УДК 004.056.53

А.Л. Волошин, Г.Я. Криховецький

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

МЕТОД МОДЕРНІЗАЦІЇ КОМПЛЕКСУ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ В СУЧАСНИХ АВТОМАТИЗОВАНИХ СИСТЕМАХ

В статті розглядаються питання модернізації комплексів засобів захисту інформації від несанкціонованого доступу (КЗЗ) сучасних автоматизованих (інформаційних, телекомунікаційних та інформаційно-телекомунікаційних) систем, комплексні системи захисту інформації (КСЗІ) яких пройшли експертизу. Запропоновано загальні правила проведення модернізації КЗЗ, які не потребують проведення додаткової експертизи КСЗІ. Розроблені практичні рекомендації до порядку модернізації КСЗІ та змісту організаційно-розпорядчої документації на неї, які дозволяють реалізувати зазначені правила на практиці при проектуванні, побудові та модернізації комплексних систем захисту інформації автоматизованих систем різного функціонального призначення.

Ключові слова: *технічний захист інформації, автоматизована система, комплекс засобів захисту від несанкціонованого доступу, модернізація.*

Вступ

На виконання вимог законодавства України з питань захисту інформації [1, 2] для забезпечення захисту інформації з обмеженим доступом (в тому числі, службової інформації та інформації, що становить державну таємницю) в автоматизованих (інформаційних, телекомунікаційних та інформаційно-телекомунікаційних) системах державних органів, комерційних установ та організацій України повинні використовуватись комплексні системи захисту інформації (КСЗІ). Ці системи являють собою сукупність організаційних заходів та технічних засобів, спрямованих на забезпечення захисту інформації, яка обробляється, зберігається та передається в автоматизованих системах (АС), 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 АС. Згідно прийнятої практики атестат відповідності має термін п'ять років, а експертний висновок (який є невід'ємною частиною такого атестату) згідно вимог [4]) фіксує склад комплексної системи захисту інформації, зокрема, комплексу засобів захисту від несанкціонованого доступу (далі – КЗЗ), який використовується в складі КСЗІ.

Сучасні вимоги до забезпечення гнучкості, а також безперебійного та якісного функціонування сучасних АС вимагає постійного проведення оновлення її апаратного та програмного забезпечення. Так, зазвичай, необхідним є застосування накопичувачів даних із більшою ємністю, більш потужної обчислювальної платформи, системного та прикладного програмного забезпечення, вимоги до характеристик з обробки та зберігання даних якого постійно підвищуються, тощо. Але фіксування в експертному висновку складу апаратного та програмного забезпечення АС та відсутність в організаційно-розпорядчій документації обгрунтованого порядку модернізації КСЗІ вимагає проведення додаткової експертизи КСЗІ в разі внесення до складу АС будь-яких змін. Зважаючи на значний час, необхідний для проведення такої додаткової експертизи (близько 4 місяців) та необхідність призупинення роботи АС на період проведення експертних випробувань, потенційні наслідки для організації, існування якої критичним чином залежить від роботи такої системи, можуть бути катастрофічними.

Тому розроблення порядку модернізації складу апаратного та програмного забезпечення АС, який не потребує проведення додаткової експертизи КСЗІ, є актуальною науковою задачею. Практична цінність його полягає в зменшенні витрат організації – власника АС, пов'язаних із призупиненням роботи АС та проведення додаткової експертизи її КСЗІ.

В роботах [5, 6] були розглянуті підходи до розробки нормативно-розпорядчої документації комплексної системи захисту інформації, який дозволяє вносити (в певному обсязі) зміни до АС із діючим атестатом відповідності КСЗІ, 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. Проте наведений в [5, 6] обсяг допустимих змін стосується лише апаратного та програмного забезпечення АС, що не входить до складу КЗЗ.

В цій статті запропоновано загальні правила проведення модернізації комплексу засобів захисту інформації від несанкціонованого доступу, які не потребують проведення додаткової експертизи КСЗІ. Зазначені правила забезпечують збереження належного рівня захисту інформації в АС при заміні окремих компонентів КЗЗ. На основі запропонованих правил розроблені практичні рекомендації до порядку модернізації КСЗІ та змісту організаційно-розпорядчої документації на неї, які дозволяють реалізувати зазначені правила на практиці при проектуванні, побудові та модернізації комплексних систем захисту інформації АС різного функціонального призначення.

