УДК 004.056

Кондратенко Ю. В.;
Зотова І. Г.;
Грицюк В. В.

Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, Київ

Візуальний аналіз політик безпеки в ERP-системах

Резюме. Стаття розкриває можливості, переваги та недоліки візуалного аналізу стану політик безпеки, встановлених в ERP-системах підприємств, враховуючи здатності людського візуального сприйняття всесвіту та можливостей сучасних інформаційних технологій.

Ключові слова: візуальний аналіз; ERP-система; аналіз політик безпеки; візуалізація політик безпеки; модель RBAC.

Постановка проблеми. Візуальний аналіз інформаційних систем на наявність проблем у налагодженні політики безпеки дає можливість адміністратору провести екстракцію корисних даних з великої кількості надлишкової і одночасно зашумленої інформації журналювання безпеки.

На сьогодні існує достатня кількість програмного забезпечення, яке дає змогу проводити аналіз стану ефективності використання мережевої інфраструктури, але не політики безпеки в підприємстві в цілому. Суть їх полягає у збалансованому поєднанні фізичних властивостей людини щодо візуального сприйняття предметів і явищ реального світу та використання можливостей сучасних інформаційних технологій [1, 2] для аналізу загального стану мережі, виявлення наявності аномалій, пов'язаних із надмірним перевантаженням та підозрілою активністю кінцевих користувачів, фактів несанкціонованого доступу та використання vpn-з'єднань тощо.

На основі отриманих результатів візуального аналізу маємо оцінку захищеності комп'ютерних мереж, яка в графічному вигляді відображає найбільш вразливі вузли інформаційної системи [4]. Використовуючи певні методики та моделі, які будуть зазначені в матеріалах цієї статті, для проведення візуального аналізу встановленої політики безпеки в ERP-системах підприємства, є можливим в подальших дослідженнях сформувати шаблони атак залежно від початкових умов та, на основі отриманих результатів, відповідним чином сформувати перелік заходів щодо забезпечення безпеки інформаційної системи.

Аналіз останніх досліджень і публікацій. Аналізуючи існуючий стан використання механізмів візуалізації безпеки саме в секторі IT, наявність наукових досліджень з проблематики цих питань, дійшли до висновку, що зазначена тематика не набула широкого вивчення. У роботі [5] для графічного відображення інформації було запропоновано підхід, у якому усі події, пов'язані з безпекою системи, відображено на колах, радіус яких відповідає шкалі часу. Події мають різне забарвлення, яке характеризує їх за певними ознаками, визначеними як вихідні дані. Для того, щоб визначитись з вихідними даними для проведеного аналізу, розберемося в поняттях політики безпеки та їх використанні в інформаційних системах планування ресурсами як в Збройних Силах України, так і в цивільному секторі.

В ERP-системі, яка впроваджується або вже функціонує, для задоволення вимог політики безпеки повинні бути реалізовані такі аспекти:

- аутентифікація користувачів;
- авторизація входу;
- аудит та журналювання подій;
- цілісність даних;
- конфіденційність.

Для цього в системі пропонуються такі сервіси:

- правила ведення паролів;
- моніторинг несанкціонованого доступу в систему;
- відповідне реагування на несанкціонований доступ.

SAP пропонує такі сервіси із захисту авторизації:

- перевірка повноважень;
- інструментарій щодо ведення ролей;
- інформаційна система з питань авторизації;
- механізми трасування.

Щодо проведення аудиту та журналювання активності користувачів, у системі ERP реалізовані такі сервіси:

- інформаційна система аудиту (AIS);
- журнал аудиту безпеки;
- журнали додатків та ведення таблиць бази даних.

Метою статті є проведення дослідження методики візуального аналізу політик безпеки в ERP-системах, порівняння з існуючими методиками, виявлення переваг та недоліків.

Виклад основного матеріалу. Основою для організації процесу розроблення інформаційно-безпечних технологій захисту інформації є політика безпеки. Політику безпеки необхідно сформулювати для того, щоб визначити, від яких саме загроз і яким чином захищається інформація в автоматизованій системі.

Під політикою безпеки розуміється набір правових, організаційних і технічних заходів щодо захисту інформації. Політика безпеки повинна бути оформлена у вигляді спеціального документа (або комплекту документів), з яким повинні бути ознайомлені всі користувачі системи.

