УДК 004.415.056.5

Хлапонін Юрій Івановіч
Доктор технічних наук, старший науковий співробітник, завідувач кафедри кібернетичної безпеки і комп'ютерної інженерії
Київський національний університет будівництва і архітектури, Київ
Ізмайлова Ольга Василівна
Кандидат технічних наук, доцент, доцент кафедри кібернетичної безпеки і комп'ютерної інженерії, *orcid.org/0000-0002-2905-1827*
Київський національний університет будівництва і архітектури, Київ

ПІДХІД ДО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ В БУДІВНИЦТВІ

Анотація. *Проаналізовано шляхи та принципи побудови складних комплексних систем інформаційної безпеки, що розглядаються як складова частина корпоративних інформаційних систем в будівництві. Інформаційна модель будівлі BIM (Building Information Modeling) є інформаційною основою їх побудови. Обґрунтовано актуальність забезпечення на загальносистемному рівні конфіденційності даних, їх прозорості, доступності та цілісності в умовах, що визначають можливі загрози та ризики порушення достатнього рівня інформаційної та кібернетичної безпеки функціонування системи. Головну увагу приділено передпроектній стадії розробки системи та стадії ескізного проектування. Проаналізовано та запропоновано основні принципи розробки захищених систем. При цьому визначено, що головним принципом пошуку шляхів захисту інформації є неухильне дотримання системного підходу до розв'язання проблеми захисту інформації.*

Ключові слова: комплексна система інформаційної безпеки; інформаційна модель будівлі; інформаційна та кібернетична безпека; конфіденційність; прозорість; доступність та цілісність даних; принципи системного підходу

Постановка проблеми

В галузі будівництва кінець XX – початок XXI століть ознаменувався появою принципово нової ідеї, сукупності шляхів, підходів та засобів її втілення. Вона полягає в реалізації всіх етапів життєвого циклу (ЖЦ) будівлі від самих ранніх (створення концепцій проекту) до робочого проектування, будівництва, супроводження, експлуатації та зносу на основі єдиної інформаційної моделі будівлі **BIM (Building Information Modeling),** керуючись BIM – технологією її колективного поступового створення та загального використання. Основа технології BIM – це процеси, способи спільної роботи з інформацією про об'єкт будівництва. Процеси регулюють роботу з BIM-моделлю, яка складається з інтелектуальних об'єктів і параметричних взаємозв'язків. Для кожного етапу роботи над проектом прописано рівень деталізації BIM-моделі. Це дозволяє приймати управлінські рішення, маючи всю необхідну інформацію і при цьому не перевантажуючи модель [4; 5].

Рішення щодо обов'язкового застосування BIM і інформаційних систем для BIM з проведення робіт по будівельних проектах, базування на її інформації в умовах торгів за контрактами, експертизи проектних рішень прийняті на урядовому рівні в багатьох розвинених країнах світу: Великобританії, Нідерландах, Данії, Фінляндії, Норвегії, Північній Америці, Америці. Китаї. Найбільш інноваційні підприємства Білорусі, Казахстана, Росії активно переходять на BIM і вже відчули переваги від використання технології. На сьогодні в Україні розроблюється комплекс заходів щодо поглиблення можливостей і поширення застосування BIM [4]. Функціонує ряд будівельних фірм, які проектують у 3D з використанням зарубіжних програмних комплексів (AUTODESK, TEKLA, NEMETSCHEK, ARCHICAD, BENTLEY), виконують інтеграцію побудови 3D-проекту з побудовою календарних графіків, розподілом робіт по конструктивних елементах, виконавцях, виходом на різні кошторисні бази (система IBMS компанії «Інфобуд»), здійснюється ряд пілотних проектів, проводяться семінари, навчання, розширюються зарубіжні контакти. Велика частина з тих, хто поки не перейшов на BIM, усвідомили незворотність змін, що відбуваються в будівельній галузі, і сьогодні вибирають ефективний метод впровадження інформаційного моделювання.

