УДК 004.056.53

А.Л. Волошин

Інститут спеціального зв'язку та захисту інформації НТУ України «КПІ», Київ

КЕРУВАННЯ ТИПОВИМИ РОБОЧИМИ МІСЦЯМИ У ВЕЛИКИХ РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

В статті розглядаються питання модернізації комплексних систем захисту інформації у великих розподілених інформаційно-телекомунікаційних системах, які стосуються зміни складу типових робочих місць користувачів. Пропонується новий підхід до розробки нормативно-розпорядчої документації, який дозволяє включати до складу інформаційно-телекомунікаційної системи нові типові робочі місця та виводити з її складу існуючі. Наведені зміни не потребують проведення додаткової державної експертизи її комплексної системи захисту інформації в сфері технічного захисту інформації.

Ключові слова: *технічний захист інформації, інформаційно-телекомунікаційна система, комплексна система захисту інформації, модернізація.*

Вступ

Відповідно до нормативно-правових актів у сфері захисту інформації [1, 2] для захисту державних інформаційних ресурсів та інформації з обмеженим доступом, що передаються, обробляються або зберігаються в інформаційно-телекомунікаційних системах (ІТС), застосовуються комплексні системи захисту інформації (КСЗІ). Ці системи являють собою сукупність організаційних заходів та технічних засобів, спрямованих на забезпечення захисту інформації, яка циркулює в ІТС, від загроз несанкціонованого доступу до неї [2, 3].

Досвід практичного застосування різноманітних КСЗІ після проходження державної експертизи в сфері технічного захисту інформації (далі – експертиза) свідчить про організаційні проблеми, які виникають при спробах змінити (оновити) програмне та апаратне забезпечення ІТС. Зазвичай, зміна складу програмного та апаратного забезпечення системи за відсутності відповідного нормативного врегулювання (див., наприклад, результати аналізу нормативної бази з питань модернізації КСЗІ, проведеного в [4]) розцінюється державними контролюючими органами як достатня підстава для проведення додаткової експертизи з метою підтвердження, що рівень захисту інформації в ІТС після проведення таких змін не погіршився. Особливого значення ця проблема набуває у великих розподілених ІТС, в яких питання додавання або виключення нових типових робочих місць користувачів виникає практично щодня. Прикладом таких систем можуть бути великі корпоративні мережі обробки даних, розподілені мережі кредитних агентів банківських установ, розташовані в пунктах роздрібної торгівлі тощо.

Огляд основних видів модернізації та відомих проблем, пов'язаних із модернізацією КСЗІ, які пройшли експертизу та мають відповідні атестати відповідності, наведений в [4]. Також в зазначеній статті запропонований підхід до розробки нормативно-розпорядчої документації КСЗІ, який дозволяє вносити зміни до автоматизованої системи, КСЗІ якої має атестат відповідності, без проведення її додаткової експертизи. Водночас через обмеження на обсяг питання введення до складу та виключення зі складу ІТС типових (локальних або віддалених) робочих місць користувачів після проходження експертизи відповідною КСЗІ в статті [4] розглянуто не була.

Ця стаття є безпосереднім продовженням роботи [4] та присвячена вирішенню проблеми введення / виключення до / зі складу ІТС, КСЗІ яких пройшла експертизу, типових робочих місць користувачів. Результатом роботи є підхід до розробки нормативно-розпорядчої документації КСЗІ, 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.

1. Порядок введення до (виведення зі) складу ІТС локальних типових робочих місць користувачів

В загальному випадку до складу ІТС можуть входити як локальні, так і віддалені типові робочі місця користувачів. Локальні робочі місця розташовуються в фізичних межах організації – власника ІТС, віддалені робочі місця розташовуються в приміщеннях інших організацій. Типові локальні робочі місця (ЛРМ) належать організації – власнику ІТС. Типові віддалені робочі місця (ВРМ) належать тим організаціям, в яких вони розташовані. Віддалені робочі місця використовуються для забезпечення надання інформаційно-телекомунікаційною системою інформаційних послуг іншим організаціям, підприємствам та установам. Далі

в цьому розділі наведений опис порядку додавання та виключення локальних типових робочих місць. Аналогічний порядок для віддалених типових робочих місць викладений в наступному розділі.

