УДК 004.056

DOI: 10.18372/2310-5461.36.12230

О. К. Юдін
д-р техн. наук, проф.
Національний авіаційний університет
orcid.org/0000-0001-5098-7796
e-mail: kszi@ukr.net;

М. А. Стрельбіцький
канд. техн. наук, доц.
orcid.org/0000-0001-8030-3228
Національна академія ДПС України імені Б. Хмельницького
e-mail: m.strelb@ukr.net

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ НА СТАДІЇ МОДЕРНІЗАЦІЇ

Актуальність дослідження

Аналіз основних напрямів державної політики з питань забезпечення національної безпеки показав, що практично кожний із них залежить від рівня інформатизації суспільства [1]. Держава законодавчо закріпила власні пріоритети в інформаційній сфері, які полягають зокрема у підвищенні рівня координації діяльності правоохоронних органів та впровадженні новітніх технологій в інформаційній сфері [2].

Розвиток інформаційних технологій спричинив створення на державному та відомчих рівнях великої кількості взаємно не пов'язаних інформаційних систем спрямованих здебільшого на накопичення даних та використання їх лише за напрямками діяльності суб'єктів національної безпеки. Практично повна відсутність стандартизації підходів до розробки та функціонування систем збору, обробки, аналізу, висвітлення, а саме головне ефективного обміну інформацією між суб'єктами забезпечення національної безпеки, а також технологічна комерціалізація цього напрямку досліджень є передумовою для уповільнення розвитку загальнодержавних систем моніторингу обстановки та підтримки прийняття управлінських рішень.

Аналіз досліджень та публікацій

Значний внесок у розвиток інформаційних технологій створення гарантоздатних автоматизованих систем управління критичного застосування та дослідження моделей і методів забезпечення функціональної безпеки та надійності інформації внесли відомі вчені Бараннік В. В., Богуш В. М., Герасименко В. А., Грицюк Ю. І., Грушо А. А., Дудикевич В. Б., Катеринчук І. С., Корнієнко Б. Я., Конахович Г. Ф., Ліпаєв В. В., Литвиненко О. Є., Мачалін І. О., Потій О. В., Скляр В. В., Харченко В. С., Шеннон К., Юдін О. К. та ін.

Проведений аналіз існуючих підходів до забезпечення функціональної безпеки інформаційних систем показав достатньо глибоке опрацювання досліджень окремо за кожною інформаційною системою. Однак залишаються невивченими особливості взаємодії зазначених систем, зокрема при модернізації окремих інформаційних систем з погляду забезпечення функціональної безпеки загалом.

Інтегрована інформаційна система ДПСУ, як суб'єкта національної безпеки, має велику кількість підсистем які розподілені на всій території держави. Особливістю такої системи є вимога функціонування в реальному масштабі часу та оперування критичним для прийняття рішень інформаційним ресурсом, при чому, навіть незначне порушення надійності якого може призвести до серйозних збитків національного масштабу.

При такому розумінні інформаційного ресурсу прикордонного відомства виникає потреба у забезпеченні складових його функціональних критеріїв: цілісності, доступності, конфіденційності та спостереженості, тобто забезпечення функціональної безпеки інтегрованої інформаційної системи прикордонного відомства в цілому [3].

Аналіз такого типу систем показав з одного боку сталу тенденцію до зростання множини інформаційних дестабілізуючих факторів які впливають на функціональну безпеку, що спричинено:

– розширенням умов застосування та функціонування;
– збільшенням кола користувачів системи;
– зростанням кількості складових інтегрованої інформаційної системи;
– потребою у взаємодії з міжвідомчими та міжнародними інформаційними ресурсами;
– збільшенням обсягів інформації;

© Юдін О. К., Стрельбіцький М. А., 2017

– збільшенням кількості дестабілізуючих інформаційних впливів;

– запровадженням нових інформаційних технологій.

