УДК 004.681.5

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 3, pp. 195-200

МОДЕЛІ ЗАГРОЗ ІНФОРМАЦІЙНОМУ ПРОСТОРУ СИСТЕМ УПРАВЛІННЯ ПОВІТРЯНИМ РУХОМ ТА МЕХАНІЗМИ ЙОГО ЗАХИСТУ

А.М. Орєхов, В.О. Хорошко

Національний авіаційний университет,
пр. Космонавта Комарова, 1, Київ, 03058, Україна; e-mail: professor_va@ukr.net

Розглянуто життєвий цикл інформації в системі управління повітряним рухом, яка знаходиться у інформаційному просторі, та вимоги до системи захисту. На їхній основі визначено перелік класів загроз та внутрішніх і зовнішніх зловмисників. З урахуванням дослідження створена модель загроз інформації.

Ключові слова: системи управління повітряним рухом, системи захисту інформації, інформаційний простір

Вступ

Сьогодні здійснюється перехід нашого суспільства від індустріального до інформаційного. Це стало можливим завдяки розвитку технологій, які дають змогу зберігати та обробляти великі масиви інформації, передавати її на великі відстані, здійснювати обмін цією інформацією між різними користувачами.

Перед Україною стала задача щодо входження до європейського та світового інформаційного простору для розширення взаємних зв'язків з різними державами. Тому питання захисту інформаційного простору та інформації, що передається, приймається та зберігається у ньому, є надзвичайно актуальними.

З урахуванням рівня втілення інформаційних технологій сучасності, розглядаючи інформацію як об'єкт діяльності, треба відзначити, що залежно від її важливості та значення для користування нею витрачаються відповідні ресурси. Але важливість та значення інформації для тих чи інших суб'єктів інформаційних відносин в умовах прихованого інтересу визначити складно. Тому зрозуміло, що задоволення інформаційних потреб перебуває в пропорційній залежності від умов та методів і засобів практичної діяльності відповідних суб'єктів, а високий рівень автоматизації, до якого прагне людство, ставить його в залежність від рівня безпеки інформаційних технологій, які воно використовує. Особливо це важливо для систем управління повітряним рухом (СУПР).

СУПР становить ключову складову національної аеронавігаційної системи України. На розвиток цієї системи відбиваються загальносвітові глобалізаційні тенденції, а саме відбувається інтенсивна інтеграція інформаційних активів систем на регіональному, національному та глобальному рівнях.

Інформаційний простір (ІП), що використовується зараз у СУПР, співпрацює за допомогою автономних локальних мереж. Проте, в перспективі завдяки розвитку глобального ІП інформаційні системи усіх участків процесу управління повітряним рухом інтегруватимуться в єдину систему, яка матиме відкриту розподілену архітектуру глобального масштабу.

Об'єднання ресурсів СУПР – це не самоціль, а за умов зростання попиту на авіаперевезення – це основа забезпечення потрібного рівня безпеки польотів, підвищення пропускної спроможності та економічної ефективності авіаційної галузі.

Авіаційна спільнота вже звернула увагу на той факт, що ІП і мережі, які використовуються СУПР, є потенційно вразливими при втручанні віддалених хакерів та інсайдерів. Експерти з питань інформаційної безпеки виявляють значну кількість «шпарин» у них, неспроможність авіаційних адміністрацій виявити вторгнення і підтримувати працездатність системи у разі порушення захисту через неадекватне управління ІП, оновленням програмного забезпечення, обліковими записами, паролями і привілеями користувачів, а також через ігнорування потреби у відслідкуванні причин подій, що стосуються безпеки.

Основна частина

Будь-яку інформацію розглядають у вигляді потоків, які діють на органи сприйняття користувача формами зображення, звуку та тексту, що призводять до породження потоків відповідних форм.

Визначення 1. Інформація – такий стан суспільно - політичних та соціально – економічних відносин у державі (групи держав), за якого реальні важелі впливу на формування і введення державної зовнішньої і внутрішньої політики мають особи (угрупування), що ініціюють та/або контролюють основні процеси та/або явища в інформаційному середовищі, а також розподіляють інформаційні потоки у зазначеній державі (групи держав).