Аналогічно до порядку, наведеного в [4], процедура забезпечення можливості введення до складу ІТС нових типових ЛРМ полягає в розробці на етапі створення КСЗІ нормативно-розпорядчого документу (інструкції з модернізації), який визначає (рис. 1):

- підстави для введення до (виведення зі) складу ІТС типових ЛРМ;
- порядок надання дозволу на введення до (виведення зі) складу ІТС типових ЛРМ;
- вимоги до складу апаратного та програмного забезпечення типових ЛРМ;
- порядок введення до (виведення зі) складу ІТС типових ЛРМ (перелік посадових осіб, які вводять в дію (виводять з дії) зазначені робочі місця, здійснюють їх налаштування та перевіряють їх коректність, вносять відповідні відмітки до супровідної документації).

Інструкція з модернізації інформаційно-телекомунікаційної системи та КСЗІ в її складі
Підстави для введення до (виведення зі) складу ІТС типових ЛРМ
Порядок надання дозволу на введення до (виведення зі) складу ІТС типових ЛРМ
Вимоги до складу апаратного та програмного забезпечення типових ЛРМ
Порядок введення до (виведення зі) складу ІТС типових ЛРМ

Рис. 1. Схематичний склад типової інструкції з модернізації КСЗІ та ІТС в цілому

Очевидною підставою для введення до складу ІТС нових типових ЛРМ є приймання на роботу нових працівників та виділення для їх роботи відповідних комп'ютерів. Також розгортання нових ЛРМ є необхідним при фізичному переміщенні підрозділів організації до інших приміщень (будівель). Відповідно до наведеного, підставами для виведення з дії таких робочих місць є звільнення (переміщення) працівників.

Надання дозволу на введення в дію або виведення з дії типових ЛРМ зазвичай надається керівником організації (у великих організаціях – керівником структурного підрозділу). Для цього безпосереднім керівником працівника – користувача, для якого потрібно розгортання відповідного робочого місця, готується заявка (службова записка), яка за необхідності узгоджується із службою захисту інформації (системним адміністратором організації) та підрозділами матеріально-технічного забезпечення. В зазначеній заявці за необхідності зазначаються права доступу, які потрібно надати користувачу для виконання функціональних обов'язків з обробки інформації в ІТС. При розгляді керівництвом організації (керівником структурного підрозділу) цієї заявки, на ній робляться відповідні резолюції. Після отримання дозволу підрозділами матеріально-технічного забезпечення проводяться заходи з виділення відповідного мобільного або персонального комп'ютера, а службою захисту інформації (системним адміністратором організації) робляться відповідні системні налаштування (перелік типових заходів наведений нижче). Про проведені заходи зазвичай робляться відповідні відмітки на заявці, які засвідчуються підписами посадових осіб, що їх проводили. В разі наявності в організації діючої системи електронного документообігу зазначена заявка може готуватись в електронному вигляді. Виведення з дії типових ЛРМ здійснюється в аналогічному порядку.

В інструкції з модернізації в обов'язковому порядку передбачається перелік системного та прикладного програмного забезпечення, яке може бути в загальному випадку встановлено на комп'ютер типового ЛРМ. Зазвичай цей перелік розділяється на дві частини. Перша частина визначає програмне забезпечення, яке в обов'язковому порядку встановлюється на комп'ютер (операційна система, антивірусне програмне забезпечення, програмні засоби захисту тощо). Друга частина містить програмне забезпечення, яке може бути встановлено додатково для виконання користувачем покладених обов'язків (пакет офісних програм, спеціалізоване прикладне програмне забезпечення, програмне забезпечення бухгалтерського обліку, переглядачі та редактори графічних та мультимедійних об'єктів тощо). В залежності від функціональних завдань структурних підрозділів організації, для кожного її підрозділу може складатись окремий перелік. При формуванні цього переліку доцільно передбачити можливість використання іншого (ніж включено до переліку) програмного забезпечення. В цьому випадку наводиться опис порядку прийняття рішення про застосування такого програмного забезпечення (порядок дій посадових осіб з формування відповідної заяви, погодження із зацікавленими підрозділами організації, надання дозволу на використання, закупівлі, встановлення (інсталяції), налаштування та перевірки коректності роботи програмного забезпечення).

