Захист інформації

УДК 004.056.53

А.Л. Волошин

Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут», Київ

МЕТОД МОДЕРНІЗАЦІЇ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ БЕЗ ПОТРЕБИ ДОДАТКОВОЇ ЕКСПЕРТИЗИ В СФЕРІ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

В статті розглядаються питання модернізації комплексних систем захисту інформації в автоматизованих системах. Аналізуються вимоги нормативних документів системи технічного захисту інформації з питань проведення модернізації, розглядаються основні види оновлення апаратного та програмного забезпечення автоматизованих систем. На підставі проведеного аналізу пропонується новий підхід до розробки нормативно-розпорядчої документації, який дозволяє вносити зміни до складу автоматизованої системи та не потребує проведення додаткової державної експертизи її комплексної системи захисту інформації в сфері технічного захисту інформації.

Ключові слова: *технічний захист інформації, автоматизована система, комплексна система захисту інформації, модернізація.*

Вступ

На цей час на виконання вимог законодавства України з питань захисту інформації [1, 2] в автоматизованих (інформаційних, телекомунікаційних та інформаційно-телекомунікаційних) системах державних органів, комерційних установ та організацій України активно створюються комплексні системи захисту інформації (КСЗІ). Ці системи являють собою сукупність організаційних заходів та технічних засобів, спрямованих на забезпечення захисту інформації з обмеженим доступом (в тому числі, службової інформації з грифом «Для службового користування» та інформації, що становить державну таємницю), яка обробляється, зберігається та передається в автоматизованих системах, від загроз несанкціонованого доступу до неї [2, 3].

Відповідно до нормативно-правових актів у сфері захисту інформації [1, 2] створені КСЗІ в обов'язковому порядку повинні пройти процедуру державної експертизи в сфері технічного захисту інформації (далі – експертиза), за результатами якої отримати атестат відповідності, який підтверджує здатність КСЗІ забезпечити належний рівень захисту інформації в певній автоматизованій системі. Згідно прийнятої практики атестат відповідності, зазвичай, має термін п'ять років, а експертний висновок (який є невід'ємною частиною такого атестату) фіксує склад комплексної системи захисту інформації, зокрема, комплексу засобів захисту від несанкціонованого доступу (далі – КЗЗ), який використовується в КСЗІ з метою захисту інформації.

Різні за призначенням автоматизовані системи висувають різні вимоги до можливості оновлення або зміни власного програмного або апаратного забезпечення. Так, локалізовані обчислювальні комплекси, побудовані на базі однієї ЕОМ (системи класу «1» згідно [4]), як правило, не передбачають необхідності внесення змін у програмне або апаратне забезпечення (крім випадків виходу з ладу відповідного обладнання). Тому ймовірність змін складу автоматизованої системи протягом дії атестату відповідності незначна. В той же час важко уявити розподілену багатокомп'ютерну систему, яка обслуговує територіально розгалужену установу із значною кількістю користувачів, серверів застосувань, локальних та віддалених робочих місць (системи класу «2» або «3» [4]). Для забезпечення безперебійного та якісного виконання покладених на установу – власника системи – функціональних завдань, необхідним є постійне оновлення такої системи, включення до її складу нового прикладного програмного забезпечення, більш потужних апаратних засобів обробки та зберігання даних. Отримання атестату відповідності (експертного висновку) на таку систему, в якому, наприклад, буде зафіксований (на момент проведення експертизи) склад програмного забезпечення, що використовується для обробки даних, виключає можливість внесення до нього будь-яких змін. Адже при перевірці КСЗІ контролюючими органами протягом дії атестату відповідності відразу будуть виявлені невідповідності між фактичним складом програмного забезпечення системи та відомостями, наведеними в експертному висновку. Нас-

лідком таких дій в переважній більшості випадків є призупинення функціонування модифікованої автоматизованої системи до проведення додаткової експертизи її комплексної системи захисту інформації. Зважаючи на значний час, необхідний для проведення такої експертизи (близько 4 – 6 місяців), потенційні наслідки для організації, існування якої критичним чином залежить від роботи такої системи, можуть бути катастрофічними. Аналогічна проблема стосується типових робочих місць користувачів в організаціях з великим штатом працівників, де нові (однакові за складом) робочі місця користувачів вводяться в дію (наприклад, при прийнятті на роботу нового співробітника) або виводяться з дії (відповідно, при звільненні або переведенні до іншого підрозділу) майже щодня.