Застосування BIM є інформаційною основою реалізації корпоративної (інтегрованої) інформаційної

системи управління ЖЦ (КІС ЖЦ) будівлі, де кожна функціональна складова: система, підсистема або комплекс задач (навіть при розробці як прототипу майбутньої системи) може бути розроблена індивідуально залежно від вимог предметної області, але вона базується на даних інформаційної 3D-моделі. При цьому застосовується формат файлів, що забезпечує обмін інформацією між різними функціональними складовими, які можуть базуватися на різних програмно-апаратних платформах [6]. Так, на сьогодні створено безліч можливих форматів програмних засобів (наприклад, Revit, ADT, Bentley, Nemetschek, 3D-моделі S, ArchiCAD, Tekla, Sketch up, Rhino, Maya) та засобів реалізації бізнес-процесів : CAD / CAM / CAE / PDM / PLM / ERP / MS Office / Estimating / Scheduling. Інформаційна модель стає постачальником даних для системи закупівель, системи календарного планування, системи управління проектами, внутрішньої ERP-системи і інших систем підприємства[4; 5].

У спектрі інтересів суб'єктів, що пов'язані з побудовою і використанням системи, існує суттєва проблема забезпечення достатнього рівня інформаційної та кібернетичної безпеки її функціонування. Її розв'язання є одним з визначальних важелів не тільки досягнення очікуваних фінансових, проектних та експлуатаційних результатів на різних етапах життєвого циклу будівлі, але і гарантом збереження інноваційних розробок, забезпечення інформаційної та інтелектуальної власності.

Мета статті

Актуальним при створенні КІС ЖЦ на різних управлінських рівнях (загальносистемні проектні рішення, функціональні складові різних стадій та етапів життєвого циклу) є вирішення завдання – забезпечити та оптимізувати за встановленими критеріями результати знайденого компромісу між двома пріоритетними потребами – прозорість, доступність для всіх користувачів єдиної інформаційної моделі, з одного боку, і гарантія захищеності даних та надійний рівень інформаційної та кібернетичної безпеки, з іншого боку. При цьому, система захисту не повинна створювати помітних незручностей в процесі роботи користувачів інформаційної системи. Мають бути гарантовані: повна свобода доступу кожного користувача та незалежність його роботи в межах наданих йому прав і повноважень.

Аналіз останніх досліджень і публікацій

На думку спеціалістів у питаннях захисту даних [2; 7 – 9] на сучасному етапі розвитку інформаційних технологій забезпечення інформаційної та кібернетичної безпеки в масштабах всієї КІС поки що проблематично в силу відсутності на ринку реальних рішень, що дозволяють будувати саме інтегровані системи захисту даних. Спеціалістами це пояснюється недостатньою зрілістю міжнародних стандартів у галузі захисту інформації, хоча рух у цьому напрямку простежується вже досить явно. Констатується, що жоден окремо вибраний засіб захисту інформації не може захистити від різноманіття існуючих загроз безпеки, а проста комбінація різноманітних засобів може призвести до зниження рівня захисту в цілому внаслідок можливої їх конфліктності. Тому останнім часом намітилася тенденція до побудови складних комплексних систем інформаційної безпеки (КСЗІ), що розглядаються як складова частина корпоративних інформаційних систем і в сьогоднішній термінології синтез КСЗІ та КІС розглядаються як захищені корпоративні інформаційні системи. При цьому проектування захищеної корпоративної системи є досить складним системно-аналітичним завданням розв'язання слабоструктурованої проблеми. В якості методологічного інструмента її розв'язання в умовах складних інформаційних систем розглядаються методи системного аналізу на етапі формування вимог та розгляду альтернативних варіантів і методи прийняття рішень для синтезу систем захисту [1; 2]. Таким чином аналіз останніх досліджень надав можливість зробити висновок, що обґрунтованим та найбільш важливим шляхом побудови захищених КІС ЖЦ є базування на системному підході до розв'язання проблеми забезпечення достатнього рівня інформаційної та кібернетичної безпеки.