1. Типовий склад комплексу засобів інформації від несанкціонованого доступу

В загальному випадку до складу комплексу засобів інформації від несанкціонованого доступу КСЗІ можуть входити КЗЗ такого апаратного та програмного забезпечення АС:

- КЗЗ операційної системи;
- КЗЗ прикладного програмного забезпечення;
- КЗЗ антивірусного програмного забезпечення;
- КЗЗ засобів криптографічного захисту інформації;
- КЗЗ комутаційного обладнання.

Наведемо стислу характеристику кожного типу комплексу засобів інформації.

КЗЗ операційної системи зазвичай використовується з метою ідентифікації та автентифікації користувачів, розмежування доступу до конфігураційних параметрів операційної системи (в тому числі обмежити можливість зміни складу програмного забезпечення ЕОМ) та файлів користувачів, а також ведення системних журналів реєстрації подій. Головне призначення цього КЗЗ – забезпечити коректний вхід користувачів до технічних засобів АС та безпечне функціонування іншого програмного забезпечення.

Основною метою використання *КЗЗ прикладного програмного забезпечення* є розмежування доступу користувачів до спеціалізованих інформаційних об'єктів баз даних прикладних інформаційних систем, що використовуються в АС, а також реєстрацію подій, пов'язаних із доступом до цих об'єктів. КЗЗ прикладного програмного забезпечення може містити власні засоби ідентифікації та автентифікації користувачів, а може використовувати ідентифікатор поточного зареєстрованого користувача в операційній системі. В нескладних за своєю архітектурою АС, де немає потреби розмежування доступу користувачів до наведених спеціалізованих інформаційних об'єктів, КЗЗ прикладного програмного забезпечення може не використовуватись.

КЗЗ антивірусного програмного забезпечення забезпечує цілісність виконуємих файлів системного та прикладного програмного забезпечення. Деякі антивірусні продукти надають можливість доступу до власних конфігураційних даних лише попередньо автентифікованому адміністратору, в інших така можливість надається користувачу, обліковий запис якого входить до групи адміністративних користувачів операційної системи.

КЗЗ засобів криптографічного захисту інформації використовується з метою забезпечення захисту конфіденційності, цілісності та підтвердження автентичності інформації, що передається каналами зв'язку між розподіленими компонентами АС через незахищене середовище, а також взаємної автентифікації цих компонент.

КЗЗ комутаційного обладнання призначений для розмежування інформаційних мережевих потоків всередині обчислювальної мережі АС та захисту мережевих ресурсів від інформаційних атак з боку телекомунікаційних мереж загального користування.

2. Основні поняття та позначення

Позначимо через $\Ï \in \{\hat{O}\Ï\ \acute{A}_{\ddot{e}}\text{-}n_i\}$ – функціональний профіль захищеності, який реалізується певним КЗЗ, що використовується при побудові КСЗІ в АС, $i \in \overline{1,22}$. Під позначенням «$\hat{O}\Ï\ \acute{A}_{\ddot{e}}\text{-}n_i$», $i \in \overline{1,22}$, розуміється певна функціональна послуга безпеки, набір яких визначений в НД ТЗІ 2.5-004-99. Зазначимо, що $ФПБ_i \in$ {КД, КА, КО, КК, КВ, ЦД, ЦА, ЦО, ЦВ, ДР, ДС, ДЗ, ДВ, НР, НИ, НК, НО, НЦ, НТ, НВ, НА, НП}, а $n_i \in \overline{1,n_{MAX}}$, де n_{MAX} – максимальний рівень відповідної функціональної послуги безпеки (див. НД ТЗІ 2.5-004-99), $i \in \overline{1,22}$.

Згідно положень попереднього розділу при побудові КСЗІ можуть використовуватись декілька, в загальному випадку, незалежних КЗЗ різних типів. Зауважимо, що загальний профіль, що реалізується КЗЗ КСЗІ, буде являти собою результат логічного поєднання (додавання) профілів використаних КЗЗ:

$$\Ï_{\hat{E}\tilde{N}\c{C}^{2}} = \bigcup_{j=1}^{m} \Ï_{j},$$

де m – кількість використаних типів комплексів засобів захисту від несанкціонованого доступу.