В цій статті проведено аналіз чинних нормативних документів системи технічного захисту інформації в частині, що стосується порядку проведення модернізації КСЗІ, та запропоновано підхід до розробки нормативно-розпорядчої документації комплексної системи захисту інформації, який дозволяє вносити (в певному обсязі) зміни до автоматизованої системи, КСЗІ якої має атестат відповідності, без проведення її додаткової експертизи. Застосування наведеного підходу на практиці дозволяє значним чином підвищити гнучкість (а отже, практичну ефективність) сучасних розподілених автоматизованих систем, що використовуються в державних та комерційних установах та організаціях України, із збереженням належного рівня захисту інформації в них.

1. Проблемні питання проведення модернізації комплексної системи захисту інформації

Аналіз сучасних нормативних документів системи технічного захисту інформації в Україні свідчить про відсутність визначення в них єдиного конкретного порядку внесення змін (оновлення, модернізації) КСЗІ, що пройшли експертизу та мають чинний атестат відповідності. Так, переважна більшість з них розглядає модернізацію як цілком природній етап життєвого циклу комплексної системи захисту інформації і автоматизованої системи, в якій вона функціонує, в цілому (див., наприклад, [5, 6]). Відповідальність за проведення модернізації покладається на службу захисту інформації, яка формує відповідні пропозиції, організовує та безпосередньо проводить заходи з оновлення програмного та апаратного забезпечення автоматизованої системи [5]. Об'єктами модернізації, як правило, може бути системне та функціональне програмне забезпечення, засоби захисту інформації та засоби управління КСЗІ, засоби адміністрування та управління обчислювальною системою АС, окремі периферійні пристрої (принтери, накопичувачі та змінні носії інформації тощо), які задіяні для обробки інформації [6].

Технічні заходи з проведення модернізації навіть виділені в окрему функціональну послугу безпеки – «Гаряча заміна (ДЗ)», яка дозволяє гарантувати доступність автоматизованої системи (можливість використання інформації, окремих функцій або системи в цілому) в процесі заміни окремих її компонентів [7]. Зазначена послуга має три рівні, які залежать від повноти реалізації заходів з модернізації: від найнижчого, в якому допускається можливість зупинки роботи системи на період проведення оновлення певних компонентів (рівень ДЗ-1), до найвищого, в якому передбачається можливість заміни будь-якого з компонентів системи без переривання обслуговування (рівень ДЗ-3). Основна мета реалізації даної послуги полягає в тому, що встановлення нової версії системи, відмова або заміна захищеного компонента не призведуть до порушень політики безпеки інформації, що реалізується цією системою.

При цьому слід зазначити, що заходи із зміни складу автоматизованої системи в будь-якому випадку проводяться при відновленні працездатності автоматизованої системи. Так, при виході з ладу певного апаратного забезпечення (блоку живлення, накопичувача на жорстких магнітних дисках (НЖМД), мережевого комутатора тощо) власнику системи необхідно проводити його заміну в найкращому випадку на обладнання того ж виробника, марки та моделі. Тому реалізація послуги з відновлення працездатності «Відновлення після збоїв (ДВ)» ([7]) повинна бути тісно пов'язана та узгоджена з політикою послуги модернізації «ДЗ».

Заходи з модернізації передбачається здійснювати в порядку, аналогічному до порядку первинного створення КСЗІ, за окремим (частковим) технічним завданням або за відповідним доповненням до основного технічного завдання на створення КСЗІ [8]. Проте, зауважимо, важко уявити, що при заміні звичайного НЖМД на певній ЕОМ на більш великий за ємністю власник автоматизованої системи буде здійснювати всі заходи, передбачені для процесу побудови КСЗІ: від обстеження середовищ функціонування та розробки відповідного технічного завдання (або доповнення до нього), до проведення попередніх випробувань та дослідної експлуатації модернізованої таким чином КСЗІ.

Але наведені положення нормативних документів системи технічного захисту інформації носять загальний характер та не визначають конкретного порядку модернізації КСЗІ, тобто не відповідають на головні практичні питання, які виникають при організації її проведення, а саме:

− заміна яких компонентів автоматизованої системи та КСЗІ в її складі потребуватиме проведення додаткової експертизи, а які можливо змінювати без проведення цієї процедури;

− які види модернізації (нарощування структури обчислювальної системи, зміна типового складу технічних засобів, оновлення програмного забезпечення тощо) допускається проводити в автоматизованій системі без проведення додаткової експертизи її КСЗІ;

− як документально оформлюється процедура зміни апаратного та програмного забезпечення автоматизованої системи (які посадові особи надають дозвіл, організовують та проводять заходи з модернізації, роблять відповідні відмітки у супроводжувальній документації).