З одного боку, політика безпеки інформує користувачів про те, як правильно експлуатувати систему, з іншого - визначає безліч механізмів безпеки, які повинні існувати в автоматизованій системі. Політика безпеки автоматизованої системи при розробленні інформаційно-безпечних технологій може складатися з множини приватних політик, спрямованих на конкретні аспекти захисту інформації.

При розробленні політики безпеки інформаційно-безпечних технологій необхідно керуватися такими правилами:

- кожна операція, описана політикою безпеки високого рівня, повинна підтримуватися політикою безпеки низького рівня;
- жодна з операцій, дозволених політикою безпеки вищого рівня, не повинна бути виключена при описанні політики безпеки вищого рівня.

Для того, щоб сформулювати політику в формі високорівневих специфікацій розмежування доступу, необхідно описати властивості суб'єктів та об'єктів організації, а також можливі операції суб'єктів системи над об'єктами. Суб'єкти в системі можна охарактеризувати за допомогою таких понять [3]:

- ступінь довіри до суб'єкта – використовується при доступі суб'єктів до інформації з урахуванням класифікації інформаційних ресурсів;
- необхідність доступу суб'єкта – атрибут вказує, що користувач повинен мати доступ до інформаційного ресурсу;
- роль, що виконується суб'єктом, – використовується при описанні функцій користувача системи і відповідних повноважень цього користувача;
- групи, до яких відноситься суб'єкт, – використовуються при групуванні користувачів з однаковими привілеями.

У свою чергу, у об'єктів можуть бути такі характеристики:

- позначка чутливості об'єкта – використовується при класифікації информаційних ресурсів. Коректна класифікація ресурсів забезпечує максимальну вартість інформації для організації. У цьому прикладі вся інформація, що створюється користувачем, повинна мати одну з таких категорій: "конфіденційна", "для службового користування", "публічна";
- ідентифікатор об'єкта – може використовуватися для визначення джерела інформації або її власника;
- мітки і атрибути об'єкта, які використовуються дискреційною політикою доступу (списки контролю доступу, біти захисту тощо).

Як основні операції, що виконуються суб'єктами системи над об'єктами, можна виділити такі:

- створення об'єктів і завдання атрибутів доступу до них, у тому числі класифікація об'єктів;
- періодичне коригування класифікації об'єктів, класифікація інформаційних ресурсів із плином часу зменшується (конфіденційна інформація може перетворитися на інформацію для службового користування, а інформація для службового користування – на публічну); якщо користувач, який створює інформацію, знає дату коригування класифікації інформації, він може зробити мітку "конфіденційна до ...";
- знищення об'єктів;
- читання інформації з об'єктів;
- запис інформації в об'єкти;
- копіювання об'єктів тощо.

У статті досліджено основні механізми забезпечення інформаційної безпеки ERP-систем. Ці системи є пакетом програм, що призначений для управління, балансування і оптимізації ресурсів підприємства. Вони забезпечують загальну модель даних і процесів

для всіх сфер діяльності Збройних Сил України. Розглянуто основні аспекти безпеки при роботі із системами, що реалізовують ERP-стратегію. Нині для забезпечення інформаційної безпеки в ERP-системах, крім штатних засобів захисту інформації, використовуються додаткові програмні засоби, в тому числі криптографічні, щоб виконати всі вимоги з інформаційної безпеки.

Розглянуто мережеву безпеку ERP-систем, безпеку на рівні бази даних, рівні сервера додатків і призначеному для користувача рівні уявлення, а також питання про надання доступу користувачеві на основі моделі RBAC.

ERP (англ. Enterprise Resource Planning, планування ресурсів підприємства) – це організаційна стратегія інтеграції виробництва, управління трудовими ресурсами, фінансового менеджменту і управління активами. ERP орієнтована на безперервне балансування та оптимізацію ресурсів, які перебувають на обліку в Збройних Сила України чи підприємства, за допомогою спеціалізованого пакета прикладного програмного забезпечення, який забезпечує загальну модель даних і процесів для всіх сфер діяльності.