Додатково в інструкції модернізації зазначаються загальні вимоги до апаратного забезпечення типових ЛРМ. Зазвичай в якості таких вимог наводяться мінімальні вимоги до апаратної платформи, а також визначається можливість використання для розгортання таких робочих місць мобільних комп'ютерів (ноутбуків).

При розгортанні нового типового ЛРМ відповідною посадовою особою (системним адміністратором, адміністратором робочих місць), як правило, здійснюються наступні заходи:

- розгортаються та підключаються до системи електроживлення та комутаційного обладнання відповідні технічні засоби (системний блок, монітор, периферійні пристрої тощо);

- налаштовуються відповідні мережеві параметри робочого місця (IP-адреси, маски мережі, введення до домену (за потреби) тощо);

- встановлюється та налаштовується програмне забезпечення, дозволене до використання в організації, відповідно до експлуатаційної документації на нього;

- перевіряться правильність інсталяції та конфігурування програмного забезпечення та технічних засобів типового ЛРМ;

- створюються облікові записи користувачів та здійснюється налаштування їх прав доступу до об'єктів захисту типового ЛРМ та загальних об'єктів ІТС;

- оформлюється формуляр на типове ЛРМ та вносяться відповідні зміни до формуляру на ІТС.

Все програмне забезпечення та обладнання, що було введено до складу ІТС, підлягає тестуванню та перевірці на працездатність. Перевірка здійснюється згідно експлуатаційної документації на відповідне програмне або апаратне забезпечення. Використовувати програмне або апаратне забезпечення, яке не перевірено встановленим порядком, або проявляє ознаки неправильного функціонування, забороняється.

Перевірка коректності налаштувань та працездатності типового ЛРМ зазвичай проводиться в обсязі, визначеному в програмі та методиці попередніх випробувань (розробленої при організації проведення попередніх випробувань згідно [5]) в частині, що стосується перевірки типових робочих місць.

Розроблена інструкція з модернізації включається до складу нормативно-розпорядчої документації, яка в обов'язковому порядку перевіряється при проведенні експертизи КСЗІ (див., наприклад, [5, 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 ІТС. В разі, якщо експертом виявлено недоліки в описах зазначених процедур (наприклад, недостатня обґрунтованість достатності відповідних перевірок типового ЛРМ), розробником КСЗІ проводяться заходи із доопрацювання зазначеного документу.

2. Порядок введення до (виведення зі) складу ІТС віддалених типових робочих місць користувачів

Порядок введення до (виведення зі) складу ІТС типових ВРМ в цілому відповідає аналогічному порядку для типових КРМ. Далі відзначимо відмінності цього порядку від наведеного в розділі 1.

Надання дозволу на введення в дію або виведення з дії типових ВРМ зазвичай надається керівником організації – власника ІТС за відповідним зверненням організації, в інтересах якої розгортається відповідне робоче місце.

Порядок розгортання типового ВРМ визначається окремою інструкцією (інструкція про порядок введення в дію типових віддалених робочих місць користувачів), яка розробляється на етапі створення КСЗІ, надається організації – власнику типового ВРМ та визначає (рис. 2):

- порядок розгортання та налаштування апаратних засобів;

- порядок встановлення та конфігурування системного та прикладного програмного забезпечення;

- порядок організаційного забезпечення;

- порядок перевірки розгорнутого типового ВРМ.

Інструкція про порядок введення в дію типових віддалених робочих місць користувачів
Порядок розгортання та налаштування апаратних засобів
Порядок встановлення та конфігурування системного та прикладного програмного забезпечення
Порядок організаційного забезпечення
Порядок перевірки розгорнутого типового ВРМ

Рис. 2. Схематичний зміст Інструкції про порядок введення в дію типових ВРМ

Розгортання та розташування апаратних засобів типового ВРМ здійснюється адміністратором організації – власника цих місць з урахуванням вказівок системного адміністратора організації – власника ІТС. За потреби розгортання цих місць здійснюється фахівцями організації – власника ІТС.

