УДК 004.056.53 DOI: 10.30748/soi.2017.148.24

М.О. Мельник, Г.Д. Нікітин, К.О. Мезенцева

Одеський національний політехнічний університет , Одеса

АНАЛІЗ ПОБУДОВИ МОДЕЛІ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

В роботі було розглянуто основні моделі політик та типів політик інформаційної безпеки. В результаті цього було виявлено, що в залежності від особливостей організації можна реалізувати ту чи іншу модель політики безпеки, яка дозволить захистити дані компанії від несанкціонованого доступу, а також зменшить втрати компанії у випадку дій з боку співробітників компанії, які можуть нанести шкоду організації.

Ключові слова: *політика безпеки, кібербезпека, моделі загроз, моделі безпеки, інформаційна безпека.*

Вступ

Важливу роль в забезпеченні кібербезпеки будь-якої організації відіграє політика безпеки, яка організована в ній. Визначити інформацію, що потребує захисту, та рівень втрат від несанкціонованого спотворення, руйнування чи поширення інформації з боку третіх осіб, під силу саме тій особі, що має чітке уявлення мети організації, а також розуміє ті умови, в яких вона функціонує.

Визначивши політику безпеки, потрібно вирішити питання стосовно технології, що буде використана для її реалізації в автоматизованому контурі. Розробка деякої формальної моделі, що дає можливість ефективно програмувати на любій формальній мові, дозволяє реалізувати норми та правила політики безпеки, що сформульовані в термінах природної мови.

Політику безпеки інформаційної системи необхідно формалізувати з метою опису поглядів керуючої гілки компанії на суть загроз інформаційній безпеці організації, а також на технології, за допомогою яких можна забезпечити безпеку її інформаційних ресурсів. Для політики безпеки можна визначити дві основні частини. Перша з них – загальні принципи роботи з інформаційними ресурсами (базами даних) для кожної із категорій користувачів. Друга – чітко визначені правила такої роботи. При побудові політики безпеки потрібно розуміти, що вона завжди буде компромісом між рівнем захищеності інформаційних ресурсів системи, який ми бажаємо отримати, тим, на скільки зручно користувачам буде працювати із системою і, звичайно тією витратою коштів, що необхідні для її експлуатації.

Оформлення політики безпеки повинно проводитись документально з розділенням на певну кількість рівнів управління. Документ, в якому визначені відповідальні за реалізацію політики безпеки, її цілі та структура повинен бути визначений для найвищої ланки керівництва. Деталізація основного документу відбувається адміністраторами безпеки інформаційних систем, які повинні враховувати принципи діяльності організації, наявність ресурсів, а також співвідношення важливості цілей, які прагне досягнути компанія, реалізувавши політику інформаційної безпеки. В результаті необхідно отримати детальні рішення, що будуть складатись із ясно визначених методів захисту різних типів ресурсів (технічних, інформаційних) та інструкцій, які визначають поведінку співробітників у певних ситуаціях.

Метою статті є аналіз основних моделей політик безпеки та типів політик інформаційної безпеки. На основі аналізу виявити залежність від особливостей підприємства, яку можна реалізувати модель політики безпеки. Вибрана модель повинна дозволити захистити дані компанії від несанкціонованого доступу, а також зменшить втрати компанії у випадку дій з боку співробітників компанії, які можуть нанести шкоду організації.

Основна частина

Почнемо розгляд з моделі Bell-LaPadula (BLP) [1]. Дана модель заснована на політиці конфіденційності і визначає поняття захищеного стану. В цілому модель BLP стала першою значною моделлю політики безпеки, яка застосовується для комп'ютерів, і до сих пір в зміненому вигляді застосовується у військовій галузі. Модель повністю формалізована математично. Основний упор в моделі робиться на конфіденційність, але крім неї фактично більше нічого не представлено. Ще з недоліків моделі варто відзначити неможливість передачі інформації від вищого рівня до нижніх, оскільки це значно знижує можливості управління суб'єктами. В рамках моделі можливе створення незахищених систем.

Наступна модель називається моделлю Biba [2]. Вона є першою спробою створення інтегрованої моделі. Основні відмінності від попередньої моделі в наявність рівнів інтеграції, і наявності додаткової властивості (властивості виклику). Дана властивість відповідає за можливість суб'єкта посилати сервісні запити. Інші властивості схожі з попередньою моделлю, тільки в них йде прив'язка до рівня інтегра-

ції, на якому знаходиться об'єкт і суб'єкт (у попередній моделі рівні класифікації).

Набір правил моделі Clark-Wilson (CW) [3] розроблений таким чином, щоб в повній мірі була забезпечена безпека і підзвітність переходів у системі за рахунок вибору необхідного для такої ситуації режиму роботи з даними. Головне досягнення цих правил в порівнянні з моделлю Біба – поділ процедур з перевірки цілісності і процедур зміни. Дозволяє запобігти або виправити більшість нелегальних дій, що здійснюються зсередини комерційної організації.