Позначимо через $\Ï^{O} \in \{\hat{O}\Ï\ \acute{A}_i^{O}\text{-}n^{O}\}$ – функціональний профіль захищеності, який реалізується певним КЗЗ, що використаний під час створення КСЗІ, а також перевірений в рамках попередніх випробувань та експертизи (*базовим КЗЗ*), через

$П^{М} \in \{ОП\ А_i^{M}\text{-}n^{M}\}$ – функціональний профіль захищеності, який реалізується *модернізованим КЗЗ*.

При побудові КСЗІ можуть використовуватись як комплекси засобів захисту інформації від несанкціонованого доступу, що пройшли експертизу та мають відповідні експертні висновки (*оцінені КЗЗ*), так і КЗЗ, що не пройшли відповідне оцінювання (*неоцінені КЗЗ*).

В разі використання оціненого КЗЗ програма та методика попередніх випробувань КСЗІ може передбачати лише заходи з перевірки його ідентифікації та перевірки налаштувань. Перевірку коректності реалізації всіх функціональних послуг безпеки та гарантій коректності їх реалізації потрібно проводити лише у випадку використання при побудові КСЗІ неоціненого КЗЗ. Повнота та достатність перевірок, наведених в програмі та методиці попередніх випробувань оцінюється під час проведення експертизи КСЗІ. В разі отримання позитивних результатів ця програма та методика попередніх випробувань може бути в подальшому використана для перевірки модернізованого КЗЗ встановленим вимогам.

Наведена система позначень дозволяє формальним чином здійснювати порівняння між собою функціональних профілів захищеності різних КЗЗ, а отже, визначати умови для проведення тих або інших заходів із перевірки коректності функціонування комплексів засобів захисту інформації від несанкціонованого доступу при проведенні модернізації КСЗІ. Розглянемо правила проведення модернізації КЗЗ, які є загальними для комплексів засобів захисту будь-якого типу.

3. Загальні правила проведення модернізації КЗЗ

Комплекс засобів захисту інформації від несанкціонованого доступу сучасних АС забезпечує захист конфіденційності, цілісності та доступності інформації, що зберігається, передається та обробляється в цих системах. Вимоги до КЗЗ формуються за результатами аналізу актуальних загроз для інформації, що циркулює в АС [7], та наводяться в технічному завданні на створення відповідної КСЗІ [8]. Відповідність базового КЗЗ вимогам технічного завдання перевіряється в рамках експертизи КСЗІ, про що зазначається в експертному висновку, який видається за її результатами. При проведенні модернізації передбачається, що модернізований КЗЗ також повинен забезпечувати виконання вимог зазначеного технічного завдання. В іншому випадку, в АС створюються передумови для витоку інформації за рахунок реалізації загроз, протидія до яких (порівняно із базовим КЗЗ) не забезпечується модернізованим КЗЗ. Наступні правила розроблені на основі аналізу можливих шляхів зміни складу апаратного та програмного забезпечення АС, досліджених в [5] з урахуванням недопустимості зниження рівня захисту інформації, що підлягає захисту в інформаційно-телекомунікаційних системах, та забезпечення доведення факту збереження властивостей модернізованого КЗЗ із захисту інформації після проведення модернізації. Зауважимо, що дотримання наведених правил не потребує проведення додаткової експертизи КСЗІ із модернізованим КЗЗ.

1. Замість КЗЗ певного типу при модернізації повинен бути застосований лише КЗЗ того ж самого типу.

Кожний тип комплексу засобів інформації, що застосовується при побудові КСЗІ, орієнтований на вирішення окремих, в загальному випадку, незалежних завдань із захисту інформації в АС (див., наприклад, основні завдання окремих типів КЗЗ в попередньому розділі). Застосування замість КЗЗ певного типу КЗЗ іншого типу призведе до неможливості ефективного вирішення завдань із захисту інформації, які були покладені на нього. Так, наприклад, замість КЗЗ прикладного програмного забезпечення може бути застосовано лише інше прикладне програмне забезпечення (з аналогічними або відмінними функціями захисту інформації), використання з цією метою засобів операційної системи недопустиме. А відсутність принципової можливості взаємозамінності певних КЗЗ взагалі призведе до неможливості забезпечення захисту окремих інформаційних об’єктів в АС.