Визначення 2. Інформаційний потік - рух інформації в ІП.

Сучасні інформаційні технології сублімують у собі якості усіх форм, різні поточні форми можуть трансформуватися між собою. Умовно всі трансформації в СУПР визначено як трансформації інформаційних потоків, модифікація яких ставить питання порушення цілісності та достовірності інформації (властивості інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом). Інформаційні потоки поділяють на елементарні структурні одиниці – файли чи повідомлення.

Визначення 3. Файл – це іменована область пам'яті системи, яка містить компоненти одного типу.

Наукова проблема цілісності інформації, яка сформульована у межах цієї статті - це цілісність окремого файлу наданого формату.

Розглядання інформаційних трансформацій на предмет реалізації поставлених вимог диктує необхідність локалізації її основних процесів.

Оскільки ми орієнтуємось на захист відомчих інтересів, тобто СУПР, треба зауважити, що на всіх етапах [1, 2] трансформації інформації (відомостей) визначається деякий проміжок часу, тобто інформація має певний життєвий цикл (див. рис.1).

Життєвий цикл інформації у ІП СУПР залежить від оцінки її цінності, а також відповідно від спроможності санкціонованих користувачів забезпечити її надійний захист, і, отже, не допустити «знецінення» та «знищення» інформації. Він передбачає, що інформація здобувається, обробляється (анімується), зберігається, охороняється, використовується, транслюється та знищується. Тому розглянемо етапи життєвого циклу інформації з позиції цільової ознаки системи контролю цілісності та достовірності інформації (СКЦДІ) детальніше, щоб відокремити вразливі ланки трансформації, які потребують захисту. Підкреслимо, що модифікації інформації охоплює всі етапи життєвого циклу. Під терміном «модифікація» будемо розуміти будь-яку зміну попереднього змісту інформації стосовно етапу її створення (див.рис.1).

Процеси створення та знищення інформації, тобто відображення або створення на матеріальному носії: електронної накопиченої інформації з урахуванням визначених

завдань користувачами. Після отримання і створення інформаційного масиву здійсняється його оцінка на предмет відповідності абстрактним і конкретним вимогам щодо подальшого використання у визначених (дозволених) межах. Зберігання вимагає розроблення порядку та правил підготовки до зберігання інформації в електронному вигляді з технологією обмеження доступу. Вибірка інформації та подальша оцінка вибору зумовлена конкретністю поставленої задачі. Критичність щодо інформації постає з моменту вибірки та подальшого такого опрацювання.

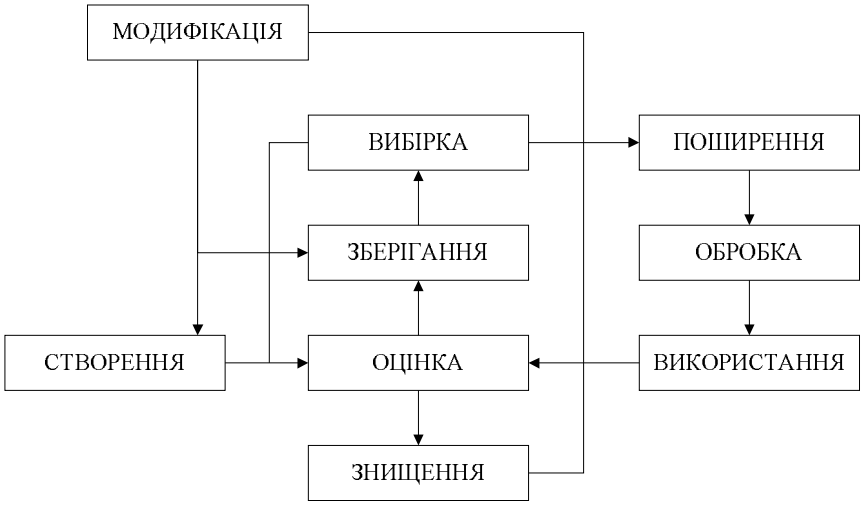

Рис. 1. Життєвий цикл інформації у ІП СУПР

Обробка та використання інформації суб'єктами ІП СУПР, які зумовлюють практичне використання інформації у своїй роботі при прийнятті рішень та реалізації тих чи інших процесів у керуванні повітряним простором, дає змогу виділити найуразливішу ланку захищеного ІП – етап передавання інформації, де є можливість несанкціонованих дій зловмисника або неавторизованого користувача (перегляду, модифікації, знищення).

