидкість каналу зв'язку;
  - o належність каналу зв'язку;
  - o оператор телекомунікацій;
  - o провайдер телекомунікацій;
  - o наявність кластерів, що входять до складу системи, призначення, кількість комп'ютерів у кластері, кількість зовнішніх систем збереження даних у кластері;
  - o наявність у системі сервера, де планується розміщення ресурсів, до яких здійснюється доступ з боку глобальних мереж передачі даних в тому числі Internet.
- Логічна структура
  - o спосіб об'єднання комп'ютерної техніки у системі;
  - o кількість одиниць комп'ютерної техніки в залежності від способу об'єднання;
  - o об'єкт до якого система має підключення;
  - o повне доменне ім'я сервера;
  - o IP-адреса сервера.

Визначити програмне забезпечення:

- основне програмне забезпечення;
- допоміжне програмне забезпечення;
- спеціалізоване програмне забезпечення.

А більш детально:

- o назва та версія операційної системи, що використовується в системі;
- o кількість комп'ютерів, де встановлена операційна система;
- o назва та версія програмного забезпечення, що використовується у системі;
- o кількість комп'ютерів, де встановлене програмне забезпечення;
- o тип сервера;
- o операційна система сервера.

Визначені дані повинні відображатися в технічному завдані на створення телекомунікаційної системи, як частини інформаційно-телекомунікаційної системи, або в додатках до нього.

Вимоги до структури проектованої телекомунікаційної системи діючими нормативно-правовими документами не встановлюються. Згідно з указом Президента України № 891 від 24.09.2001 року „Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних" Кабінету Міністрів України, центральним та місцевим органам виконавчої влади, іншим державним органам, а також підприємствам, установам та організаціям, зазначеним у статті 1 цього Указу, здійснювати передачу даних глобальними мережами виключно через підприємства (операторів), що визначатимуться Державним комітетом зв'язку та інформатизації України.

Процедуру підключення до глобальних мереж передачі даних визначає „Порядок підключення до глобальних мереж передачі даних" затверджений постановою Кабінету Міністрів України від 12 квітня 2002 р. N 522.

Вимоги до використання програмного забезпечення висвітлені в „Концепції легалізації програмного забезпечення та боротьби з нелегальним його використанням", затвердженої розпорядженням Кабінету Міністрів України від 15 травня 2002 р. N 247-р, зокрема обов'язковість придбання ліцензійного програмного забезпечення під час закупівлі комп'ютерної техніки. Стаття 18 Закону України „Про авторське право і суміжні права" містить наступне: Комп'ютерні програми охороняються як літературні твори. Така охорона поширюється на комп'ютерні програми незалежно від способу чи форми їх вираження.

Якщо планується створення комплексної системи захисту інформації (далі КСЗІ) в ІТС, частиною якої є дана телекомунікаційна система (КСЗІ в ІТС не створюється в одному випадку – коли інформація в ІТС відкрита і не потребує захисту) то слід враховувати вимоги статті 8 Закону України „Про захист інформації в інформаційно-телекомунікаційних системах": Для створення комплексної системи захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації.

Наприклад:

- Сервіси безпеки операційної системи Microsoft® Windows® XP Professional пакетом оновлення Service Pack 2 і з пакетом підтримки української мови;
- Кабельне обладнання виробництва компанії Reichle & De-Massari(Швейцарія);
- Комутатори "Business Policy Switch 2000";
- Маршрутизатори на апаратних платформах Cisco 2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM під керуванням операційної системи Cisco IOS 12.3 (3a) IP Feature Set виробництва компанії Cisco Systems, США.

Виконуючи дані вимоги, власник ІТС може заощадити фінансові ресурси при створені КСЗІ.

Етап 2. Інформаційна система. Даний етап є проміжним при створені та введені в дію ІТС. Він включає в себе комплекс організаційно-розпорядчих, нормативно-правових заходів по визначенню, класифікації за видом та правовим доступом інформації в системі, визначення носіїв та потоків інформації з урахуванням вже визначеної фізичної та логічної структури телекомунікаційної системи. На даному етапі доцільно буде акцентувати увагу, при визначенні вимог щодо захисту інформації користувачів (персональні дані), що обробляється в ІТС державних органів. Згідно з Законом України „Про інформацію", за

режимом доступу, персональні данні відносяться до інформації з обмеженим доступом, тому на цей вид відомостей поширюються вимоги Закону України „Про захист інформації в інформаційно-телекомунікаційних системах", але вимог щодо профілів захищеності (НД ТЗІ 2.5-005-99) персональних даних в ІТС, нормативно-правовими актами України не встановлено.