Виклад основного матеріалу

Захист інформації в КІС ЖЦ будівлі повинен являти собою регулярний процес забезпечення безпеки даних як на загальносистемному (першому) рівні, так і на інших рівнях ієрархії функціональних компонентів на різних стадіях та етапах ЖЦ споруди, що базуються на 2D – 6D технологіях розв'язання. Для різних рівнів функціональної ієрархії спільним є те, що захист даних буде розглядатися на загальних типових рівнях захисту [2], кожний з яких вирішує свої задачі. Так, в якості типових розглядаються рівень мережевих послуг, рівень операційних систем, рівень систем керування базами даних та рівень виконання прикладних функцій системи (рівень прикладного програмного забезпечення). При цьому забезпечення захисту даних полягає в розв'язанні задачі гарантування надійного рівня забезпечення таких головних властивостей інформації, як конфіденційність, цілісність та доступність [2; 8]. Під ***конфіденційністю*** інформації розуміється, що інформація, яка закладена в BIM – модель не може

бути отримана та використана неавторизованим користувачем (людиною або іншим процесом системи). ***Цілісність*** передбачає можливість модифікування інформації моделі тільки користувачеві з відповідним рівнем повноваження та доступу, який має бути пов’язаний з характером задачі, що розв’язується, етапом ЖЦ, часовим інтервалом тощо. ***Доступність*** полягає в комфортному забезпеченні відповідно до встановлених уповноважень користувачів доступу до інформації, подання даних в установленому вигляді без тривалого проміжку часу.

Високу міру актуальності розв’язання цієї задачі в період створення та експлуатації КІС ЖЦ будівлі можна обґрунтувати такими сьогоденними умовами та властивостями загроз та ризиків в системі будівництва.

– Умови конкуренції при прийнятті рішень на всіх стадіях та етапах ЖЦ будівлі.

– Ризик корупційних схем управління ЖЦ будівлі.

– Вплив суттєвих відмінностей між розробленням корпоративної стратегії будівельного підприємства та КІС в цілому та бізнес-стратегії, яка охоплює управління в рамках певного функціонального компонента на окремій стадії та етапі ЖЦ.

– Варіантний підхід у процесі аналізу прийняття рішень на всіх етапах ЖЦ, де цільові установки, вибір, критерії оцінювання та їх пріоритету, прогнозування альтернативних результатів є прерогативою «людини» з об’єктивним розходженням локальних інтересів [3].

– Недостатній сьогоденний рівень підготовленості користувачів до застосування сучасних методів комп’ютерного моделювання та реалізації бізнес-процесів.

– Множина різноаспектних бізнес-процесів системи, що повинні бути зв’язані в єдину інформаційну технологію в умовах широкого спектру учасників їх реалізації (замовники-інвестори, компанії-проектувальники, компанії-виробники, компанії-підрядники, оператори, ремонтники, постачальники, ІТ-спеціалісти, кошторисники, менеджери).

– Необхідність підтримки цілісності, доступності та конфіденційності BIM – моделі протягом реалізації різноаспектних функцій системи протягом тривалого життєвого циклу споруди, що може відповідати декільком десятиріччям. При цьому BIM-технологія потребує об’єднання інформації, якою вже володіє організація, з новими знаннями, які з'являються у компанії при переході на BIM. Вона забезпечує обмін даними між наявними системами підприємства і BIM-моделлю.

– В інформаційному моделюванні будівля і все, що має до неї відношення, розглядаються як єдиний об'єкт, тобто будівельний об'єкт проектується як єдине ціле і зміна будь-якого його параметра тягне за собою автоматичну зміну інших, пов'язаних з ним параметрів, від креслень, і їх візуалізації, до змін специфікацій, кошторисів і графіків будівництва. Це висуває особливі вимоги до цілісності даних.

