КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1(13), 2021
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2021.13.5062
УДК 65.015.3:004.056

Мужанова Тетяна Михайлівна
к.держ. упр., доцент, доцент кафедри управління
інформаційною та кібернетичною безпекою
Державний університет телекомунікацій, Київ, Україна
ORCID: 0000-0002-7435-0287
muzanovat@gmail.com

Легомінова Світлана Володимирівна
д.екон.н., професор, завідувач кафедри управління
інформаційною та кібернетичною безпекою
Державний університет телекомунікацій, Київ, Україна
ORCID: 0000-0002-4433-5123
chiarasvitlana77@gmail.com

Якименко Юрій Михайлович
к.військ.н. доцент, доцент кафедри управління
інформаційною та кібернетичною безпекою
Державний університет телекомунікацій, Київ, Україна
ORCID: 0000-0002-6848-852X
yakum14@ukr.,net

Мордас Ірина Василівна
к.екон.н., доцент, доцент кафедри публічної політики
Навчально-науковий інститут публічного управління
та державної служби Київського національного
університету імені Тараса Шевченка, Київ, Україна
ORCID: 0000-0002-2908-7555
mordas_iv@ukr.net

ТЕХНОЛОГІЇ МОНІТОРИНГУ Й АНАЛІЗУ ДІЯЛЬНОСТІ КОРИСТУВАЧІВ У ЗАПОБІГАННІ ВНУТРІШНІМ ЗАГРОЗАМ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ОРГАНІЗАЦІЇ

Анотація. Зростання кількості інцидентів інформаційної безпеки, пов'язаних з діяльністю персоналу, частота яких за останні два роки збільшилася майже вдвічі, обумовила організації використовувати ефективні технології запобігання і протидії внутрішнім загрозам інформаційній безпеці. Важлива роль у цьому контексті належить інструментам моніторингу й аналізу діяльності користувачів. За оцінкою експертів, у найближчі роки такі технології будуть впроваджені у 80% рішень щодо виявлення загроз і встановлення пріоритетності інцидентів інформаційної безпеки. У статті розкрито сутність і проаналізовано функціонал декількох систем, які здійснюють моніторинг і аналіз поведінки працівників, зокрема систем запобігання втраті даних (DLP), контролю доступу, аналізу поведінки користувачів та IT-об'єктів (UBA/UEBA). Встановлено, що система DLP відстежує і звітує про спроби користувача передати конфіденційну інформацію шляхом здійснення контролю поштового і веб-трафіку, засобів бездротового доступу, зовнішніх накопичувачів, пристроїв введення і виведення, роботи ПЗ робочого місця користувача, аудіо- та відео нагляду за його діяльністю тощо. Засоби контролю доступу виконують, зокрема, функції моніторингу доступу і пересування особи у захищених зонах об'єкта, збору інформації з камер спостереження, ведення обліку робочого часу. В умовах пандемії розроблені рішення, які дозволяють ідентифікувати особу в масці на обличчі, виконувати функції відстеження стану здоров'я.
Аналіз функціональних характеристик систем поведінкової аналітики UBA/UEBA показав, що вони вирішують не тільки завдання щодо збору даних з усіх можливих доступних джерел (програмного й апаратного забезпечення, реєстраційних записів, листування користувачів тощо), але й аналізують зібрані дані і звітують про нетипову поведінку користувачів у разі її виявлення. Відзначено, що засоби поведінкової аналітики застосовують у цілому ряді

технологій безпеки, таких як системи управління інформацією і подіями безпеки, виявлення і запобігання вторгненням та інших, доповнюючи і розширюючи їхні можливості, сприяючи створенню комплексних практично всеохоплюючих рішень з інформаційної безпеки. Рекомендовано застосування засобів контролю й аналізу діяльності користувачів у різних варіантах поєднання або у складі комплексних рішень з управління інформаційною безпекою для досягнення належного рівня інформаційної безпеки в умовах зростання рівня загроз з боку персоналу.

Ключові слова: інформаційна безпека організації; внутрішні загрози інформаційній безпеці організації; запобігання втраті даних (DLP); контроль доступу; аналітика поведінки користувачів та IT-об'єктів (UBA/ UEBA).

ВСТУП

Статистика у сфері інформаційної та кібербезпеки беззаперечно свідчить про значний вплив людського чинника на стан захищеності інформаційно-телекомунікаційних систем та інформаційних ресурсів організацій. Так, відповідно до звіту компанії Verizon у 2020 році 22% порушень безпеки даних сталися внаслідок випадкових людських помилок, 22% - через застосування методів соціальної інженерії і 8% становлять випадки неправильного поводження з інформацією авторизованих користувачів [1]. А один зі звітів компанії IBM взагалі стверджує, що 95% порушень інформаційної безпеки викликані неналежною поведінкою людини або її помилками [2]. Крім того, за останні роки частота інцидентів, пов'язаних з внутрішніми загрозами, збільшилася на 47%. Такі порушення інформаційної безпеки включають як зловмисні крадіжки даних, так і випадки ненавмисної втрати інформації.

У зв'язку з цим аналіз загроз і розробка заходів щодо зниження рівня впливу персоналу на інформаційну безпеку організації є надзвичайно актуальними напрямами в сучасних умовах. З огляду на великий відсоток порушень інформаційної безпеки з вини персоналу важливим кроком є запобігання і протидія внутрішнім загрозам. Впровадження надійних технічних засобів захисту інформації є важливим кроком у зменшенні інсайдерських загроз. **Постановка проблеми.** Як свідчить практика, сьогодні традиційні засоби захисту такі як антивіруси, міжмережеві екрани, системи запобігання вторгненням та інші не здатні забезпечити цілковитий захист від внутрішніх порушників (інсайдерів), метою яких може бути передача інформації за межі організації для подальшого використання: продажу, передачі третім особам, опублікування у відкритому доступі тощо.