Відсутність таких чітких, однозначних та практично прийнятних правил можна пояснити значним різноманіттям складу апаратного та програмного забезпечення самих автоматизованих систем, їх топології та архітектури, специфіки функціональних завдань тощо. Дійсно неможливо визначити для будь-якої автоматизованої системи хоча б типовий обсяг змін, які можуть бути внесені її власником без впливу на рівень захисту інформації в ній.

Так, зміни, які можуть бути «безболісно» внесені до однієї системи (наприклад, надання користувачам локальної обчислювальної мережі, що розташована в межах одного будинку та не має підключень до будь-яких інших мереж передачі даних, передавати дані між собою з використанням внутрішнього поштового серверу), можуть призвести до суттєвого зниження рівня захисту в інших (якщо зазначена дія дозволяється в розподілених системах, які мають підключення до мережі Інтернет і, отже, можливість передачі даних за межі таких систем).

Досвід з побудови та проведення державних експертиз в сфері технічного захисту інформації комплексних систем захисту інформації автоматизованих систем, різних за призначенням, складом та функціональними завданнями свідчить про існування наступних проблем, пов'язаних із модернізацією КСЗІ, які пройшли експертизу та мають відповідні атестати відповідності:

1. При створенні КСЗІ автоматизованої системи не передбачена можливість проведення оновлення її апаратного або програмного забезпечення. Насамперед, це відсутність в функціональному профілі захищеності комплексу засобів захисту автоматизованої системи наведеної вище послуги «ДЗ» (наприклад, в стандартних профілях 1.К.х, 1.Ц.х, 2.К.х, 2.Ц.х, 2.КЦ.х тощо згідно [4]), а також невизначеність в нормативно-розпорядчій документації порядку проведення оновлення програмного та апаратного забезпечення автоматизованої системи.

В цьому випадку будь-які зміни в складі такого забезпечення (навіть при заміні обладнання, що вийшло з ладу, на цілком аналогічне – того ж виробника, марки та моделі, але з іншим заводським (серійним) номером) призводять до суттєвих ускладнень при перевірках КСЗІ відповідними контролюючими органами. Так, власнику системи дуже важко довести перевіряючим особам, що відновлення налаштувань обладнання, що відмовило, проведено якісно та не призвело до зниження рівня захисту інформації.

2. При створенні КСЗІ автоматизованої системи можливість оновлення її апаратного або програмного забезпечення передбачена, але порядок проведення таких робіт визначений недостатньо чітко і не дає можливості однозначно встановити обсяг змін, які можуть бути внесені до складу автоматизованої системи без необхідності проведення додаткової експертизи КСЗІ.

В цьому випадку функціональний профіль захищеності комплексу засобів захисту автоматизованої системи містить відповідну послугу «ДЗ», але документовані умови її практичного застосування не визначають, що саме і як саме може бути змінено (оновлено).

3. При створенні КСЗІ в розподілених автоматизованих системах не передбачена можливість введення до складу таких систем типових (локальних або віддалених) робочих місць користувачів. Після проведення експертизи таких КСЗІ власник таких систем може використовувати лише ті робочі місця, які перебували в складі системи на момент проведення експертизи, без будь-якої можливості додавання нових (ідентичних за складом) робочих місць або виключенням робочих місць, потреба в яких відпала.

Негативними наслідками таких підходів є суттєве зниження ефективності застосування автоматизованих систем (щонайменш, через неможливість нарощування їх обчислювальних та накопичувальних потужностей), а також потенційні проблеми з контролюючими органами при проведенні перевірок КСЗІ, які мають відповідні атестати відповідності.

Невипадково при описі наведених ситуацій використано термін «при створенні КСЗІ». Дійсно, специфікація політики модернізації повинна розроблятись ще на етапі побудови комплексної системи захисту інформації та розробленні основних принципів її практичної організаційної та технічної реалізації. Тому рекомендації щодо запобігання зазначеним проблемам орієнтовані на використання саме під час розробки проекту КСЗІ (див. етапи створення КСЗІ згідно [8]). Коректність реалізованих при побудові КСЗІ організаційно-технічних рішень має бути перевірена при проведенні експертизи, а її висновки будуть містити опис допустимих змін в апаратно-програмному забезпеченні автоматизованої системи та порядок їх внесення (рис. 1).