В ERP-системі, як в центральній інформаційній системі, зосереджена велика кількість конфіденційної інформації. Наприклад, фінансова інформація, дані про бази забезпечення чи заводи по виробництву озброєння та військової техніки, кадрові дані тощо. Розкриття такої інформації може принести національним інтересам України значних збитків. Тому проблеми інформаційної безпеки особливо актуальні для ERP-систем [6].

Завданнями інформаційної безпеки ERP-систем є:

- зменшення ризиків втрати/розкриття інформації;
- відповідність державним і внутрішньокорпоративних нормам захисту інформації;
- захист цілісності даних;
- гарантія конфіденційності внутрішньої інформації організації.

Інформаційну безпеку необхідно забезпечити для всіх компонентів ERP-системи, тому розглянемо її архітектуру.

Сучасна ERP-система складається з трьох компонентів, пов'язаних через клієнт-серверну архітектуру (рис. 1).

Виділяють такі рівні ERP-системи:

- рівень бази даних (БД);
- рівень додатків;
- рівень представлення (призначений для користувача).

Зберігання даних здійснюється в базі даних (рівень БД), їх обробка виконується на сервері додатків (рівень додатків), а безпосередня взаємодія з користувачем відбувається через клієнтську програму (рівень представлення). Як така програма останнім часом використовується і клієнтський додаток GUI, і звичайний веб-браузер.

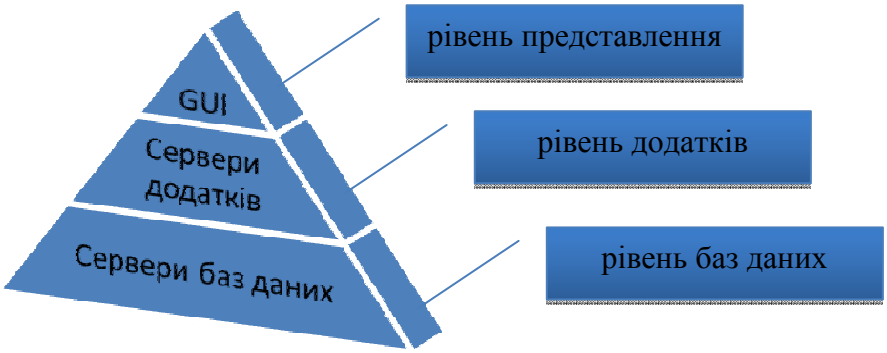

Рис. 1. Типова трирівнева архітектура ERP-системи

Забезпечення у тій чи іншій мірі захищеності інформації можливо на кожному з цих рівнів.

У SAP ERP безпарольна аутентифікація і шифрування каналів зв'язку реалізуються з використанням механізму SNC (Secure Network Communications) при обміні даними за протоколом DIAG, і протоколом SSL/TLS при обміні даними по HTTP/FTP [7].

Одним з найважливіших компонентів будь-якої ERP-системи є СУБД. Необхідно жорстко обмежувати доступ до фізичних серверів і компонентів обладнання. Операційна система, під якою функціонує СУБД ERP-системи, теж повинна бути налаштована таким чином, щоб доступ до БД був відкритий тільки серверу додатків. Жоден користувач ERP-системи не повинен мати прямого доступу до

бази даних [7], тільки через транзакційну систему.

На сервері додатків відбувається обробка даних, і тим самим він забезпечує авторизацію користувачів, тобто забороняє або дозволяє доступ до різних об'єктів ERP-системи [6].

У більшості сучасних ERP-систем застосовується модель RBAC (Role-Based Access Control, керування доступом на основі ролей) для того, щоб дозволити користувачам виконувати тільки певні транзакції і отримувати доступ лише для цього бізнес-об'єкта. У моделі RBAC рішення про надання доступу користувачеві приймаються на основі функцій, які користувач виконує в організації [8]. Роль можна представити як сукупність транзакцій, які користувач або група користувачів можуть виконувати в організації для забезпечення виконання бізнес-задач. Транзакція – це деяка процедура з перетворення даних у системі, та дані, над якими цю процедуру можна виконувати. Роль, що призначена користувачеві, складається з набору повноважень, і саме наявність необхідного повноваження перевіряє сервер під час виконання транзакції. Таким чином, наявність повноважень дає змогу досягти необхідного рівня деталізації в розмежуванні доступу.