Дискреційна (матрична) модель [4].

Розглянемо так звану матричну модель захисту (її ще називають дискреційною моделлю). Вона, на момент написання статті була самою розповсюдженою на практиці. Стан системи захисту можна описати наступною трійкою (на основі термінів матричної моделі):

$$(S, O, M), \qquad (1)$$

де S – безліч суб'єктів, які є активними структурними елементами моделі; O – безліч об'єктів доступу, є пасивними захищеними елементами моделі. Для ідентифікації об’єкта використовується його ім’я; M – матриця доступу. Для визначення права доступу суб'єкта до об'єкта використовується значення елемента матриці M. Звернення до різних типів об’єктів доступу з боку суб’єкта необхідно здійснювати, керуючись правами доступу, в яких описані способи такого звернення. Зазвичай права доступу суб'єктів до файлових об'єктів визначають як читання (R), запис (W) і виконання (E).

Аналіз рядка матриці доступу за зверненням суб'єкта до об'єкта береться за основу реалізації управління доступом. Він проводиться наступним чином, а саме: для перевірки обирається відповідний до об’єкта рядок матриці. Під час перевірки визначається наявність необхідних прав доступу для суб’єкта. По результатах перевірки робиться відбувається надання чи заборона доступу.

Наочність і гнучкість налаштувань політики доступу до ресурсів у матричних моделях є їх великим плюсом, але на противагу йому встає ряд недоліків такої моделі. До них можна віднести зайвий деталізований рівень опису відносин суб'єктів і об'єктів. Він призводить до підвищення складності адміністрування системи захисту під час завдання параметрів і їх підтримці в актуальному стані при включені до схеми розмежування доступу нових елементів (об'єктів чи суб'єктів, чи і тих і інших одночасно). В результаті ми отримаємо ризик допустити достатньо багато помилок при адмініструванні. Виходячи з цього цей недолік можна назвати основним для дискреційної моделі.

Коли мова йде про велику кількість користувачів, то традиційні підсистеми управління доступом потрібно адмініструвати, використовуючи об’єктно-орієнтовані рішення, що дозволяють знизити складність адміністрування. Це необхідна міра, тому що число зв'язків пропорційно добутку кількості користувачів на кількість об'єктів, що робить процес адміністрування надскладною задачею.

Є кілька різновидів об’єктно-орієнтовані рішень. Наприклад: рольове управління доступом (РУД). Реалізується воно шляхом додавання проміжних сутностей (ролей) між користувачами та їх привілеями. Це дозволяє користувачу в різні проміжки часу мати різні права, за рахунок зміни ролі. Один користувач може мати кілька ролей.

При використанні рольового доступу можна спростити процес адміністрування системи, оскільки збільшення його складності при зростанні кількості користувачів відбувається значно повільніше. Досягається це за рахунок абстрагування від конкретних видів і способів перевірки прав користувачів та встановлення зв’язків між ролями. Ролей в такому випадку потрібно значно менше, ніж значно менше, ніж користувачів. Відповідно число зв'язків, які потрібно адмініструвати стає пропорційним сумі, а не добутку кількості користувачів і об'єктів.

У 2001 році Національний інститут стандартів і технологій США запропонував проект стандарту рольового управління доступом [4].

Створивши роль, ми можемо визначити для неї права доступу та зв’язати з нею користувача. За рахунок цього між користувачем та його правами отримаємо відносини "багато до багатьох". Великій кількості користувачів можна надати одну і ту саму роль або кілька ролей одному користувачу. Коли користувач починає сеанс роботи, то активізуються одразу всі його ролі. В результаті він отримує усі права, від кожної із ролей, разом. Кожен користувач в один момент часу може мати не обмежену кількість сеансів.

У випадку необхідності можна встановити спадкування між ролями. Воно дозволяє ролі, що є спадкоємицею отримати всі права від ролі спадкодавця і доповнити її тими правами, які необхідні для комплексної реалізації створеної ролі. Можна провести відповідність ролей у РУД та класів у об’єктно орієнтованому програмуванні (ООП). Права доступу у РУД, в такому випадку, відповідають методам класів в ООП, а користувачам – об’єкти.

Робити спадкування ми можемо з будь-якою глибиною ієрархії, причому права доступу будуть більшими для тих користувачів, у яких ця глибина більша. Причому кожна роль може успадковувати права у будь-якої кількості ролей і надавати у спадок свої права також не обмеженій кількості інших ролей.

Спадкування починається з найвищого рівня абстрагування. При побудові політики інформаційної безпеки вищою ланкою абстракції буде співробітник компанії, а далі, в залежності від особливостей роботи будуть створюватись додаткові ролі з більш

розширеними правами. Надаючи права тій чи іншій ролі, необхідно чітко розуміти ті обов'язки, які вона виконує. Роль керівника не означає необмежені права. Вони в такій ролі просто не потрібні.