Для систем, які вже побудовані, пройшли відповідну експертизу та мають атестат відповідності, є необхідними впровадження відповідних організаційно-технічних процедур, спрямованих на проведення модернізації, перегляд та доопрацювання нормативно-розпорядчої документації на КСЗІ, а отже, і додаткова експертиза такої КСЗІ з метою визначення коректності реалізації зазначених процедур.

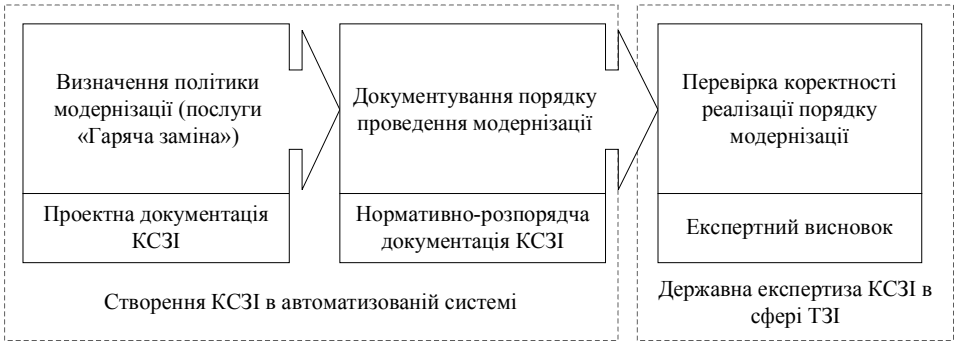

Рис. 1. Загальний порядок визначення та реалізації заходів з модернізації автоматизованої системи та КСЗІ в її складі

Підхід до розробки нормативно-розпорядчої документації, який дозволяє запобігти першій та другій з наведених проблем, розглядається далі. Типове організаційно-технічне рішення із введення в дію (та виведення з дії) типових робочих місць користувачів в розподілених автоматизованих системах та порядок його практичної реалізації через обмеження на обсяг автор планує навести в окремій статті.

Проте, перед тим, як безпосередньо перейти до опису порядку проведення модернізації, необхідно розглянути та охарактеризувати, які види модернізації можуть бути в загальному випадку застосовані до апаратного та програмного обладнання автоматизованої системи. Розгляду цих видів присвячений наступний розділ.

2. Основні види модернізації апаратного та програмного обладнання автоматизованої системи

Основні види модернізації, спрямовані на покращення якості функціонування автоматизованої системи, а отже, і підвищення рівня надання відповідних інформаційних послуг, наведені на рис. 2.

Рис. 2. Основні види модернізації автоматизованої системи

Розглянемо кожний з видів модернізації більш детально:

Нарощування структури обчислювальної системи проводиться шляхом додавання (виключення) до (зі) складу автоматизованої системи окремих компонентів для забезпечення надійного та безперебійного рівня її функціонування у разі збільшення кількості даних, збільшення кількості одночасних підключень користувачів, підключення інших розподілених автоматизованих систем з метою сумісної обробки та передачі даних тощо.

Зміна складу технічних засобів автоматизованої системи включає наступні заходи:

- заміна технічного засобу на повністю ідентичний зразок;
- заміна технічного засобу на аналогічний за функціональним призначенням;
- включення до складу автоматизованої системи додаткових одиниць технічних засобів;
- зміни місця розміщення технічного засобу.

Заміна технічного засобу на повністю ідентичний зразок, але з іншим серійним номером, як правило, здійснюється з дотриманням вимог забезпечення неперервності функціонування (відновлення працездатності) автоматизованої системи у випадках:

- проведення технічного обслуговування технічного засобу у спеціалізованих умовах (тимчасова заміна, на час обслуговування засобу);
- виникнення несправності технічного засобу (тимчасова заміна, на час ремонту засобу);
- неможливості відновлення працездатності несправного технічного засобу;
- відпрацювання встановленого ресурсу (терміну служби) технічного засобу.

Заміна технічного засобу на аналогічний за функціональним призначенням зазвичай проводиться з дотриманням вимог забезпечення неперервності функціонування (відновлення працездатності) автоматизованої системи у випадках:

- неможливості відновлення працездатності несправного технічного засобу (тимчасова заміна, на час ремонту засобу);
- необхідності розширення та (або) покращення експлуатаційних можливостей (характеристик) автоматизованої системи;
- відпрацювання встановленого ресурсу (терміну служби) технічного засобу, зняття технічного

засобу, який підлягає заміні, з виробництва та відсутності запасів або ремонтних фондів.