– Масштабність і варіантність програмно-апаратної платформи (сервери, операційні системи, системи комунікації, СУБД), робота в неоднорідному обчислювальному середовищі, де має бути забезпечена взаємодія всіх робочих обчислювальних платформ і операційних систем, які використовуються.

– Орієнтованість КІС ЖЦ на великі компанії і необхідність підтримки роботи територіально рознесених вузлів або мереж. Використання персональних обчислювальних машин (ПЕОМ), підключення їх до локальних обчислювальних мереж, а тим більше – до глобальних мереж, ускладнюють реалізацію заходів безпеки інформаційних систем. Це пов'язано із забезпеченням цілісності інформації як у пам'яті ЕОМ, так і на носіях, що зберігаються окремо від ЕОМ, а також з ідентифікацією прийнятої інформації та зі збереженням її достовірності під час передачі по каналах зв'язку.

На сьогодні в світі існує новий імператив управління, що визначає вирішальну значущість обґрунтованого варіантного проектування на ранній передпроектній стадії (стадії формування концепції) при розробці інформаційних систем. Це нагадує, що якісне розв’язання проблеми захисту інформації в таких складних інформаційних системах насамперед визначається обґрунтованістю рішень передпроектної стадії життєвого циклу системи захисту. Реалізація етапів цієї стадії базується на дослідженні предметної області функціонування КІС, аналізі та декомпозиції проблеми захисту даних інформаційної системи, аналізі можливих загроз, ризиків, пошуку і оцінці варіантів удосконалення діючої або розробки нової системи захисту та зводиться до формування головних вимог, що будуть визначені в рамках технічного завдання на створення системи захисту.

При цьому ефективність рішень побудови системи, по суті, буде залежати від вдалого вибору компромісного рішення, що забезпечує домінант глобальних цілей інформаційної безпеки і засобів їх досягнення при проектуванні на локальному рівні, з одного боку, і досконалий аналіз локальних вимог і врахування їх раціонального впливу на загальні системні рішення, з іншого боку. Тобто, на основі визначених критеріїв ефективності системи захисту необхідно визначити обґрунтований баланс поліпшення одних рішень на можливе погіршення інших.

Міністерство регіонального розвитку, будівництва та житлово-комунального господарства України приділяє значну увагу поширенню можливостей будівельної галузі на основі застосування BIM. На сьогодні розробляється "Програма реорганізації будівельної галузі та житлово-комунального господарства України" на основі впровадження системи інформаційного моделювання (Building Information Modeling – BIM). В рамках цієї програми визначено, що залогою успішного впровадження інформаційного моделювання в будівництво є підготовка кадрів, що володіють сучасними методами проектування, управління будівництвом і експлуатацією об'єктів нерухомості із застосуванням BIM. Для цього в профільних вищих навчальних закладах ставиться задача створення відповідних програм підготовки та перепідготовки фахівців. Головною масштабною складовою підготовки таких фахівців повинні стати галузеві будівельні вищі навчальні заклади (або відповідні факультети технічних ВНЗ) з напрямами підготовки як будівельних спеціальностей, так і IT-спеціалістів з проектування (САПР, ІТЕП), управління будівництвом (ІУСТ) та захисту даних в інформаційних системах. Вони повинні стати головними центрами підготовки фахівців. Розв'язання цього питання визначене як вкрай актуальне для України.

У Київському національному університеті будівництва і архітектури для студентів з галузі знань «Інформаційні технології» спеціальностей «Інформаційно-управляючі системи і технології», «Інформаційні технології проектування» та «Кібербезпека» введені ряд дисциплін, що присвячені інформаційному моделюванню в будівництві на основі BIM, запропонована тематика наукової роботи студентів, дипломного та курсового проектування зі створення прототипів окремих функціональних підсистем або їх окремих локальних функціональних компонентів з врахуванням паралельної розробки прототипів систем захисту даних як складової частини захищених КІС ЖЦ будівлі. В рамках цієї роботи значну увагу приділено передпроектній стадії розробки системи та етапу ескізного проектування.