Засоби контролю цілісності та достовірності інформації функціонують на різних структурних рівнях її обробки. Це низький, середній та високий: низький (структурний рівень), середній (семантичний рівень подання інформації) та високий (логічний рівень контексту інформації) рівні. Розглядання високого рівня виходить за межі цієї статті, засоби середнього рівня аналізується у цій роботі.

На низькому (структурному) рівні обробки інформації автоматизованим робочим місцем [2, 3] функціонують методи, які відповідають СКЦДІ.

Отже, вирішення проблеми цілісності та достовірності інформації зумовлює розгляд елементів його сигнатурного аналізу та побудови функцій хешування даних, які формулюються з урахуванням та систематизації переліку загроз інформації та класифікації характеристик файлу ІП, які критичні до модифікування.

Обробка інформації пов'язана з формою подання на подразники остаточної інформації (текст, зображення, звук). Крім перелічених інформаційних потоків, існують ще деякі службові дані, що характеризують програмне середовище та відображають його функціональність (відповідність призначенню). Тобто інформаційний потік залежно від сприйняття поданій в формі текстового, графічного або звукового потоку, потоку відео зображення та службового потоку, який циркулює на рівні функціонування вузлів обробки інформації, СУПР та забезпечує існування перерахованих потоків в сучасному ІП управління повітряним простором.

На низкому рівні інформаційні потоки – це послідовність байтів стандартного оформлення (формати даних). Під модифікацією файлів розуміється модифікація потоків, оскільки перший є структурною одиницею потоку.

Визначення 4. Загроза інформаційної безпеки ІП СУПР – це можливість реалізації впливу на інформацію у ІП, що призводить до створення, знищення, блокування доступу до інформації, також можливість впливу на компоненти СУПР, що призводить до втрат, знищення або збою функціонування системи, засобів взаємодії з постачальником інформації або засобів управління системою та ІП.

Необхідність класифікації загроз інформаційній безпеці зумовлена тим, що архітектура сучасних засобів автоматизованої обробки, організаційна структурна та функціональна побудова СУПР та їх мереж, технології та умови обробки такі, що інформація потрапляє під вплив надмірної кількості чинників, за якими і потрібно формалізувати задачу описання загроз та ефективної протидії їм. Перелік загроз інформаційної безпеки [3] будемо розглядати за цільовою ознакою класифікації та описання складних інформаційних потоків, критичних до модифікування та впливів. Аналіз цих загроз повинен бути здійснений на основі їхньої класифікації за низкою ознак [4]. Кожне з цих ознак відображає одну із узагальнених вимог до системи захисту (конфіденційність, цілісність, достовірність): необхідність дії, що призводить до можливості несанкціонованого доступу до конфіденційної інформації або роблять її загальнодоступною; ігнорування організаційних обмежень (встановлених правил) під час визначення рангу системи; несанкціоноване втручання в роботу ІП або модифікування інформації, що впливає на штатну роботу СУПР.

Для системи визначимо перелік класів загроз (якості моделі): за природою виникнення; за ступенем навмисності; за безпосереднім джерелом загроз; за станом джерел загроз; за мірою залежності від активності СУПР; за мірою впливу на СУПР та ІП; за станом доступу користувачів або програм до ресурсів ІП СУПР; за способом доступу до ресурсів ІП СУПР; за поточним місцем розміщення інформації, що зберігається і обробляється в СУПР.