З іншого боку, захист життєво важливих інтересів держави потребує від таких систем:

- забезпечення підвищених вимог до надійності інформації;
- оперативності доступу до інформаційних ресурсів;
- реалізації розширених можливостей щодо аналізу та узагальнення інформації;
- скорочення часу для прийняття рішень;
- контроль за виконанням розпоряджень.

Вищезазначене потребує постійної модернізації відомчих систем, що призводить до спільного функціонування на загальному полі даних старих, модернізованих та нових версій інформаційних систем, як складових суперсистеми. Це призводить до виникнення протиріччя між наявною теоретичною базою забезпечення функціональної безпеки та потребою у постійній модернізації інформаційних систем у складі інтегрованої інформаційної системи.

Таким чином, на цій стадії життєвого циклу виникає проблема переходу на нову програмно-апаратну платформу без порушення життєвого циклу, при цьому для відомчих інформаційних систем одною з найважливіших задач є забезпечення функціональної безпеки інформаційних систем, що і визначає актуальність дослідження.

Метою статті є розробка технології забезпечення функціональної безпеки інтегрованої інформаційної системи Держприкордонслужби на стадії модернізації.

Виклад основного матеріалу

Технології обробки даних залежать від цільового призначення інформаційних систем, наявних апаратних і програмних засобів та режимів роботи. Введення до складу інформаційних систем (ІС) нових апаратних засобів, спеціального програмного забезпечення може бути здійснено тільки за умови узгодження їх спільного функціонування на загальному полі даних із існуючим програмно-апаратним забезпеченням.

При сполученні існуючої ІС із більш досконалими засобами обчислювальної техніки і спеціальним програмним забезпеченням розпорядника інформаційної системи необхідно чітко визначити величину допустимих витрат, необхідну захищеність даних, аспекти сумісності. Важливим аргументом на користь тієї чи іншої версії може бути: розроблене спеціальне програмне забезпечення, що є розвитком уже відпрацьованих функціональних завдань; існуюча функціональна безпека для цієї платформи.

Таким чином, першочерговим етапом технології забезпечення функціональної безпеки інформаційних систем на стадії модернізації є визначення розпорядником ІС базових засад, а саме:

– стратегія функціональної безпеки;

– завдання на модернізацію конкретних ІС;

– критерії ефективності щодо кожної складової узгодження;

– умов функціонування модернізованих ІС.

Загальна структура технології забезпечення функціональної безпеки інформаційних систем на стадії модернізації наведена на рисунку.

Обґрунтування стратегій модернізації здійснюється за наступними групами критеріїв: рівня функціональної безпеки, особливостей функціонування ІС.

Формуванню першої групи критеріїв присвячена значна кількість робіт, у яких дослідники обґрунтовують його фізичний сенс.

У більшості досліджень, зокрема у працях [4; 5], у якості показника рівня функціональної безпеки пропонується використовувати ймовірність попередження шкоди, враховуючи стохастичну природу дестабілізуючих впливів.

На наш погляд, найбільш доцільними є розподіл даної групи критеріїв на три складові критеріїв рівня забезпечення функціональної безпеки:

- нормативний — критерій, за якого поточне значення ймовірностей порушення функціональної безпеки не перевищуватиме заданого;
- середній — критерій, за якого середнє значення ймовірностей порушення функціональної безпеки не перевищуватиме заданого;
- зважений — критерій, за якого середнє зважене значення ймовірностей порушення функціональної безпеки не перевищуватиме заданого;

Друга група критеріїв, яка визначає особливості функціонування ІС на стадії модернізації характеризує можливості щодо втручання в процес роботи системи (див. рисунок).