Останнім кроком захисту інформації є безпосередньо робоче місце користувача, тобто клієнтський комп'ютер. Як показує світова практика, більшість злочинів у сфері IT відбувається самими співробітниками організації, а не зовнішніми зловмисниками [6].

З погляду політики безпеки в ERP-системах критичним місцем є вхід користувача в систему, тобто його аутентифікація та подальша авторизація. Традиційний підхід передбачає, що у користувача є логін і пароль для входу в ОС, а також логін, пароль та відповідна роль для входу в ERP-систему та виконання функціональних задач. Альтернативою традиційному підходу може служити аутентифікація користувача за допомогою цифрових сертифікатів, виданих в акредитованих центрах сертифікації ключів Збройних Сил України АЦСК ЗСУ, тим більше що ті чи інші механізми на основі інфраструктури відкритих ключів PKI присутні в більшості сучасних ERP-систем.

Перераховані механізми забезпечення захисту становлять основу політики безпеки ERP-систем.

Враховуючи сказане, проведемо аналіз параметрів політики безпеки ERP-системи, як таку було використано відому програмну платформу компанії SAP AG – SAP ERP. Використовуючи вбудований інструментарій адміністратора безпеки отримали певний перелік даних, які характеризують критичні події в системі, та використовуючи методику візуалізації проведемо їх аналіз.

На приведеному вище результаті вивантаження (рис. 2), ми можемо побачити активність користувачів, які виконують щоденну роботу в системі SAP ERP, пов'язану зі створенням, обробкою, редагуванням та збереженням даних. Цю інфомацію можливо отримати виконуючи транзакцію *SM20*.

Журнал безпеки відображає усі події, які виконуються як системними користувачами (вбудованими в систему розробником), так і створеними адміністратором безпеки для виконання функціональних обов'зків кінцевими користувачами. Як ми бачимо ця сукупність містить багато корисної інформації з погляду безпеки, а саме час і дата проведення транзакції користувачем, з якого терміналу була виконання подія, код транзакції, що використовується для перевірки наявності повноважень на виконання цієї транзакції чи дії над даними у цій транзакціїї, яку саме програму було використано та результат її виконання, а також факт входу в систему користувачем чи відмови, у разі порушення вимог аутентифікації.

Зацікавленість викликає той факт, що всі події та помилки, які виникають у системі, відображаються різним кольором, що з користю можна використати під час методу візуального аналізу.

Для графічного подання інформації скористуємось підходом, запропонованим в роботі [5], де отримані події журналу безпеки ERP-системи відображені на колах, радіуси яких показує шкалу часу (рис. 3).

Як видно з діаграми, всі події пов'язані з такими критеріями, як рольовою моделлю розмежування доступу RBAC, мережевою активністю та процесом аутентифікації користувачів у систему. Кольором відображаються важливість подій з погляду політики безпеки, а саме зеленим – події які дають суто інформативний потік даних, необхідний для статистики та аналітики. Жовтим та коричневим кольорами визначаються події в системі, на які необхідно звернути увагу, здійснити аналіз причин виникнення, дійти відповідних висновків та прийняти рішення щодо подальшого їх

уникнення. Червоним кольором та бурим відображені події, які потребують негайного реагування. Серед прикладів таких подій можуть бути зміни в налагодженні системи, зміни в основних записах користувачів (заміна пароля, створення нового користувача в системі або видалення існуючого, злом програмно-апаратних засобів на мережевому рівні тощо).