Включення до складу автоматизованої системи додаткових одиниць ідентичних або аналогічних за функціональним призначенням технічних засобів, як правило, здійснюється у випадках необхідності розширення та (або) покращення її експлуатаційних можливостей (характеристик).

Зміна місця розміщення технічного засобу зазвичай здійснюється у випадку необхідності зміни розміщення автоматизованої системи, пов'язаної з аварійним станом приміщення, де розміщено її компоненти, проведенням ремонтних, будівельно-монтажних робіт у приміщенні тощо.

Підключення до автоматизованої системи інших автоматизованих систем проводиться в разі необхідності сумісної обробки даних з іншими системами (шляхом підключення до інших автоматизованих систем) та збільшення кількості користувачів (шляхом підключення нових локальних або віддалених робочих місць користувачів). Зазвичай підключення інших автоматизованих систем передбачає підвищені вимоги до мережевого обладнання автоматизованої системи, яке при такому підключенні повинно підтримувати швидкісні канали передачі з можливістю нарощування пропускної спроможності каналу до належного рівня.

Оновлення програмного забезпечення автоматизованої системи полягає у виправленні помилок, недоліків та вразливостей програмного забезпечення, що виявлені його розробниками після виходу програмного продукту, а також розширення та (або) поліпшення функціональних характеристик програмного продукту шляхом впровадження таких типів оновлень:

– оновлення – виправлення, що знімає конкретну помилку, яка не є важливою і не відноситься до системи безпеки;

– критичного оновлення – виправлення, що направлене на усунення важливої помилки, яка не відноситься до системи безпеки (механізмів захисту);

– пакету функцій – набору додаткових функцій програмного забезпечення, що розповсюджується окремо від продукту;

– оновлення системи безпеки (механізмів захисту) – виправлень, направлених на усунення уразливості в системі безпеки конкретного продукту;

– пакету оновлення – набору виправлень, оновлень, критичних оновлень і оновлень системи безпеки (механізмів захисту), які формуються за накопичувальним принципом;

– оновлень програмного забезпечення – оновлень, набору оновлення, пакету оновлень, пакету функцій, критичних оновлень, оновлень системи безпеки або виправлень, які призначені для усунення помилки або для поліпшення роботи програмного продукту;

– набору виправлень – накопичувального комплекту оновлень і виправлень, що відноситься до певної області (наприклад, до системи безпеки) програмного продукту і зібраних в один пакет для зручності установки;

– заміна поточної версії продукту новою версією цього ж продукту.

Заміна програмного забезпечення на сумісне за функціональним призначенням, яке має додаткові функціональні можливості, зручний інтерфейс та поліпшену сумісність, і здійснюється з метою поліпшення функціональних характеристик програмного забезпечення у випадках:

– неможливості здійснити поліпшення характеристик наявними засобами;

– припинення виробником супроводження програмного забезпечення;

– необхідності усунення проблем сумісності програмного забезпечення з іншим програмним забезпечення, які виникають внаслідок проведення модернізації технічних засобів автоматизованої системи.

Заміна програмного забезпечення на сумісне за функціональним призначенням здійснюється лише відносно програмного забезпечення, функції (механізми) якого не використовуються у складі КЗЗ автоматизованої системи.

Приклади робіт, які ілюструють практичний зміст наведених видів модернізації, наведені в табл. 1.

Далі наводиться опис порядку проведення зазначених процедур в автоматизованих системах, комплексні системи захисту інформації яких мають чинний атестат відповідності, який не потребує проведення додаткової експертизи.

3. Порядок модернізації апаратного та програмного забезпечення автоматизованих систем

Першочерговою задачею, яку необхідно вирішити при розробці порядку внесення змін до складу автоматизованих систем, є визначення всього апаратного та програмного забезпечення, що входить до складу їх КЗЗ. До складу КЗЗ згідно [9] входить сукупність всіх програмно-апаратних засобів, задіяних під час реалізації політики безпеки.

Визначення складу КЗЗ здійснюється шляхом аналізу функцій, які виконуються кожною складовою компонентою апаратного та програмного забезпечення автоматизованої системи. В разі, якщо відповідний компонент призначений для виконання функцій, спрямованих на забезпечення захисту інформації в системі, та ці функції реально використовуються, робиться висновок про належність зазначеного компоненту до КЗЗ автоматизованої системи.