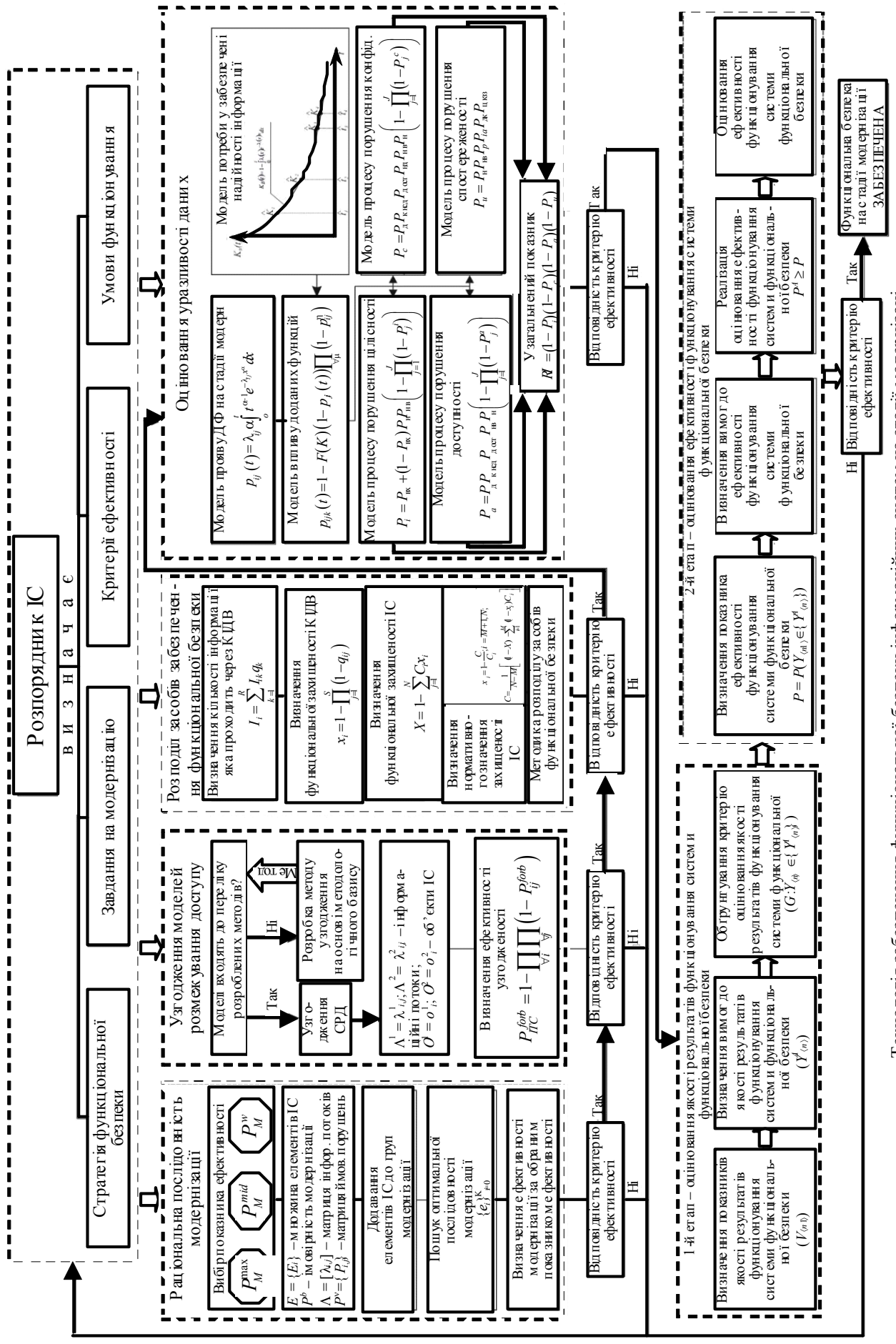
За даною групою критерії поділяються на три види:

1) системи реального часу характеризуються практичною відсутністю будь-яких можливостей щодо втручання в процес їх функціонування. Зупинка такої системи навіть на невеликий термін недопустима, оскільки може призвести до збитків національного масштабу;

2) системи з можливістю часткової зупинки характеризуються більшими можливостями для процесу модернізації;

3) системи з можливістю повної зупинки характеризуються максимальними можливостями для процесу модернізації. Такого типу системи мають обмеження тільки терміном експлуатації.