Дата	Момент	Користувач	Терминал	Код транзакції	Программа	Текст сообщения контр. журнал
11.04.2018	10:53:03	SAPSYS			TASK_VITAL_RUN	Report TASK_VITAL_RUN Started
11.04.2018	10:53:03	548158DEE4D0	r3d		SAPMSSY1	RFC/CPIC Logon Successful (Type = R)
11.04.2018	10:53:03	548158DEE4D0	r3d		SAPMSSY1	Successful RFC Call TASK_VITAL_START_MONITORING (Function Group = TASK_VITAL)
11.04.2018	10:53:03	548158DEE4D0	r3d		SAPMSSY1	RFC/CPIC Logon Successful (Type = F)
11.04.2018	10:53:03	548158DEE4D0	r3d		SAPMSSY1	Successful RFC Call ENQUEUE_READ (Function Group = SENT)
11.04.2018	10:53:03	SAPSYS			RSWSRMEH	Report RSWSRMEH Started
11.04.2018	10:53:03	548158DEE4D0	r3d		SAPMSSY1	RFC/CPIC Logon Successful (Type = R)
11.04.2018	10:53:03	548158DEE4D0	r3d		SAPMSSY1	Successful RFC Call WSRM_DISPATCH (Function Group = WSRM_SOAP)
11.04.2018	10:53:03	SAPSYS			SSFALRTEXP	Report SSFALRTEXP Started
11.04.2018	10:53:04	O.ZINCHENCO	PS311006	SESSION_MANAGER	SAPMSYST	Logon Failed (Reason = 1, Type = A)
11.04.2018	10:53:24	O.CHELOB	PS311006	SESSION_MANAGER	SAPMSYST	Logon Successful (Type=A)
11.04.2018	10:53:25	O.CHELOB	PS311006	SESSION_MANAGER	RSRZLLG0	Report RSRZLLG0 Started
11.04.2018	10:53:25	O.CHELOB	PS311006	SESSION_MANAGER	RSRZLLG0_ACTUAL	Report RSRZLLG0_ACTUAL Started
11.04.2018	10:53:28	O.CHELOB	PS311006	PFCG	SAPLSMTR_NAVIGATION	Start of transaction PFCG failed (Reason=6)
11.04.2018	10:53:34	SAPSYS			RSBTCRTE	Report RSBTCRTE Started
11.04.2018	10:53:34	WF-BATCH			RSBTCRTE	Logon Successful (Type=B)
11.04.2018	10:53:34	SAPSYS			RSBTCRTE	Report RSBTCRTE Started
11.04.2018	10:53:34	IGNATENKO			RSBTCRTE	Logon Successful (Type=B)
11.04.2018	10:53:34	IGNATENKO			ZHROM_UPDATE_9004	Report ZHROM_UPDATE_9004 Started
11.04.2018	10:53:34	WF-BATCH			RSWWDHEX	Report RSWWDHEX Started
11.04.2018	10:53:34	WF-BATCH			RSWWDHEX_INTERNAL	Report RSWWDHEX_INTERNAL Started
11.04.2018	10:53:35	O.CHELOB	PS311006	SE80	SAPLSMTR_NAVIGATION	Transaction SE80 Started
11.04.2018	10:53:35	O.CHELOB	PS311006	SEU_INT	SAPMSEU0	Report SAPMSEU0 Started
11.04.2018	10:54:34	SAPSYS			RSBTCRTE	Report RSBTCRTE Started

Рис. 2. Кольорова візуалізація журналу безпеки

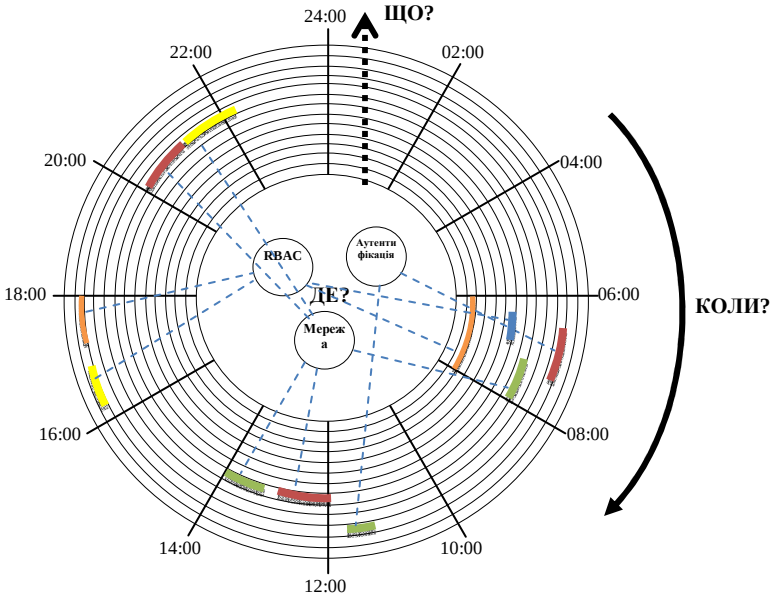

Рис. 3. Візуалізація політики безпеки ERP-системи

Нажаль запропонована модель візуалізації інформації не дає можливість у повній мірі провести оцінку коректності використання політик безпеки підприємства, оскільки вона лише дає дані щодо наявності небезпечних елементів у системі, а не причини їх прояву. Отже виникає нагальна потреба у додатковому аналізі отриманих результатів з можливістю подальшого формування варіантів для підтримки прийняття рішень у галузі безпеки.