Першочерговою вимогою, яка носить рекомендаційний характер даного етапу, є класифікація інформації за видом згідно із статтею 18 Види інформації Закону України „Про інформацію":

Основними видами інформації є:

- статистична інформація;
- адміністративна інформація (дані);
- масова інформація;
- інформація про діяльність державних органів влади та органів місцевого і регіонального самоврядування;
- правова інформація;
- інформація про особу;
- інформація довідково-енциклопедичного характеру;
- соціологічна інформація.

Відкрита інформація, що є власністю держави і належить до статистичної, правової, соціологічної інформації, інформації довідково-енциклопедичного характеру та використовується для забезпечення діяльності державних органів або органів місцевого самоврядування, а також інформація про діяльність зазначених органів, яка оприлюднюється в Інтернет, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами під час обробки в системі повинна зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення (Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах).

Далі згідно із статтею 2 Класифікація інформації, що обробляється в АС НД ТЗІ 1.4-001-2000 „Типове положення про службу захисту інформації в автоматизованій системі", затвердженого наказом ДСТСЗІ СБ України від 4 грудня 2000 р. № 53 необхідне виконання наступних рекомендаційних вимог:

- Повинні бути класифіковані всі відомості за режимом доступу, за правовим режимом, а також за типом їхнього представлення в АС. Класифікація є підставою для визначення власником (розпорядником) інформації або АС методів і способів захисту кожного окремого виду інформації.
- За режимом доступу інформація в АС має бути поділена на:
  - відкриту;
  - з обмеженим доступом.

Відкриту інформацію слід поділити на відкриту, яка не потребує захисту, або захист якої забезпечувати недоцільно, та відкриту, яка такого захисту потребує. До другої слід відносити інформацію, важливу для особи, суспільства і держави (відповідно до Концепції технічного захисту інформації в Україні), важливі для організації відомості, порушення цілісності або доступності яких може призвести до моральних чи матеріальних збитків.

- За правовим режимом інформація з обмеженим доступом повинна бути поділена на таємну та конфіденційну.

До таємної інформації має бути віднесена інформація, що містить відомості, які становлять державну, а також іншу, передбачену законом таємницю.

Інформація, що становить державну таємницю, в свою чергу, поділяється на категорії відповідно до Закону України "Про державну таємницю".

Наступними діями, при створені інформаційної системи повинно бути розроблено структурну схему інформаційних потоків в системі, яка б відображала інформаційну взаємодію між основними компонентами системи з прив'язкою до кожного елемента схеми категорій інформації. Неформальне визначення схеми інформаційних потоків повинно передувати визначенню проекту телекомунікаційної системи.

Вихідними даними даного етапу, відповідно до „Положення про Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління" затвердженого постановою Кабінету Міністрів України від 3 серпня 2005 року № 688 та „Порядку формування й користування інформаційним фондом Реєстру інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління", затвердженого наказом ДСТСЗІ СБ України від 20.01.2006 № 9, мають бути:

- технічне завдання на створення системи;
- віднесення інформації у системі до державних електронних інформаційних ресурсів;
- стан обробки державних електронних інформаційних ресурсів;
- режим доступу до державних електронних інформаційних ресурсів, які планується обробляти у системі;
- вид оброблення державних електронних інформаційних ресурсів в системі;
- метод оброблення державних електронних інформаційних ресурсів в системі;
- види електронних носіїв інформації для державних електронних інформаційних ресурсів в системі.

Відомості даного етапу повинні відображатися в технічному завданні на створення інформаційної системи, або в додатках до нього.

Етап 3. Інформаційно-телекомунікаційна система – це сукупність телекомунікаційних та інформаційних систем, які у процесі обробки діють як єдине ціле. Даний етап є ключовим при створенні інформаційно-телекомунікаційної системи, та містить в собі всі засоби та заходи щодо введення інформаційно-телекомунікаційної системи в експлуатацію. Проводиться аналіз отриманих даних попередніх етапів та висуваються вимоги із захисту інформації.

Згідно із статтею 8 Умови обробки інформації в системі Закону України „Про захист інформації в інформаційно-телекомунікаційних системах":

Інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством.

Для створення комплексної системи захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються в порядку, встановленому законодавством.

Вимоги до порядку проведення КСЗІ викладені в НД ТЗІ 3.7-003-05 „Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі", затвердженого наказом ДСТСЗІ СБ України від 8 листопаду 2005 року № 125.

Дозвіл на оброблення державних інформаційних ресурсів дається наказом керівника установи (підприємства, організації), яка є власником системи за результатами проведення

державної експертизи КСЗІ, та при наявності атестату відповідності КСЗІ вимогам нормативних документів із захисту інформації.