Відповідно для ІП та СУПР будемо розглядати наступні види загроз: порушення конфіденційності (інформація стає відома тим, хто не повинен нею володіти); порушення цілісності (включає в себе поняття будь-якої навмисної зміни інформації, що зберігається або обробляється в СУПР або при її передаванні між елементами системи; розкриття параметрів СУПР.

Розглядаючи питання захисту ІП та СУПР, доцільно використовувати чотирирівневу градацію доступу до інформації, що зберігається, обробляється та залишається в ІП та СУПР: рівень інформаційних ресурсів; рівень засобів взаємодії з інформаційними ресурсами; рівень надання інформації; рівень захисту інформації.

Потрібно сформулювати додаткові вимоги щодо аналізу загроз інформації:

- перелік загроз повинен бути максимально повним та деталізованим. Для кожної із загроз необхідно визначити, на порушення яких властивостей інформації або СУПР вона спрямована (конфіденційності, цілісності, доступності, а також відмови служб СУПР);
- можливі методи реалізації загроз [5].

З урахуванням технології обробки інформації та побудови моделі загроз інформації необхідно розробити модель зловмисника, яка повинна бути адекватна реальному зловмиснику для певної СУПР.

Визначення 5. Модель зловмисника – абстрактне формалізоване або неформалізоване описання дій зловмисника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце тощо.

Стосовно СУПР зловмисники можуть бути зовнішніми або внутрішніми. Модель зловмисника повинна визначати: можливу мету зловмисника та її градацію за ступенем

небезпеки для СУПР; категорії осіб, із яких може бути зловмисник; передбачення про кваліфікацію зловмисника; передбачення про характер дій зловмисника.

Метою зловмисника може бути можливість вносити зміни в інформаційні потоки згідно зі своїми намірами та завдання завдати збитків через знищення інформації.

Будь-яка якісна система протидії апріорно передбачає високий досвід та кваліфікацію зловмисника (можливість використання недоліків проектування комплексної системи захисту СУПР за допомогою методів та засобів активного впливу на СУПР, які змінюють конфігурацію системи).

Також передбачається, що за місце дій зловмисники можуть одержати доступ до засобів адміністрування СУПР та засобів управління комплексною системою захисту.

Перелік загроз [4, 5], оцінка їхньої реалізації, модель зловмисника є основою для аналізу ризику реалізації загроз та формулювання рис моделі реєстрації даних.

Дія моделі реєстрації даних поширюється на рівень аутентифікації файлів.

Перша умова функціонування моделі – автономність СКЦДІ (незалежність від дій системного адміністрування). Умова друга – обов'язковість (застосування алгоритмів СКЦДІ до кожного елемента потоку). Умова третя – компактність засобів СКЦДІ (застосування мінімальних обчислювальних ресурсів). Умова четверта - реагування (комплекс організаційних заходів щодо порушення цілісності об'єкта).

Враховуючи, що файл є одиницею між різними системами обробки інформації і він виступає як індикатор СКЦДІ, розглядаємо характеристики файлу як одиниці, до якої можливе застосування моделі реєстрації та підтвердження їхньої цілісності.

Створення механізму ефективного захисту інформації з обмеженням доступом передбачає, насамперед, уявлення, що в основі існує стандартна система, яка складається з об'єкта нападу (ІП СУПР та сам СУПР) та суб'єкта, який намагається використати інформацію всупереч встановленим нормам поводження з нею.

Проаналізувавши життєвий цикл інформації в СУПР, визначимо питання щодо його аналізу: як транспортувати інформацію; який вид аналізу застосувати для визначення стану інформації після її транспортування?

Якщо позначка дослідження – вибір виду аналізу, то об'єктом аналізу, зважаючи на це, стає структурування інформації у ІП.

Сформулюємо тезисно відповіді на ці два питання, які були поставлені. Інформаційний потік, що контролюється, переважно передаватиметься у відкритому вигляді (для безпосереднього подальшого опрацювання) з подальшою обов'язковою обробкою СКЦДІ у СУПР.

За наявності такого функціонуючого механізму, у разі нападу на передачу інформацію своєчасне виявлення цього факту надасть додаткові можливості щодо запобігання подальшому розвитку негативних подій.