Проведений аналіз результатів перших етапів роботи в цьому напрямі дозволив аргументувати необхідність керування такими принципами реалізації системного підходу.

Інтегрований тріадний принцип побудови захищеної інформаційної системи, де аналізуються альтернативи побудови при наступному ранжируванні пріоритетів оцінювання: «цілі ефективного функціонування інформаційної системи» – «цілі удосконалення системи захисту» – «засоби захисту».

Цільовий аналіз вимог до захисту даних залежно від встановленого рівня безпеки. Базування на визначенні структури цілей до захисту даних в КІС ЖЦ і першочергових системних кроків щодо досягнення встановленого рівня безпеки системи в цілому відповідно до визначеного рівня категорії захисту інформації про будівлю (державна, комерційна, професійна, службова тощо).

Ієрархічний підхід до аналізу вимог. Аналіз вимог і розгляд засобів інформаційного захисту системи на різних рівнях декомпозиції функціональних компонент. Перевага – це шлях суттєвого спрощення процесу проектування системи, прийняття рішень проектування системи в цілому розгалужується на паралельне проектування набагато менш складних компонент.

Принцип єдності та зв'язності. Оцінка рішень на деталізованому рівні з точки зору «локальної» корисності для функціональної складової, так і з точки зору системних цілей, вимог та можливостей. Синтез рішень щодо побудови системи полягає в контролі цілісності для кожного рівня окремо й завершального етапу контролю ефективності системи захисту при переході від рівня до рівня [10].

Врахування неоднорідності рішень захисту даних в КІС ЖЦ будівлі. Багатоаспектна структура системи, різноманітність функціональних призначень, тривалість життєвого циклу, відмінність середовищ функціонування кожної складової системи обґрунтовують неоднорідність її побудови. Для кожної окремої функціональної системи можуть існувати індивідуальні «ризикові» інформаційні ресурси, програмно-апаратні засоби обробки даних, архітектури обчислювальної системи, характеристики середовища користувачів та технології обробки інформації, канали обміну інформацією, свій перелік конкретних загроз, порушень та ризику тощо. А, отже, і вимоги до політики безпеки інформації, вимоги до функціонального профілю захищеності інформації, вимоги до реалізації послуг безпеки в різних складових КІС ЖЦ на різних об'єктах будівництва мають бути різними.

Принцип модульності. Існує принцип декомпозиції системи на функціональні модулі, що призначені для виконання окремої функції системи на різних стадіях та етапах ЖЦ, мають закінчене оформлення та засоби сполучення з іншими модулями. При обстеженні інформаційного середовища реалізації кожного модуля КІС інформація повинна бути класифікована за режимом доступу, за правовим режимом, визначені й описані можливі загрози, види порушень та ризики їх виникнення. При цьому аналізується міра досягнення основних властивостей захищених систем – конфіденційність, цілісність, доступність, яким вони повинні задовольняти.

Тріадний принцип розробників. Процес формування вимог та проектування захищеної КІС потребує створення та застосування ефективної методології взаємодій в рамках **«аналітик інформаційної системи – спеціалісти-користувачі** (архітектори, замовники-інвестори, проектувальники, виробники, підрядники, кошторисники, менеджери) **– аналітики системи захисту даних».**

Висновки

1. Захист інформації в системах управління життєвим циклом будівлі на основі інформаційного моделювання BIM є актуальним завданням. Це стало одним з визначальних важелів не тільки досягнення очікуваних фінансових, проектних та експлуатаційних результатів, але і гарантом збереження інноваційних розробок та інтелектуальної власності.

2. Для того щоб забезпечити надійний захист інформації при проектуванні і розробці КІС повинні бути реалізовані самі прогресивні й перспективні методи та засоби інформаційної безпеки як складової частини КІС ЖЦ будівлі у вигляді комплексної системи захисту даних.

3. Головним напрямом пошуку шляхів захисту інформації є неухильне дотримання системного підходу до розв'язання проблеми захисту інформації. Це передбачає аналіз і оптимізацію рівня безпеки всієї системи, з врахуванням вимог окремих її частин.