Загальними питаннями даного етапу, відповідно до „Положення про Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління" затвердженого постановою Кабінету Міністрів України від 3 серпня 2005 року № 688 та „Порядку формування й користування інформаційним фондом Реєстру інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління", затвердженого наказом ДСТСЗІ СБ України від 20.01.2006 № 9, мають бути:

- документальне визначення відповідальної особи та/або підрозділу, на яких покладено функції служби захисту інформації за стан технічного захисту державних електронних інформаційних ресурсів у системі;
- документальне визначення відповідальної особи та/або підрозділу за стан криптографічного захисту державних електронних інформаційних ресурсів у системі;
- наявність плану захисту інформації в системі;
- наявність технічного завдання на комплексну систему захисту інформації у системі;
- наявність засобів криптографічного/технічного захисту в системі;
- категорія, тип засобу криптографічного/технічного захисту інформації у системі;
- наявність сертифікату, експертного висновку та/або документу щодо допуску до експлуатації засобу криптографічного/технічного захисту інформації в системі;
- стан виконання заходів щодо проведення державної експертизи комплексної системи захисту інформації системи;
- наявність атестату відповідності комплексної системи захисту інформації системи;
- опис факту спроби вчинення або вчинення несанкціонованих дій щодо державних інформаційних ресурсів у системі;
- документальне інформування ДСТСЗІ СБ України щодо факту спроби вчинення або вчинення несанкціонованих дій щодо державних інформаційних ресурсів у системі.

Відомості отримані на даному етапі повинні фіксуватися в технічному завданні на комплексну систему захисту інформації, плані захисту інформації, та інших документах передбачених НД ТЗІ 3.7-003-05.

Введення в дію ІТС в не державних підприємствах, організаціях, установах

Якщо в ІТС не державних підприємств, установ, організацій не обробляються державні електроні ресурси, то власники даних систем вживають заходи і засоби із захисту інформації в них на свій розсуд. На відміну від ІТС державних органів, в ІТС не державних структур, вимоги щодо захисту від несанкціонованого доступу до інформації користувачів (інформація з обмеженим доступом) не встановлені. Згідно із статтею 5. Відносини між власником інформації та власником системи Закону України „Про захист інформації в інформаційно-телекомунікаційній системи"

Власник системи забезпечує захист інформації в системі в порядку та на умовах, визначених у договорі, який укладається ним із власником інформації, якщо інше не передбачено законом.

Власник системи на вимогу власника інформації надає відомості щодо захисту інформації в системі.

Власник інформації може вимагати створення захищеного середовища обробки його інформації, спираючись на статті 31, 32, 54 Конституцію України та Закон України „Про захист персональних даних", прийнятий ВР України 16 березня 2006 року.

Висновки

Вже на етапі проектування ІТС, необхідно чітко формулювати вимоги до телекомунікаційної, інформаційної систем з точки зору захисту інформації, виходячи з відомостей про те, яка інформація буде оброблятися в інформаційно-телекомунікаційній системі.

- При створені комплексної системи захисту інформації, особливо в державних органах, більше уваги необхідно приділяти захисту персональної інформації.
- Служба захисту інформації підприємства, установи, організації повинна формувати базу даних відомостей по кожному з етапів для аналізу стану захисту інформації та адекватного впровадження комплексу мір щодо захисту інформаційних ресурсів.

Список літератури

1. Конституція України;
2. Закон України „Про інформацію";
3. Закон України „Про захист персональних даних";
4. Закон України „Про захист інформації в інформаційно-телекомунікаційних системах";
5. Закону України „Про авторське право і суміжні права"
6. Указ Президента Украйни № 891 від 24.09.2001 року „Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних";
7. Порядок підключення до глобальних мереж передачі даних, затверджений постановою Кабінету Міністрів України від 12 квітня 2002 р. N 522;
8. Концепція легалізації програмного забезпечення та боротьби з нелегальним його використанням, затверджена розпорядженням Кабінету Міністрів України від 15 травня 2002 р. N 247-р;
9. Положення про Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління, затверджене постановою Кабінету Міністрів України від 3 серпня 2005 року № 688;
10. Порядок формування й користування інформаційним фондом Реєстру інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління, затверджений наказом ДСТСЗІ СБ України від 20.01.2006 № 9;
11. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою КМУ від 29 березня 2006 року № 373;
12. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі, затверджений наказом ДСТСЗІ СБ України від 4 грудня 2000 р. № 53;
13. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі, затверджений наказом ДСТСЗІ СБ України від 8 листопаду 2005 року № 125;
14. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 28 квітня 1999 р. № 22.

Надійшла 25.09.2006