© Юдін О. К., Стрельбіцький М. А., 2017



Технологія забезпечення функціональної безпеки інформаційних систем на стадії модернізації

© Юдін О. К., Стрельбіцький М. А., 2017

Вищенаведене дозволяє сформувати узагальнену таблицю раціональних стратегій модернізації, як декартового добутку обох критеріїв (див. таблицю).

Раціональні стратегії модернізації

Критерій рівня забезпечення функціональної безпеки	Особливості функціонування ІС		
	реального часу	часткова зупинка	повна зупинка
Нормативний	+	–	–
Середній	–	+	–
Зважений	–	+	–

Таким чином, нормативний рівень варто застосовувати до систем реального часу з причини забезпечення не перевищення значення ймовірностей порушення функціональної безпеки протягом усього терміну модернізації.

Середній та зважений критерії захисту доцільно використовувати при модернізації систем з можливістю часткової зупинки функціонування. Вибір критерію залежить від величин часу та періодичності часткової зупини системи.

На другому етапі технології, залежно від визначених на попередньому етапі засад здійснюються заходи узгодження різних версій спеціального програмного забезпечення та апаратних засобів забезпечення функціональної безпеки. Особливістю даного етапу є можливість паралельного їх проведення. Таким чином, ґрунтуючись на стратегії функціональної безпеки, завдання на модернізацію та умов функціонування обирається показник ефективності процесу модернізації. Відповідно до розробленого методу визначається раціональна послідовність модернізації та здійснюється оцінювання її ефективності за обраним показником. Відповідність показника обраному критерію ефективності свідчить про успішне виконання частини другого етапу. В іншому випадку пропонується розпоряднику ІС змінити базові засади з причини неможливості їх дотримання.

Разом із тим здійснюється узгодження моделей розмежування доступу модернізованих ІС. У випадку відсутності розроблених методів узгодження моделей розмежування доступу на основі сформованого методологічного базису провадиться розробка необхідного методу. Після узгодження СРД проводиться оцінювання ефективності цього процесу. При невідповідності показника ефективності пропонується розпоряднику змінити умови функціонування ІС, завдання на модернізацію або сам критерій ефективності.

Третьою складовою етапу є розподіл засобів забезпечення функціональної безпеки ІС. Провадиться за потреби їх розподіл та оцінюється загальна функціональна безпека системи. У випадку відповідності всіх розглянутих показників ефективності критеріям здійснюється перехід до третього етапу технології — оцінювання уразливості даних.

На третьому етапі, ґрунтуючись на визначених базових засадах визначається вплив дестабілізуючих факторів, які викликані стадією модернізації на складові функціональних критеріїв: цілісності, доступності, конфіденційності та спостереженості. Моделювання зазначених процесів дозволяє провести оцінювання уразливості даних викликаних стадією модернізації. При відповідності узагальненого показника визначеному розпорядником ІС критерію здійснюється перехід до четвертого етапу технології — оцінювання ефективності системи функціональної безпеки.

На четверному етапі здійснюються оцінювання ефективності функціонування системи функціональної безпеки. Результатом зазначеного етапу є значення ймовірності виконання системою функціональних завдань. При умові дотримання значення цієї ймовірності в визначених розпорядником ІС межах функціональну безпеку на стадії модернізації забезпечено. В іншому випадку, пропонується змінити умови функціонування системи або критерії оцінювання.