4. Системний підхід базується на врахуванні всіх взаємопов'язаних, взаємодіючих і змінних в часі компонентів КІС, важливих для забезпечення інформаційної безпеки. В статті сформульовані найбільш вагомі, з точки зору авторів, принципи реалізації системного підходу.

Запропоновані принципи розглядаються авторами як еволюційний прототип першого етапу знайомства з особливостями КІС ЖЦ будівлі, що не претендує на повне й точне формулювання принципів реалізації системного підходу і передбачає подальшу роботу щодо приближення до реалій бізнес-застосування.

Список літератури

1. *Богуш Б.М., Довидков О.А. Проектування захищених інформаційних систем і мереж. – К.: ДУІКТ, 2006. – 414 с.*
2. *Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с.*
3. *Ізмайлова О.В., Горгураки В.Ф. Моделі та методи оцінки критеріїв ефективності рішень забезпечення техногенної безпеки у будівництві // Управління розвитком складних систем. – 2010. – Вип. 3. – С. 48 – 55.*
4. *Николаев В. П. Новейшие методы и информационные технологии управления в строительстве. [Електроний ресурс]: http://www. infobud. com. ua/ru]*
5. *Попов В. BIM – информационная модель здания: пора или не пора. [Електроний ресурс] – http://scadsoft. com/download/BIM2011. pdf]*
6. *Совместное использование BIM-модели: IFC [Електроний ресурс]: http://helpcenter. graphisoft. ru]*
7. *Толюпа С.В. Аналіз підходів моделювання процесів прийняття рішень при проектуванні систем захисту інформації / С.В. Толюпа, І.М. Павлов // Науково-технічний журнал. Сучасний захист інформації. – К.: ДУТ, 2014. – №2. – С. 96 – 104.*
8. *Хлапонін Ю. І. Модель системи оцінки рівня захищеності інформації на основі нейромережі //Сучасні інформаційні технології в сфері безпеки та оборони. – 2014. – № 1. – С. 96 – 100.*
9. *Хлапонін Ю. І. Управління інформаційною безпекою на основі інтелектуальних технологій / Technology audit and production reserves (Технологический аудит и резервы производства). – 2014. – № 6/4(20). – С. 47 – 50.*
10. *Krasovska H. V., Izmailova O. V., Krasovska K. K. Prototyping of intellectual decision support system for organizational and technological trainings in construction // Materials of the XII International scientific and practical conference, "Areas of scientific thought". – 2015/2016. – Volume 16. Mathematics. Physics. Modern Information technologies. Sheffield. Science and Education LTD – P. 101-105.*

Стаття надійшла до редколегії 25. 07. 2017

Рецензент: д-р техн. наук, проф. А. О Білощицький, Київський національний університет ім. Тараса Шевченка, Київ.

Хлапонин Юрий Иванович
Доктор технических наук, старший научный сотрудник, заведующий кафедрой кибернетической безопасности и компьютерной инженерии
Киевский национальный университет строительства и архитектуры, Киев
Ізмайлова Ольга Васильевна
Кандидат технических наук, доцент, доцент кафедры кибернетической безопасности и компьютерной инженерии, *orcid.org/0000-0002-2905-1827*
Киевский национальный университет строительства и архитектуры, Киев

ПОДХОД К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ КОРПОРТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ В СТРОИТЕЛЬСТВЕ

Аннотация. *Проанализированы пути и принципы построения сложных комплексных систем информационной безопасности, которые рассматриваются как составная часть корпоративных информационных систем в строительстве. Информационная модель здания BIM (Building Information Modeling) является информационной основой*

их построения. Обоснована актуальность обеспечения на общесистемном уровне конфиденциальности данных, их прозрачности, доступности и целостности в условиях, определяющих угрозы и риски нарушения достаточного уровня информационной и кибернетической безопасности функционирования системы. Главное внимание уделено передпроектной стадии разработки системы и стадии эскизного проектирования. Проанализированы и предложены основные принципы разработки защищенных систем. При этом определено, что главным принципом при поиске путей защиты информации является неукоснительное соблюдение системного подхода к решению проблемы защиты информации.