Технічні засоби (ЕОМ), на основі яких розгортаються типові ВРМ, повинні бути взяті на облік відповідними господарчими службами організації, в якій вони використовуються. Допускається здійснювати розгортання типових ВРМ як на базі ЕОМ, так і на базі мобільного персонального комп'ютеру (ноутбуку). При цьому повинні виконуватись наведені вище вимоги щодо господарського обліку відповідних технічних засобів. В разі розгортання типових ВРМ на базі мобільного персонального комп'ютеру, цей комп'ютер повинен мати визначене місце фізичного розташування, експлуатація такого комп'ютеру поза межами цього визначеного місця зазвичай не допускається.

На ЕОМ, на якій розміщується типове ВРМ, засобами операційної системи можуть бути обмежені права для персоналу, який на ньому працює:

- по використанню іншого програмного забезпечення, окрім програмного забезпечення, дозволеного до використання на типовому віддаленому робочому місці;

- по зміні установок операційної системи.

Програмне забезпечення ЕОМ, на якій розміщується типове ВРМ, не повинно містити наступних засобів:

- засобів розробки та відлагодження програм;
- засобів, що дозволяють здійснювати несанкціонований доступ до системних ресурсів.

Для ЕОМ, на якій розміщується типове ВРМ, є доцільним вжиття таких заходів:

- по виключенню можливості по входу в режим зміни конфігурації BIOS для всіх користувачів, окрім адміністратора, який обслуговує це робоче місце;
- по забороні (настроюваннями BIOS) завантаження з будь-якого носія, окрім жорсткого диску;
- по демонтажу зовнішніх пристроїв, що не використовуються при роботі типового віддаленого робочого місця користувачів;
- по відключенню через BIOS інтерфейсних з'єднувачів, що не використовуються при роботі типового віддаленого робочого місця користувачів;
- по видаленню програмного забезпечення, що не використовується при роботі типового віддаленого робочого місця користувачів;
- по відключенню інтерфейсів, що використовуються для організації бездротового мережевого зв'язку (Bluetooth, Wi-Fi тощо, для ноутбуків, за наявності таких інтерфейсів), якщо інше не передбачається вказівками системного адміністратора організації – власника ІТС.

При встановленні системного та прикладного програмного забезпечення необхідно керуватись загальними вимогами до встановлення та перевірки працездатності програмного забезпечення, наведеними в експлуатаційній документі на відповідне програмне забезпечення. Перелік програмного забезпечення, дозволеного до використання на типових ВРМ узгоджується з організацією – власником ІТС.

Після встановлення програмного забезпечення необхідно здійснити його налаштування в порядку, визначеному експлуатаційною документацією на нього, а також налаштувати відповідні мережеві параметри типового ВРМ (IP-адреси, маски мережі тощо) відповідно до вказівок системного адміністратора організації – власника ІТС.

Крім зазначених налаштувань встановлюються інші налаштування, передбачені проектною та нормативно-розпорядчою документацією КСЗІ, зокрема, в загальному випадку, встановлюються наступні обмеження на роботу користувачів:

- адміністратору організації – власника типового ВРМ повинен відповідати окремий обліковий запис в операційній системі; обліковий запис цього адміністратора повинен входити до групи користувачів «Адміністратори» операційної системи;
- кожному користувачу типового ВРМ повинен відповідати окремий обліковий запис в операційній системі; всі облікові записи користувачів типового ВРМ повинні входити до групи «Користувачі» операційної системи;
- обліковий запис «Гість» повинен бути заблокований;
- обліковим записам користувачів типового ВРМ повинен бути наданий доступ лише до каталогів та файлів, які містять матеріали, необхідні для виконання посадових обов'язків (прикладне програмне забезпечення, експлуатаційна документація тощо);
- вбудований міжмережевий екран операційної системи повинен бути ввімкнений та налаштований на пропускання інформаційних потоків лише системного та прикладного програмного забезпечення (в тому числі, протоколів електронної пошти та антивірусного програмного забезпечення);