2. Набір функціональних послуг безпеки в профілі модернізованого КЗЗ $П^{М}$ повинен містити, щонайменш, всі функціональні послуги безпеки базового профілю $П^{О}$: $П^{О} \subseteq П^{М}$.

Використання модернізованого КЗЗ з меншим набором функціональних послуг безпеки ніж реалізує базовий КЗЗ, створить передумови для порушення безпеки інформації в АС. Так, набір функціональних послуг безпеки в базовому КЗЗ формується за результатами аналізу можливих загроз інформації в АС шляхом вибору рішень з протидії всім виявленим загрозам (див., наприклад, [9]). Тому відсутність в профілі модернізованого КЗЗ хоча б одної послуги, що була присутня в профілі базового КЗЗ, означатиме відсутність заходів з протидії певній актуальній загрозі.

3. Для кожної функціональної послуги безпеки модернізованого КЗЗ $ОП\ А_i^{M} \in П^{І}$ повинна виконуватись умова $n_i^{M} \geq n_i^{O}$, $i \subseteq \overline{1,22}$.

Фактично, це правило означає, що функціональні послуги безпеки, які реалізуються модернізованим КЗЗ, повинні мати рівень реалізації не нижче за рівень реалізації відповідної послуги базового КЗЗ. Аналогічно до попереднього правила, зниження рівня реалізації послуги в модернізованому КЗЗ озна-

чатиме відсутність заходів з протидії певній актуальній загрозі безпеки інформації в АС.

4. Функціональні послуги безпеки $\hat{O}\ddot{I}\ \acute{A}_i^{M} \in \ddot{I}^{\grave{I}}$, що реалізуються модернізованим КЗЗ, повинні стосуватись тих самих інформаційних об'єктів та користувачів, на які розповсюджуються відповідні послуги $\hat{O}\ddot{I}\ \acute{A}_i^{O} \in \ddot{I}^{O}$, реалізовані в базовому КЗЗ, $i \subseteq \overline{1,22}$.

При оформленні технічного завдання на КСЗІ специфікаціями відповідних функціональних послуг безпеки передбачається визначення відповідної політики їх реалізації [8], тобто уточнення інформаційних об'єктів, користувачів, на яких вони поширюються, а також умов та особливостей їх застосування. Тому при модернізації КЗЗ необхідно однозначним чином пересвідчитись, що функціональні послуги безпеки модернізованого КЗЗ мають таку ж саму політику реалізації, що й відповідні послуги базового КЗЗ. В іншому випадку, модернізований КЗЗ не буде відповідати вимогам технічного завдання на створення КСЗІ та, відповідно до цього, не забезпечить необхідний рівень захисту інформації в АС.

5. Рівень гарантій реалізації функціональних послуг безпеки модернізованого КЗЗ повинен бути не нижчим за рівень гарантій базового КЗЗ.

Рівень гарантій реалізації функціональних послуг безпеки безпосередньо визначає надійність реалізації тієї або іншої послуги в КЗЗ. Більший рівень гарантій свідчить про більш високу надійність функціонування відповідного механізму захисту. Тому застосування засобів захисту інформації в модернізованому КЗЗ із меншим рівнем за рівень гарантій реалізації відповідних послуг в базовому КЗЗ призведе до погіршення надійності функціонування механізмів захисту в АС та, як наслідок, до зниження захисту інформаційних ресурсів АС в цілому.

6. Програма та методика попередніх випробувань передбачає перевірку функціональних послуг безпеки як для оцінених, так і для неоцінених КЗЗ.

Визначення та наведення в програмі та методиці попередніх випробувань методів перевірки як оцінених, так і неоцінених КЗЗ робить можливим її застосування при перевірці відповідності модернізованого КЗЗ вимогам технічного завдання на створення КСЗІ та здатності цього комплексу засобів захисту забезпечити потрібний рівень захисту інформації в АС. Повнота та достатність наведених методів перевірки оцінюється в рамках експертизи КСЗІ, а в експертному висновку фіксується вимога щодо обов'язкової перевірки модернізованого КЗЗ в обсязі методів, наведених в програмі та методики попередніх випробувань.