На етапі розробки проекту КСЗІ до функціонального профілю захисту в обов'язковому порядку включається функціональна послуга «Гаряча заміна (ДЗ)» відповідного рівня (при виборі стандартного функціонального профілю захисту з [4] обирається відповідний профіль, який містить зазначену послугу).

Таблиця 1

Приклади робіт, які ілюструють практичний зміст видів модернізації

Види модернізації	Приклад змісту робіт, які проводяться по відношенню до:		
	засобів збереження даних	комутаційного обладнання	засобів обробки даних
нарощування структури обчислювальної системи	1) встановлення додаткових накопичувачів, їх підключення та налаштування; 2) підключення додаткових інформаційних масивів; 3) додавання нових серверів баз даних та їх подальше налаштування.	1) встановлення додаткових мережевих комутаторів та їх подальше налаштування; 2) об'єднання мережевих комутаторів в мережевий стек.	1) встановлення додаткових серверів та їх подальше налаштування; 2) встановлення додаткових компонентів на існуючих технічних засобах автоматизованої системи (модулів оперативної пам'яті, НЖМД тощо).
зміна складу технічних засобів	1) додавання комутаторів мереж зберігання даних або комутаторів рівня агрегації/доступу з підтримкою Fiber Channel; 2) заміна інформаційних масивів; 3) віртуалізація існуючих серверів.	1) заміна існуючих мережевих комутаторів на нові та їх подальше налаштування.	1) віртуалізація існуючих серверів; 2) об'єднання серверів в серверні платформи (блейд-системи).
підключення до автоматизованої системи інших систем	1) налаштування процесів реплікації даних в базах даних автоматизованих систем, які взаємодіють між собою.	1) встановлення додаткових комутаторів та їх налаштування; 2) підключення нових комутаторів та їх подальше налаштування; 3) встановлення додаткових мережевих плат на мережевому обладнанні.	1) об'єднання серверів в серверні платформи (блейд-системи).
оновлення програмного забезпечення або заміна програмного забезпечення на сумісне	1) оновлення програмного забезпечення: – серверних операційних систем; – систем керування базами даних.	1) оновлення операційних систем на активному мережевому обладнанні.	1) оновлення програмного забезпечення: – серверних операційних систем; – прикладного програмного забезпечення служб керування.

При розробці політики послуги «Гаряча заміна (ДЗ)» оформлюється нормативно-розпорядчий документ (інструкція з модернізації), який, в загальному випадку, визначає (рис. 3):

- підстави для проведення модернізації;
- порядок надання дозволу на проведення модернізації;
- визначає допустимі види (обсяг) модернізації;
- визначає обсяг змін, які можуть бути внесені до складу автоматизованої системи за кожним видом модернізації, які не потребують додаткової експертизи КСЗІ цієї системи;
- визначає порядок проведення зазначених змін (перелік посадових осіб, які вносять зміни та перевіряють коректність їх проведення, вносять відповідні відмітки до супровідної документації);
- визначає порядок перевірки працездатності автоматизованої системи та КСЗІ в її складі після проведення модернізації.

Підставою для проведення модернізації зазвичай є вихід з ладу технічного обладнання (в рамках відновлення працездатності автоматизованої системи), збільшення обсягу даних, які обробляються в системі, збільшення мережевого навантаження та навантаження з обробки даних на серверах системи тощо.

Інструкція з модернізації автоматизованої системи та КСЗІ в її складі
Підстави для проведення модернізації
Порядок надання дозволу на проведення модернізації
Допустимі види (обсяг) модернізації
Обсяг змін, які не потребують додаткової державної експертизи КСЗІ в сфері ТЗІ
Порядок внесення змін до автоматизованої системи
Порядок перевірки працездатності автоматизованої системи та КСЗІ після модернізації

Рис. 3. Схематичний склад типової інструкції з модернізації комплексної системи захисту інформації та автоматизованої системи в цілому

Порядок надання дозволу на проведення модернізації повинен визначати форми службових записок (заяв, замовлень тощо) на проведення модернізації, перелік посадових осіб, які готують, погоджують та затверджують зазначені документи, конкретні дії посадових осіб з підготовки цих документів. Допустимі види модернізації обираються з наведених в попередньому розділі (приклади наведені в табл. 1). За необхідності (за умови наявності відповідного обґрун-

тування) допускається здійснювати інші види модернізації, відмінні від наведених в розділі 2.