З метою визначення якісного ступеня впливу факту порушення властивостей інформації на загальний рівень функціональної безпеки інформаційної системи наведемо графік різниці двох складових. Позитивне значення свідчить про перевагу першого параметру, негативне — другого (рис. 2, 3). Аналіз різниці ймовірностей порушення функціональної безпеки за параметрами цілісності та конфіденційності показав, що на початку модернізації більший вплив на рівень функціональної безпеки ІС має складова цілісності, разом із тим, при збільшенні нормативного часу кожного із них характерна різка зміна ступеня впливу конфіденційності (стрибок площини у межах восьми годин модернізації). Причому, така зміна властива незалежно від нормативного значення цілісності. Таким чином, аналіз впливу нормативних значень властивостей інформації при дослідженні ймовірностей порушення функціонування системи функціональної безпеки показав загальну тенденцію до зростання при зростанні нормативних значень. Зазначена тенденція є прогнозованою з причини збільшення часу дотримання кожної властивості інформації. Разом із тим, аналіз динаміки впливу окремих властивостей на результуючу функцію показав наявність стрибка зміни впливу окремих параметрів, при чому для різних параметрів у межах одного і того самого значення.

© Юдін О. К., Стрельбіцький М. А., 2017

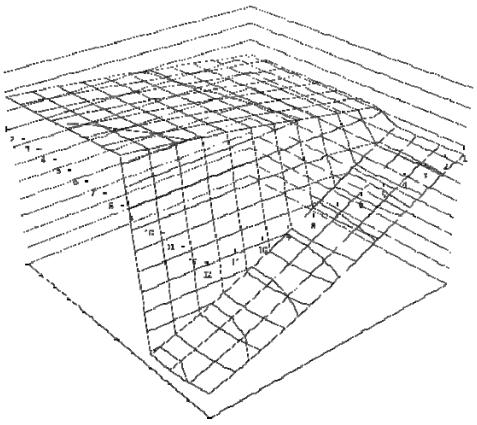


Рис. 2. Різниця ймовірностей порушення функціональної безпеки за параметрами цілісності та конфіденційності

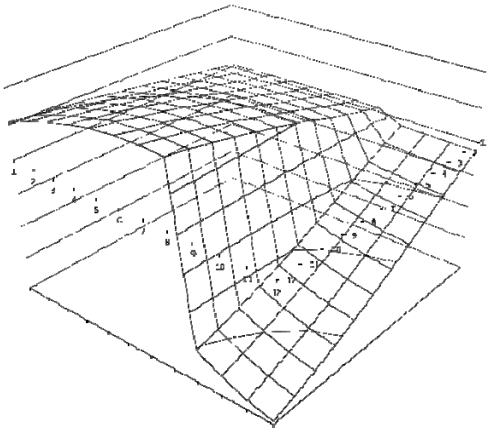


Рис. 3. Різниця ймовірностей порушення функціональної безпеки за параметрами цілісності та спостереженості

Вищенаведене дозволить визначити спільне для всіх нормативних параметрів значення, за яких їх вплив на загальний рівень функціональної безпеки ІС буде однаковий.

Висновок

Розроблена інформаційна технологія забезпечення функціональної безпеки інформаційних систем на стадії модернізації дозволить забезпечити нормативне значення якості функціонування системи функціональної безпеки при здійсненні заходів із вдосконалення складових відомчих інформаційних систем.

ЛІТЕРАТУРА

1. Про основи національної безпеки України: Закон України // Офіційний Вісник України. — 2003. — № 39. — Ст. 351.

2. Доктрина «Інформаційної безпеки України» [Електронний ресурс] // Офіційна веб-сторінка Верховної Ради України: Законодавство.

3. **Стрельбіцький М. А.** Прикордонний інформаційний ресурс: визначення поняття «Сучасні інформаційні технології у сфері безпеки та оборони». Національний університет оборони України імені Івана Черняховського, №1(25) 2016. — С. 205–208.

4. **Липаев В. В.** Технологические процессы и стандарты обеспечения функциональной безопасности в жизненном цикле программных средств / В. В. Липаев // Информационный бюллетень "JetInfo". — 2003. — № 3 (130). — 27 с.