Висновки

На основі проведеного дослідження можна зробити такі висновки. Розгляд особливостей функціонування існування інформації в електронному вигляді дає змогу виділити такі риси інформаційної моделі реєстрації даних у ІП СУПР.

Трансляція інформації в мережах телекомунікацій відбувається у вигляді інформаційних потоків, класифікація яких залежить від сприйняття їх оператором (текстові, графічні, відео та службові потоки: кодування архівація, стиснення) та характеризується внутрішньою структурою формату потоку. Елементарною структурною одиницею потоку є файл, який будується з однотонних даних.

Інформація в сучасних СУПР часто може піддаватися несанкціонованій модифікації (прояви тероризму). Найуразливішим із основних етапів життєвого циклу інформації є її поширення між операторами (користувачами) у ІП.

Розглядаючи питання захисту ІП СУПР та самої системи, доцільно використовувати чотирирівневу градацію доступу до інформації, що зберігається, обробляється та захищається у СУПР.

Стосовно інформації необхідно виділити методи реалізації загроз на кожному рівні. Характеристика потенційних зловмисників припускає їхніх високий досвід та кваліфікацію, а також передбачається, що за місцем здійснення дій зловмисника можуть одержати доступ до засобів адміністрування СУПР та засобів управління комплексною системою захисту.

Дія моделі реєстрації даних поширюється на рівень аутентифікації файлів. Виділені критичні параметри файлу, що схильні до модифікації. Це як зовнішні, так і внутрішні файли.

Визначені умови функціонування моделі реєстрації даних, які поширюються на рівень аутентифікації файлів.

Список літератури

1. Ленков, С.В. Методы и средства защиты информации в 2-х томах / Ленков С.В., Перегудов Д.А., Хорошко В.А.-К.: Арий, 2008.
2. Бурячок, В.Л. Політика інформаційної безпеки / Бурячок В.Л., Грищук Р.В., Хорошко В.О.-К.: ПВП «Задруга», 2014.-222с.
3. Кобозева, А.А. Аналіз захищеності інформаційних систем / Кобозева А.А., Мачалін І.О., Хорошко В.О.-К.: Вид ДУІКТ, 2010.-316С.
4. Иванченко, Е.В. Модель и метод оценки эффективности организации процесса функционирования систем воздушного движения / Иванченко Е.В., Орехов А.Н., Хорошко В.А. // Сучасний захист інформації, Спец. Випуск, 2013.-с. 73-81.
5. Капустян, М.В. Оценка эффективности функционирования сложных систем / Капустян М.В., Хорошко В.А. // Інформаційна безпека, №1, 2011.-с. 5-8.

МОДЕЛИ УГРОЗ ИНФОРМАЦИОННОМУ ПРОСТРАНСТВУ СУВД И МЕХАНИЗМЫ ЕГО ЗАЩИТЫ

А.М. Орехов, В.А. Хорошко

Национальный авиационный университет,
пр. Космонавта Комарова, 1, Киев, 03058, Украина; e-mail: professor_va@ukr.net

Рассмотрен жизненный цикл информации в системе управления воздушным движением, которая находится в информационном пространстве и требования к системе защиты. На их основе определен перечень классов угроз и внутренних и внешних злоумышленников. С учетом исследования создания модель угроз информации.

Ключевые слова: системы управления воздушным движением, системы защиты информации, информационное пространство

AIR-TRAFFIC CONTROL SYSTEM CYBERSPACE: MODELS OF THREATS AND PROTECTION MECHANISMS

A.M. Orehov, V.O. Khoroshko

National Aviation University,
1, prosp. Kosmonavta Komarova, Kiev, 03058, Ukraine; e-mail: professor_va@ukr.net

Lifecycle of air-traffic control system information related to cyberspace, as well as requirements to the protection system were discussed. On this basis, a list of classes of both the threats and external and internal intruders was identified and a model for cyberspace threats was developed.

Keywords: air-traffic control system, information protection systems, cyberspace