Наведені загальні правила модернізації КЗЗ стосуються всіх типів комплексів засобів захисту інформації від несанкціонованого доступу, застосованих при побудові КСЗІ (див. розділ 1). На основі цих загальних правил можуть бути розроблені окремі часткові правила модернізації КЗЗ певного типу з урахуванням їх специфіки та особливостей умов практичного застосування з метою забезпечення захисту інформації. Розробка таких часткових правил модернізації кожного типу КЗЗ є окремою науковою задачею та становить напрямок подальших досліджень в цій галузі.

4. Рекомендації щодо змісту нормативно-розпорядчої документації в частині модернізації КЗЗ

За результатами аналізу запропонованих правил модернізації КЗЗ можливо запропонувати наступні рекомендації до розробки нормативно-розпорядчої документації на КСЗІ, які дозволять в подальшому змінювати склад комплексу засобів захисту інформації від несанкціонованого доступу без проведення додаткової експертизи комплексної системи захисту інформації.

1. При розробці проекту КСЗІ доцільно визначити перелік комплексів засобів захисту від несанкціонованого доступу, які можуть бути застосовані в складі комплексної системи захисту інформації в рамках модернізації, обґрунтувати доцільність переходу на використання (міграції) цих КЗЗ та провести аналіз функціональних можливостей цих комплексів та принципову можливість їх використання при модернізації КСЗІ.

На цьому етапі передбачається можливим відбракувати КЗЗ, які не забезпечують захист від наведених в технічному завданні актуальних загроз інформації в АС, не містять відповідних засобів захисту та принципово не можуть бути використані при модернізації КСЗІ. В той же час при проектуванні комплексної системи захисту інформації можливо передбачити можливість поступового переходу на інші версії використаного системного та прикладного програмного забезпечення. Так, при нарощуванні структури обчислювальної системи при збільшенні обсягів даних, що зберігаються та обробляються в АС, доцільно передбачити можливість переходу на систему керування базами даних більш потужної версії (наприклад, з версії Standard Edition на версію Enterprise Edition). Вочевидь, більш потужна версія системи керування базами даних буде підтримувати всі механізми захисту інформації, які реалізовані в її базовій версії. При аналізі функціональних можливостей КЗЗ необхідно керуватись загальними правилами 2 – 5 щодо взаємозамінності різних комплексів засобів захисту інформації одного типу. Наведене стосується КЗЗ всіх типів, наведених в розділі 1.

2. Під час підготовці програми та методики попередніх випробувань передбачити можливість

перевірки функціональних послуг безпеки та гарантій коректності їх реалізації в усіх КЗЗ, досліджених при розробці проекту КСЗІ.

Так, програма та методика попередніх випробувань буде містити не лише перевірки КЗЗ, безпосередньо застосованих при побудові КСЗІ, а й комплексів засобів захисту інформації від несанкціонованого доступу, які за своїми технічними характеристиками можуть бути застосовані при подальшій модернізації КСЗІ. Для неоцінених КЗЗ випробування повинні включати перевірку всіх передбачених в технічному завданні на створення КСЗІ функціональних послуг безпеки та рівня гарантій коректності їх реалізації. Випробування оцінених КЗЗ можуть бути зведені лише до перевірки факту встановлення та відповідності налаштувань комплексу засобів захисту вимогам експлуатаційної документації на нього та проектної документації на КСЗІ.

Наведені особливості програми та методики попередніх випробувань потребують викладення порядку перевірки окремих функціональних послуг безпеки без відношення до конкретного КЗЗ. При викладенні змісту окремих перевірок функціональних послуг безпеки та рівня гарантій коректності їх реалізації доцільно керуватись рекомендаціями [10, 11].

Результат перевірки повинен оформлюватись відповідним протоколом, який містить результати випробувань та висновки про відповідність модернізованого КЗЗ вимогам технічного завдання на створення КСЗІ.

3. При розробці проекту КСЗІ оформлювати нормативно-розпорядчий документ (інструкція з модернізації), який, в загальному випадку, визначає:

- підстави для проведення модернізації;
- порядок надання дозволу на проведення модернізації;
- визначає допустимі види (обсяг) модернізації;
- визначає обсяг змін, які можуть бути внесені до складу АС 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 АС та КСЗІ в її складі після проведення модернізації.