При розгортанні типового ВРМ організацією – власником ІТС виготовляються копії, забезпечується передача та ознайомлення користувачів організації – власника робочого місця щонайменш з наступними матеріалами та експлуатаційними документами:

- інструкція користувачу із безпечного використання типового ВРМ;
- експлуатаційна документація на прикладне програмне забезпечення типового ВРМ;
- форми (шаблони) документів, які обробляються на типовому ВРМ;
- формуляр типового ВРМ;
- інструкція розгортання типового ВРМ;
- акт щодо можливості введення типового ВРМ до експлуатації у складі ІТС;
- інформаційні матеріали (пам'ятки), що визначають:
  - контактну інформацію (посади, прізвища, ім'я, по батькові, телефони, електронні адреси тощо) системного адміністратора організації – власника ІТС;
  - системні налаштування ІТС, необхідні для виконання покладених на користувачів типового ВРМ функціональних завдань (електронні адреси, DNS-адреси, IP-адреси, програмні порти відповідних серверів тощо).

Після розгортання апаратних засобів, встановлення та конфігурування системного та прикладного програмного забезпечення, виготовлення необхідних експлуатаційних документів проводиться перевірка правильності налаштування типового ВРМ. Ця перевірка проводиться відповідно до вимог окремого нормативно-розпорядчого документу (методика перевірки відповідності віддалених робочих місць вимогам до захисту інформації від несанкціонованого доступу). Склад та зміст перевірок типового ВРМ в загальному випадку наведені в табл. 1.

Таблиця 1

Склад та зміст перевірок типового ВРМ

№ з/п	Склад перевірок	Типовий зміст перевірок
1	Перевірка складу апаратного та програмного забезпечення	Перевірка відповідності складу апаратного та програмного забезпечення типового ВРМ вимогам нормативно-розпорядчої документації КСЗІ; ідентифікація програмного забезпечення та перевірка ліцензійних умов його використання.
2	Перевірка об'єктів захисту, суб'єктів доступу та атрибутів доступу	Перевірка відповідності вимогам нормативно-розпорядчої документації КСЗІ: - складу програмно-інформаційних ресурсів; - складу облікових записів користувачів в системному та прикладному забезпеченні; - атрибутів доступу кожного типу інформаційного об'єкту або суб'єкту доступу (користувача, локальних та мережевих об'єктів, локальних та мережевих процесів).
3	Перевірка налаштувань комплексу засобів захисту від несанкціонованого доступу	Перевірка відповідності вимогам нормативно-розпорядчої документації КСЗІ наступних реалізованих процедур: - перевірка налаштувань засобів захисту інформації; - перевірка механізмів ідентифікації та автентифікації користувачів; - перевірка механізмів виділення ролі користувачів з адміністративними правами (адміністратора); - перевірка механізмів розмежування доступу та управління правами користувачів; - перевірка механізмів реєстрації подій.
4	Перевірка антивірусного програмного забезпечення	Перевірка коректності інсталювання та конфігурування антивірусного програмного забезпечення; перевірка працездатності антивірусного програмного забезпечення; перевірка налаштувань оновлення антивірусних баз; перевірка повноважень користувачів щодо управління налаштуваннями антивірусного програмного забезпечення.
5	Перевірка вимог до фізичного середовища	Перевірка режиму доступу до приміщень; перевірка фізичного розташування засобів відображення інформації типового ВРМ.
6	Перевірка вимог до користувачів	Перевірка навичок та кваліфікації користувачів.
7	Перевірка вимог до організаційного забезпечення	Перевірити склад документів, що використовуються для забезпечення діяльності типового ВРМ; перевірка відповідності змісту документації типового ВРМ загальним характеристикам, особливостям та реальним умовам обробки інформації на цьому робочому місці.