Висновки. Враховуючи результати проведеного аналізу можна дійти висновку, що розглянута методика дає можливість адміністраторам безпеки по іншому сприймати отримані дані від інструментарію з надмірними даними, за рахунок людських якостей щодо візуального сприйняття. Але вона не дає змоги повною мірою проаналізувати стан політики

безпеки в інформаційній системі. Проте поєднання цієї методики з іншими, які також використовують можливості людського сприйняття в поєднанні з інформаційними технологіями, може привнести шалені результати. Тому інші методики та їх раціональне поєднання необхідно глибше дослідити у подальшому.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Новикова Е. С., Котенко І. В. Механізми візуалізації в SIEM-системах // Системи високої доступності. 2012. – № 2. – С. 91-99.
2. Новикова Е. С., Котенко І. В. Аналіз механізмів візуалізації для забезпечення захисту інформації в комп'ютерних мережах // Тр. СПІІРАН. 2012. – Вип. 4 (23). – С. 7-30.
3. Шаханова М. В. Современные технологии информационной безопасности: учеб. пособие / М. В. Шаханова. – Владивосток: Изд-во ДВГТУ, 2007. – 217 с.
4. Kotenko I., Chechulin A. Common Framework for Attack Modeling and Security Evaluation in SIEM Системс // 2012 IEEE Intern. Conf. on Green Computing анд Communications, Conf. on Internet of Things, анд Conf. on Cyber, Physical and Соціал Computing, Бесанçon, France, Nov. 20-23, 2012 / Los Alamitos, California. IEEE Computer Society, 2012. – P. 94-101.
5. Foresti S. et al. Visual Correlation of Network Алертс // IEEE Comput. Graph. АППЛ. 2006. – Vol. 26. Н 2. – P. 48-59.
6. Егорова Г. В., Шляпкин А. В. Информационная безопасность ERP-систем // Информационные системы и технологии: управление и безопасность. 2013. – № 2. – С. 202-211.
7. Kale V. Vnedrenie SAP R/3. Rukovodstvo dlya menedzherov i inzhenerov. M: Kompaniya AyTi, 2004. – 511 p.
8. Ненашев С. А. Криптографическая защита информации в ERP-системах компании SAP // Information Security/ Информационная безопасност, 2009. – № 3. – С. 24-25.
9. Петренко С. А., Курбатов В. А. Политики информационной безопасности. М.: ДМК Пресс, 2006. – 400 с.
10. Eyers D. M., Bacon J., Moody K. Oasis role-based access control for electronic health records // IEEE Software, 2006. – P. 16-23.
11. Sandhu R., Coyne E. J., Feinstein H. L., Youman C. E. Role-Based Access Control Models. // IEEE Computer, 1996. – 29 (2). P. 38-47.

Стаття надійшла до редакції 11.04.2018

Кондратенко Ю. В.;
Зотова И. Г.;
Грицюк В.В.

Центр военно-стратегических исследований Национального университета обороны Украины имени Ивана Черняховского, Киев

Визуальный анализ политик безопасности в ERP-системах

Резюме. Статья раскрывает возможности, преимущества и недостатки визуального анализа состояния политик безопасности, установленных в ERP-системах предприятий, учитывая способности людского визуального восприятия вселенной и возможностей современных информационных технологий.

Ключевые слова: визуальный анализ; ERP-система; анализ политик безопасности; визуализация политик безопасности; модель RBAC.

Y. Kondratenko;
I. Zotova;
V. Grytsyuk

Center of Military and Strategic Studies of the National Defense University of Ukraine named after Ivan Cherniakhovskyi, Kyiv

Visual analysis of security policies in ERP-systems

Resume. The article reveals the possibilities, advantages and disadvantages of visual analysis of the state of security policies established in the ERP systems of enterprises, taking into account the ability of the human visual perception of the universe and the possibilities of modern information technologies.

Keywords: visual analysis; ERP system; security policy analysis; security policy visualization; RBAC model.