Наявний досвід з побудови та експертизи КСЗІ різноманітних автоматизованих систем свідчить про допустимість внесення наступних змін, які не потребують проведення додаткової експертизи відповідної комплексної системи захисту інформації. Так, без необхідності переоформлення чинного атестату відповідності може бути модернізовано (оновлено) таке апаратне та програмне забезпечення автоматизованої системи:

– апаратне забезпечення (крім такого, що входить до складу КЗЗ) – шляхом заміни на аналогічне за функціональністю обладнання з покращеними технічними характеристиками (продуктивність процесору, обсяг запам'ятовуючого пристрою, розподільча здатність, потужність джерел безперебійного живлення тощо);

– апаратне забезпечення (що входить до складу КЗЗ) – шляхом заміни на таке ж саме обладнання (того ж виробника, тієї ж марки, моделі тощо, із відновленням конфігураційних файлів з резервних копій, за умови наявності відповідної документованої процедури відновлення працездатності);

– програмне забезпечення (крім такого, що входить до складу КЗЗ) – шляхом інсталювання такого ж програмного забезпечення нової версії (з виправленими помилками, додатковими функціями тощо);

– антивірусні бази антивірусного програмного забезпечення – шляхом оновлення встановленим порядком штатними засобами антивірусного програмного забезпечення (за умови наявності відповідної документованої процедури управління антивірусним забезпеченням);

– допускається у визначеному порядку застосування додаткового програмного забезпечення, що не містить механізмів захисту, не впливає на рівень захисту інформації в автоматизованій системі, але потрібне для виконання або підвищення ефективності виконання окремих технологічних завдань з обробки інформації в системі.

Порядок проведення модернізації повинен визначати перелік посадових осіб, які вносять зміни та перевіряють коректність їх впровадження, вносять відповідні відмітки до супровідної документації. Про всі зміни в складі апаратного та програмного забезпечення в обов'язковому порядку вносяться відмітки в формуляр (паспорт) автоматизованої системи.

Перевірка працездатності автоматизованої системи та КСЗІ в її складі після проведення модернізації зазвичай проводиться в обсязі програми та методики попередніх випробувань (розробленої при організації проведення попередніх випробувань згідно [10]) в частині перевірки того компоненту системи, до якого було внесені зміни.

Розроблена наведеним чином інструкція з модернізації включається до складу нормативно-розпорядчої документації, яка в обов'язковому порядку перевіряється при проведенні експертизи КСЗІ (див., наприклад, [10, п. А.2.6.3]). При проведенні експертизи перевіряється повнота опису порядку проведення модернізації та достатність контролюючих заходів, спрямованих на перевірку того, що після модернізації не знизився загальний рівень захисту інформації в автоматизованій системі. В разі, якщо експертом виявлено недоліки в описах зазначених процедур (наприклад, недостатня обґрунтованість достатності відповідних перевірок), розробником КСЗІ проводяться заходи із доопрацювання зазначеного документу.

Результатом експертних досліджень зазначеного документу є висновки (в протоколах досліджень та експертному висновку) щодо відповідності реалізованої послуги з модернізації вимогам [7], коректність реалізації заходів з оновлення програмного та апаратного забезпечення автоматизованої системи та достатність заходів з перевірки коректності проведення процедури модернізації. Наявність зазначених висновків в експертному висновку (в розділах «Результати експертних робіт», «Висновки за результатами експертизи» та «Вимоги до умов експлуатації», див. [10, п. Ж.2.6 – Ж.2.8]), виданому за результатами експертизи КСЗІ, є достатньою підставою для власника ІТС проводити модернізацію КСЗІ та автоматизованої системи в цілому (у відповідному обсязі) без необхідності проведення її додаткової експертизи.

На завершення слід наголосити, що розроблений підхід дозволяє вирішити проблеми 1 та 2 (наведені в розділі 1), пов'язані із модернізацією КСЗІ. Для вирішення третьої із зазначених проблем потрібно застосовувати інший підхід (орієнтований на введення в дію (та виведення з дії) типових робочих місць користувачів в розподілених автоматизованих системах. Однак через обмеження на обсяг статті зазначений підхід автор планує викласти окремо.