Перевірка типового ВРМ проводиться комісією, призначеною керівником організації – власника цього місця, в якій розгорнуто та використовується відповідне робоче місце. До складу комісії обов'язково включаються адміністратор цього місця та щонайменш один, закріплений за ним користувач. За результатами перевірки оформлюється акт щодо можливості введення типового ВРМ в дію. Зазначений акт оформлюється в двох примірниках, підписується всіма особами, які проводили перевірку, і затверджується керівником організації – власника типового ВРМ. Один примірник акту зберігається в цій організації, а другий надсилається системному адміністратору організації – власника ІТС та зберігається у нього.

Інструкція про порядок введення в дію типових ВРМ, методика перевірки відповідності типових ВРМ вимогам до захисту інформації від несанкціонованого доступу та форма акту щодо можливості введення типового ВРМ в дію розробляються на етапі створення КСЗІ, включаються до складу нормативно-розпорядчої документації, зміст та повнота

якої перевіряються при проведенні експертизи КСЗІ. В разі, якщо експертом виявлено недоліки в описах зазначених процедур (наприклад, недостатня обґрунтованість достатності відповідних перевірок типових ВРМ), розробником КСЗІ проводяться заходи із доопрацювання зазначених документів. Крім того, зазначені документи додаються до експертного висновку, який видається за результатами експертизи. В складі зазначеного експертного висновку вони передаються іншим організаціями – споживачам інформаційних послуг ІТС та використовуються для розгортання їх типових ВРМ.

Висновки

В статті розглянуто підхід до модернізації великих розподілених ІТС, КСЗІ яких пройшли експертизу, в частині, що стосується включення або виключення з їх складу типових робочих місць користувачів. Запропонований підхід полягає в розробці та включенні до складу нормативно-розпорядчої документації КСЗІ інструкції з модернізації, яка передбачає заходи з розгортання та налаштування таких робочих місць, а також перевірки коректності їх роботи.

Для типових ЛРМ, які належать організації – власнику ІТС, достатньо наявності однієї такої інструкції. Для типових ВРМ, як мають різних власників, додатково розробляються інструкція про порядок введення в дію типових ВРМ, методика перевірки відповідності типових ВРМ вимогам до захисту інформації від несанкціонованого доступу та форма акту щодо можливості введення типового ВРМ в дію.

Розгортання типових локальних та віддалених робочих місць, введення їх до складу ІТС та виведення з її складу після проходження експертизи КСЗІ цієї системи згідно запропонованого підходу не потребує проведення додаткової експертизи.

Зважаючи на значний час, необхідний для проведення такої експертизи (близько 4 – 6 місяців), застосування наведеного підходу на практиці дозволяє значним чином підвищити гнучкість (а отже, практичну ефективність) сучасних розподілених ІТС, що використовуються в державних та комерційних установах та організаціях України, із збереженням належного рівня захисту інформації в них

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. 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 Харківського університету Повітряних Сил ім. Івана Кожедуба. – Х., 2013. – Вип.. 6 (113).

5. 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 30.08.2013

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

УПРАВЛЕНИЕ ТИПОВЫМИ РАБОЧИМИ МЕСТАМИ В БОЛЬШИХ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

А.Л. Волошин

В статье рассматриваются вопросы модернизации комплексных систем защиты информации в больших распределенных информационно-телекоммуникационных системах, которые касаются изменения состава типовых рабочих мест пользователей. Предлагается новый подход к разработке нормативно-распорядительной документации, который позволяет включать в состав информационно-телекоммуникационной системы новые типовые рабочие места и выводить из ее состава существующие. Указанные изменения не требуют проведения дополнительной государственной экспертизы ее комплексной системы защиты информации в сфере технической защиты информации.

Ключевые слова: *техническая защита информация, информационно-телекоммуникационная система, комплексная система защиты информации, модернизация.*

MANAGING THE TYPICAL WORKSTATIONS IN A LARGE DISTRIBUTED AUTOMATED SYSTEMS

A.L. Voloshyn

Information protection subsystem modernization problems in computer system, related to managing the typical user workstations, are discussed. A new approach to the development of normative documentation is proposed. This approach allows make adding and removing typical user workstations from automated system. Such changes to the structure of the automated system do not require additional validation of its information protection subsystem.

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