Ключевые слова: комплексная система информационной безопасности; информационная модель здания; информационная и кибернетическая безопасность; конфиденциальность, прозрачность, доступность и целостность данных; принципы системного подхода

Khlaponin Yuriy
Doctor of Technical Sciences, Senior Researcher, Head of the Department of Cybernetic Security and Computer Engineering
Kyiv National University of Construction and Architecture, Kyiv
Izmailova Olga
Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Cybernetic Security and Computer Engineering, *orcid.org/0000-0002-2905-1827*
Kyiv National University of Construction and Architecture, Kyiv

APPROACH TO PROVIDING THE PROTECTION OF CORPORATE INFORMATION SYSTEMS IN CONSTRUCTION

Annotation*. The work is devoted to the analysis of ways and principles of construction of complex complex information security systems, are considered as an integral part of corporate information systems in construction. Information model building VIM (Building Information Modeling) is the information basis for their construction. The urgency of ensuring the confidentiality of data on the system-wide level, their transparency, accessibility and integrity in the conditions that determine the threats and risks of violation of a sufficient level of information and cyber security of the system functioning is substantiated. The main attention is paid to the design stage of system development and the stage of preliminary design. Analyzed and proposed the basic principles of the development of secure systems, while it is determined that the main principle in the search for ways to protect information is to strictly adhere to a systematic approach to solving the problem of information security.*

Keywords: Integrated information security system; information model of the building; Information and cybernetic security; Confidentiality, transparency, availability and integrity of data; Principles of the system approach

References

1. Bogush, B.M., Dovidkov, O.A. (2006). Designing secure information systems and networks. DUIKT, 414.

2. Grayvoronsky, M.V., Novikov, O.M. (2009). Security of Information and Communication Systems. BHV Publishing Group, 608.

3. Izmailova, O.V., Gorguraki, V.F. (2010). Models and methods of estimation of the criteria of efficiency of solutions of providing of technogenic safety in construction. Management of the development of complex systems, 3, 48-55.

4. Nikolayev, V.P. Newest methods and information technology in building management. [Electronic resource] -: http://www. infobud. com. ua/en

5. Popov, V. BIM – information model of a building: it's time or not time. [Electronic resource] – http://scadsoft. com/download/BIM2011. pdf.

6. Joint Use of the BIM Model: IFC [Electronic Resource] – http://helpcenter. graphisoft. ru.

7. Tolyuta, S.V. (2014). Analysis of approaches to modeling decision-making processes when designing information security systems. / S. V. Tolyupa, I. M. Pavlov // Modern Information Protection. DUT, 2, 96-104.

8. Khlaponin, Yu. I. (2014). The system of estimation of the level of information security on the basis of the neural network. Modern information technologies in the field of security and defense, 1, 96-100.

9. Chlaponin, Yu. I. (2014). Information Security Management based on Intelligent Technologies. Technology audit and production reserves, 6/4 (20), 47-50.

10. Krasovska, H.V., Izmailova O.V., Krasovska K.K. (2016). Prototyping of the intellectual decision support system for organizational and technological trainings in construction. Materials of the XII International scientific and practical conference, "Areas of scientific science", 2015/2016, 16. Mathematics. Physics Modern Information technologies. Sheffield Science and Education LTD, 101-105.

Посилання на публікацію

APA *Khlaponin, Yuriy & Izmailova, Olga. (2017). Approach to providing the protection of corporate information systems in construction. Management of Development of Complex Systems, 31, 126 – 131.*

ДСТУ *Хлапонін Ю. І. Підхід до забезпечення захисту корпоративних інформаційних систем в будівництві [Текст] / Ю. І. Хлапонін, О. В. Ізмайлова // Управління розвитком складних систем. – 2017. – № 31. – С. 126 – 131.*