Наведений склад інструкції модернізації є аналогічним до викладеного в [5]. Перевірку працездатності модернізованої АС та КСЗІ в її складі доцільно проводити в обсязі, передбаченому програмою та методикою попередніх випробувань, яка передбачає перевірку не лише базового КЗЗ, а й інших комплексів засобів захисту, які можуть бути використані в складі КСЗІ.

Застосування наведених рекомендацій на практиці при побудові КСЗІ сучасних АС дозволить їх власнику вносити зміни до складу комплексу засобів захисту інформації від несанкціонованого доступу без проведення додаткової експертизи комплексної системи захисту інформації.

Висновки

В цій статті розглянуто питання модернізації комплексу засобів захисту інформації від несанкціонованого доступу сучасних АС, комплексні системи захисту інформації яких пройшли експертизу та мають відповідний атестат відповідності. Запропоновано загальні правила проведення модернізації КЗЗ, які не потребують проведення додаткової експертизи КСЗІ. Зазначені правила забезпечують збереження належного рівня захисту інформації в АС при заміні окремих компонентів КЗЗ. На основі запропонованих правил розроблені практичні рекомендації до порядку модернізації КСЗІ та змісту організаційно-розпорядчої документації на неї, які дозволяють реалізувати зазначені правила на практиці при проектуванні, побудові та модернізації комплексних систем захисту інформації АС різного функціонального призначення.

Подальшим напрямком наукових досліджень в цій галузі уявляється розробка на основі розроблених загальних правил часткових правил модернізації КЗЗ певного типу (розділ 1) з урахуванням їх специфіки та особливостей умов практичного застосування.

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 2.6-001-11. 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.

5. Волошин А.Л. Метод модернізації комплексної системи захисту інформації без потреби додаткової експертизи в сфері технічного захисту інформації / А.Л. Волошин // Системи обробки інформації: збірник наукових праць. – Х.: Харківський університет Повітряних Сил імені Івана Кожедуба, 2013. – Вип. 6 (113). – С. 181 – 188.

6. Волошин А.Л. Керування типовими робочими місцями у великих розподілених інформаційно-телекомунікаційних системах / А.Л. Волошин // Збірник наукових праць Харківського університету Повітряних Сил – Х.: Харківський університет Повітряних Сил імені Івана Кожедуба, 2013. – Вип. 3 (36). – Ст. 98 – 103.

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 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі», затверджений наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

9. 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.

10. Нормативний документ системи технічного захисту інформації «НД ТЗІ 2.7-009-09. Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу», затверджений наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 24.07.2009 № 172.

11. Нормативний документ системи технічного захисту інформації «НД ТЗІ 2.7-010-09. Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу», затверджений наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 24.07.2009 № 172.

Надійшла до редколегії 14.12.2013

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

МЕТОД МОДЕРНИЗАЦИИ КОМПЛЕКСА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В СОВРЕМЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

А.Л. Волошин, Г.Я. Крыховецкий

В статье рассматриваются вопросы модернизации комплексов средств защиты информации от несанкционированного доступа (КСЗ) современных автоматизированных (информационных, телекоммуникационных и информационно-телекоммуникационных) систем, комплексные системы защиты информации (КСЗИ) которых прошли экспертизу. Предложено общие правила проведения модернизации КСЗ, которые не требуют проведения дополнительной экспертизы КСЗИ. Разработаны практические рекомендации к порядку модернизации КСЗИ та содержания организационно-распорядительной документации на нее, которые позволяют реализовать указанные правила на практике при проектировании, построении и модернизации комплексных систем защиты информации автоматизированных систем разного функционального назначения.

Ключевые слова: *техническая защита информация, автоматизированная система, комплекс средств защиты информации от несанкционированного доступа, модернизация.*

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

A.L. Voloshyn, G.Ya. Kryhovetskij

Trusted computing base (TCB) modernization problems in validated automated computer system are discussed. General TCB modernization rules, which do not require additional validation, are proposed. Practical modernization recommendations to implement these rules in practice in the construction and modernization of different functional purpose automated systems are developed.

Keywords: *information protection, automated system, trusted computing base, modernization.*