5. **Ястребенецкий. М. А.** Оценка уровня безопасности информационных и управляющих систем АЭС / М. А. Ястребенецкий, В. В. Инюшев, О. Н. Бутова // Радиоэлектронные и компьютерные системы. — 2008. — №8 (27). — С. 96–103.

Юдін О. К., Стрельбіцький М. А.

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ НА СТАДІЇ МОДЕРНІЗАЦІЇ

У статті проведено аналіз існуючих підходів до забезпечення функціональної безпеки інформаційних систем. Визначено взаємозв'язок між дотриманням функціональних критеріїв інформаційного ресурсу та забезпечення функціональної безпеки інтегрованої інформаційної системи прикордонного відомства в цілому. Показано протиріччя між наявною теоретичною базою забезпечення функціональної безпеки та потребою у постійній модернізації інформаційних систем у складі інтегрованої інформаційної системи. Розроблено технологію забезпечення функціональної безпеки інформаційних систем на стадії модернізації та описано основні її етапи. Обґрунтовано стратегії модернізації які залежать від значення нормативного рівня функціональної безпеки та особливостей функціонування інформаційної системи. Описано рекомендації щодо вибору стратегій модернізації відповідно до особливостей функціонування інформаційної системи. Визначено вплив нормативних значень дотримання властивостей інформації при дослідженні ймовірностей порушення функціонування системи функціональної безпеки.

Ключові слова: інформаційна система; функціональна безпека; технологія; модернізація.

© Юдін О. К., Стрельбіцький М. А., 2017

Юдин А. К., Стрельбицкий М. А.

ТЕХНОЛОГИЯ ОБЕСПЕЧЕНИЯ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ НА СТАДИИ МОДЕРНИЗАЦИИ

В статье проведен анализ существующих подходов к обеспечению функциональной безопасности информационных систем. Определена взаимосвязь между соблюдением функциональных критериев информационного ресурса и обеспечением функциональной безопасности интегрированной информационной системы пограничного ведомства в целом. Показано противоречия между имеющейся теоретической базой обеспечения функциональной безопасности и потребностью в постоянной модернизации информационных систем в составе интегрированной информационной системы. Разработана технология обеспечения функциональной безопасности информационных систем на стадии модернизации и описаны основные ее этапы. Обоснованы стратегии модернизации, зависящие от значения нормативного уровня функциональной безопасности и особенностей функционирования информационной системы. Описанные рекомендации по выбору стратегий модернизации в соответствии особенностей функционирования информационной системы. Определено влияние нормативных значений соблюдения свойств информации при исследовании вероятности нарушения функционирования системы функциональной безопасности.

Ключевые слова: информационная система; функциональная безопасность; технология; модернизация.

Yudin O. K., Strelbitsky M. A.

TECHNOLOGY OF PROVIDING FUNCTIONAL SAFETY OF INFORMATION SYSTEMS AT THE STAGE OF MODERNIZATION

The article analyzes the existing approaches to ensuring the functional security of information systems. The relationship between the compliance with the functional criteria of the information resource and the functional security of the integrated information system of the border authority as a whole is determined. The contradiction between the existing theoretical basis for the provision of functional security and the need for the continuous modernization of information systems as part of an integrated information system is shown. The technology for ensuring the functional security of information systems at the stage of modernization is developed and its main stages are described. Reasonable modernization strategies depend on the importance of the normative level of functional security and the peculiarities of the functioning of the information system. Recommendations on choosing modernization strategies according to the peculiarities of the functioning of the information system are described. The influence of normative values of the observance of the properties of information in the investigation of the probability of a violation of the functioning of the functional security system is determined.

Keywords: information system; functional safety; technology; modernization.

Стаття надійшла до редакції 28.11.2017 р.
Прийнято до друку 29.11.2017 р.
Рецензент — д-р техн. наук, проф. Катеринчук І. С.

© Юдін О. К., Стрельбіцький М. А., 2017