Важливим принципом інформаційної безпеки є поділ обов'язків. Він може бути як статичним, так і динамічним.

При статичному розподілу ролей користувач, фіксовано приписується до однієї ролі і не може бути після цього приписаний до множини інших ролей. В такому розподілі реалізація відбувається в наступному вигляді, а саме: створюється визначена кількість ролей із однаковими правами (не менше двох) і до них приписується визначена кількість співробітників (також не менше двох). Таким чином створюється пара: багато ролей – число. Наприклад в компанії може існувати три ролі адміністратора і десять адміністраторів. Тоді число буде дорівнювати чотирьом.

Додаючи успадкування, потрібно слідкувати за тим, щоб кількість співробітників, що отримують ролі не перевищила ту, що зафіксована у політиці безпеки організації, причому відслідковувати її необхідно по всій ієрархічній гілці.

У динамічному розподілені обов'язків є одна особливість, що відрізняє його від статичного. При ньому розглядаються ролі, що одночасно активні для даного користувача. Наприклад один користувач може мати ролі вантажника і водія, але не одночасно. Водій повинен привезти машину на місце, підготувати її для розвантаження. Потім перевдягнутися у форму вантажника і розвантажити її. Причому у формі вантажника він не може вести автомобіль. Так ми отримаємо тимчасове обмеження довіри за рахунок надання мінімальних привілеїв. Стандарт регламентує три функції, що необхідні для адміністрування РУД. До них відносяться функції адміністрування, що включають в себе створення нових ролей та супровід існуючих. Наприклад, створення чи видалення ролі чи користувача, надання користувачеві право участі у асоціації; створення нової асоціації чи видалення існуючої; створення нового відношення спадкоємства між ролями чи видалення існуючого; створення нової ролі, як спадкоємиці існуючої чи навпаки попередниці; видалення обмежень для статичного чи динамічного поділу обов'язків. Додатково до них можна віднести допоміжні функції, що використовуються для обслуговування сеансів роботи користувача. Наприклад, активація нової ролі користувача, перегляд роботи існуючого користувача, перевірка правомірності доступу.

Висновки

В роботі було розглянути основні моделі політик та типів політик інформаційної безпеки. В результаті цього, можна зробити висновок, що в залежності від особливостей організації можна реалізувати ту чи іншу модель політики, яка дозволить захистити дані компанії від несанкціонованого доступу, а також зменшить втрати компанії у випадку дій з боку співробітників компанії, які можуть нанести шкоду організації.

Таким чином, наведена інформація може використовуватись як основа для розробки політики безпеки не тільки приватних підприємств але і вищих учбових закладів.

Для реалізації цієї мети авторами було обрано три моделі. Наприклад, для розробки політики безпеки ВНЗ Ми будемо використовувати третю з них, а саме модель CW, тому що ми робимо припущення, що ця модель буде найбільш ефективна.

Список літератури

1. Петров А.А. Компьютерная безопасность. Криптографические методы защиты информации / А.А. Петров. – М.: ДМК, 2000. –- 448 с.

2. Милославская Н.Г. Интрасети: доступ в Internet, защита: Учебное пособие для вузов / Н.Г. Милославская, А.И. Толстой. – М.: ЮНИТИ – ДАНА, 2000. – 527 с.

3. Зегджа Д.П. Основы безопасности информационных систем / Д.П. Зегджа, А.М. Ивашко. – М.: Горячая линия – Телеком, 2000. – 452 с.

4. Ярочкин В.И. Служба безопасности коммерческого предприятия / В.И. Ярочкин. – М.: Ось-89, 1995. – 144 с.

Надійшла до редколегії 6.03.2017

Рецензент: д-р техн. наук проф. В.В. Скачков, Військова академія, Одеса.

АНАЛИЗ ПОСТРОЕНИЯ МОДЕЛИ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

М.А. Мельник, Г.Д. Никитин, К.А. Мезенцева

В работе были рассмотрены основные модели политик и типов политик информационной безопасности. В результате этого было выявлено, что в зависимости от особенностей организации можно реализовать ту или иную модель политики безопасности, которая позволит защитить данные компании от несанкционированного доступа, а также уменьшит потери компании в случае действий со стороны сотрудников компании, которые могут нанести вред организации.

***Ключевые слова**: Политика безопасности, кибербезопасность, модели угроз, модели безопасности, информационная безопасность.*

ANALYSIS CONSTRUCTION OF THE MODEL POLICY INFORMATION SECURITY OF THE COMPANIES

M. Melnyk, G. Nikitin, K. Mezenceva

The problems of The main types of model policies and information security policy. As a result, it was found that depending on the characteristics of the organization can implement a particular model of security policy that will protect company data from unauthorized access and reduce losses in the case of actions by employees, which may harm the organization.

***Keywords:** the security policy, the cyber security, the threat model, the security model, the information security.*