Висновки

Аналіз чинних нормативних документів системи технічного захисту інформації в частині, що стосується проведення модернізації КСЗІ автоматизованих систем, які пройшли експертизу та мають чинні атестати відповідності, свідчить про відсутність нормативно визначеного порядку проведення оновлення апаратного та програмного забезпечення системи, яке не потребує додаткової експертизи цієї комплексної системи захисту інформації. Це пов'язано, насамперед, із різноманіттям складу апаратного та програмного забезпечення автоматизованих систем, їх топології та архітектури, специфіки функціональних завдань тощо.

На основі досвіду з розробки та експертизи КСЗІ автоматизованих систем різного функціонального призначення автором запропоновано підхід до розробки нормативно-розпорядчої документації

комплексної системи захисту інформації, який дозволяє вносити (в певному обсязі) зміни до автоматизованої системи, КСЗІ якої має атестат відповідності, без проведення її додаткової експертизи. Сутність зазначеного підходу полягає в розробці на етапі створення КСЗІ інструкції з модернізації, яка визначає конкретних відповідальних посадових осіб, обсяг допустимих змін, порядок дій з проведення оновлення та контролю коректності внесених змін.

Застосування наведеного підходу на практиці дозволить підвищити гнучкість (а отже, практичну ефективність) сучасних розподілених автоматизованих систем, що використовуються в державних та комерційних установах та організаціях України, із збереженням належного рівня захисту інформації в них.

Перспективним напрямком подальших досліджень вважається розроблення порядку модернізації не лише апаратного та програмного забезпечення автоматизованої системи, яке не виконує функцій захисту інформації, але й засобів захисту інформації, та водночас не призводить до необхідності додаткової експертизи такої КСЗІ.

Список літератури

1. Закон України «Про захист інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» // Відомості Верховної Ради України. – 1994. – № 31.

2. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою Кабінету Міністрів України від 29.03.2006 № 373 // Офіційний вісник України. – 2006. – № 13.

3. Нормативний документ системи технічного захисту інформації «НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу», затверджений наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

4. Нормативний документ системи технічного захисту інформації «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 28.04.1999 № 22.

5. Нормативний документ системи технічного захисту інформації «НД ТЗІ 1.4-001-2000. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу», затверджений наказом ДСТСЗІ СБ України від 04.12.2000 № 53.

6. Нормативний документ системи технічного захисту інформації «НД ТЗІ 2.5-008-2002. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2», затверджений наказом ДСТСЗІ СБ України від 13.12.2002 № 84.

7. Нормативний документ системи технічного захисту інформації «НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», затверджений наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

8. Нормативний документ системи технічного захисту інформації «НД ТЗІ 3.7-003-2005. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі», затверджений наказом ДСТСЗІ СБ України від 08.11.2005 № 125.

9. Нормативний документ системи технічного захисту інформації «НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу», затверджений наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

10. Нормативний документ системи технічного захисту інформації «НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах», затверджений наказом Адміністрації Держспецзв'язку від 25.03.2011 № 65.

Надійшла до редколегії 12.06.2013

Рецензент: д-р техн. наук Л.В. Ковальчук, Інститут спеціального зв'язку та захисту інформації НТУУ «КПІ», Київ.

МЕТОД МОДЕРНИЗАЦИИ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ БЕЗ ПОТРЕБНОСТИ ДОПОЛНИТЕЛЬНОЙ ЭКСПЕРТИЗЫ В СФЕРЕ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

А.Л. Волошин

В статье рассматриваются вопросы модернизации комплексных систем защиты информации в автоматизированных системах. Анализируются требования нормативных документов системы технической защиты информации по вопросам проведения модернизации, рассматриваются основные виды обновления аппаратного и программного обеспечения автоматизированных систем. На основании проведенного анализа предлагается новый подход к разработке нормативно-распорядительной документации, который позволяет вносить изменения в состав автоматизированной системы и не требует проведения дополнительной государственной экспертизы ее комплексной системы защиты информации в сфере технической защиты информации.

Ключевые слова: *техническая защита информация, автоматизированная система, комплексная система защиты информации, модернизация.*

METHOD OF INFORMATION PROTECTION SUBSYSTEM MODERNIZATION IN AUTOMATED SYSTEM WITHOUT VALIDATION PROCEDURES

A.L. Voloshyn

Information protection subsystem modernization problems in computer system are discussed. The regulatory requirements of the normatives in the information protection sphere are analyzed. The main types of hardware and software upgrades (updates) are considered. Based on such analysis, a new approach to the development of normative documentation is proposed. This approach allows make changes to the structure of the automated system and does not require additional validation of its information protection subsystem.

Keywords: *information protection, automated system, information protection system, modernization.*