Щоб ефективно захистити свої активи і вчасно виявляти інсайдерські загрози організаціям варто крім зазначених вище засобів впроваджувати технології моніторингу й аналізу поведінки користувачів.

Аналіз останніх досліджень і публікацій. Дослідженням питань інформаційної безпеки підприємства, в тому числі ролі людського чинника у її забезпеченні, присвячені праці таких вчених, як В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа [3], І. О. Башинська [4], З. Б. Живко [5]. Декілька ґрунтовних робіт щодо визначення і класифікації інсайдерських загроз, встановлення видів внутрішніх порушників інформаційної безпеки та їхніх характеристик представлено колективами закордонних науковців [6], [7], [8]. Підходи і методи запобігання і протидії інсайдерським загрозам є предметом досліджень авторитетних експертних організацій у сфері інформаційної безпеки, таких як Інститут SANS, CERT та SIFMA [9], [10], [11]. Водночас, більшої уваги вимагає дослідження можливостей застосування програмних інструментів, метою яких є зменшення впливу людського чинника на процеси забезпечення інформаційної безпеки підприємства.

Мета статті - дослідити основні програмні засоби моніторингу й аналізу діяльності користувачів як інструментів запобігання й протидії внутрішнім загрозам інформаційній безпеці організації.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Сьогодні на ринку програмних рішень з інформаційної безпеки представлена велика кількість різних засобів моніторингу й аналізу діяльності користувачів, серед яких, на нашу думку, насамперед варто відзначити системи запобігання втраті даних, контролю доступу й аналізу поведінки користувачів.

Системи запобігання втраті даних (Data Loss Prevention). Вирішити проблему випадкових і навмисних витоків конфіденційних даних допомагають системи запобігання втраті даних (DLP - Data Loss Prevention). У загальному розумінні DLP – це здатність системи ідентифікувати, контролювати та захищати дані, що використовуються (наприклад, дії кінцевої точки), дані в русі (наприклад, дії мережі) та дані в стані спокою (наприклад, зберігання даних) за допомогою глибокої перевірки вмісту пакетів, контекстного аналізу безпеки транзакцій (атрибути) ініціатора, об'єкта даних, носія, часу, одержувача/місця призначення тощо) в рамках централізованої системи управління [12].

Система DLP - це технічно складне автоматизоване рішення, спеціальне програмне забезпечення, що відстежує спроби передачі конфіденційної або іншої важливої інформації з інформаційної системи за межі організації. На організаційний сервер і всі пристрої в офісі встановлюють програму, яка в режимі реального часу перевіряє всі операції з інформацією. У випадку виявлення факту відправлення критичної інформації на недозволену адресу система блокує передачу. Так, якщо працівник спробує надіслати таблицю Excel з контактами клієнтів з корпоративної пошти на особисту, DLP-система зупинить відправку і одразу повідомить про порушення відповідального фахівця.

Така система створює захищений «цифровий периметр» навколо організації, аналізуючи всю вхідну, вихідну і внутрішню інформацію. Виявлення конфіденційної інформації в потоках даних здійснюється шляхом аналізу змісту і виявлення спеціальних ознак: грифу документа, спеціально введених міток, значень хеш-функції тощо.

DLP-система вирішує завдання з контролю:

– поштового і веб-трафіку;
– переписки в месенджерах (Skype, Telegram, WhatsApp,);
– передачі даних в хмари (хмарні додатки);
– інформаційного обміну на робочих станціях працівника організації через комунікаційні порти (com-, lpt-, usb-, irda-порти тощо);
– пристроїв введення-виведення (cd, знімні накопичувачі і т.д.), засобів бездротового доступу (bluetooth, firewire, wi-fi), друку на локальних і мережевих принтерах;
– зберігання інформації на робочих станціях організації і в мережевих сховищах.

Також DLP-система забезпечує контроль дій співробітників на робочих станціях: контроль буфера обміну, кейлоггер, моніторинг відвідуваних сайтів, контроль пошукових запитів і використання додатків, контроль за робочим місцем користувача (аудіо, відео, скріншоти), тіньове копіювання всіх перехоплених файлів; консолідацію всіх перехоплених даних в єдиному сховищі та надання візуальної аналітики перехоплених даних.

ISSN 2663 - 4023

Розглянемо коротко основні функціональні модулі DLP-систем (Рис. 1) [13].

–Контроль організаційної пошти. У базі даних DLP зберігаються всі поштові повідомлення контрольованого користувача, навіть, якщо він видалив отримане або відправлене повідомлення. Система дозволяє проаналізувати перелік адресатів, яким користувач надсилав чи від яких отримував листи, і встановити, з ким і в якому обсязі він взаємодіє, дослідити текст листів на основі наявності певних словоформ.

–Контроль програм обміну повідомленнями. Усі повідомлення месенджерів контрольованого користувача можуть зберігатися в базі даних DLP. За налаштованими в DLP політиками і правилами відбувається реагування на певний контент, зокрема словоформи, й оповіщення оператора системи про підозрілі факти щодо певного користувача. Незважаючи на те, що обмін інформацією між клієнтом і сервером месенджера може відбуватися за допомогою засобів шифрування месенджера (або сторонніх), DLP-система отримує вихідні незашифровані дані, якщо вона підтримує відповідний месенджер.

–Контроль друку. Модуль дозволяє відстежувати файли, які користувач відправляє на друк, зберігаючи їх у базі даних DLP-системи, а також контролювати обсяги друку і збирати статистику.

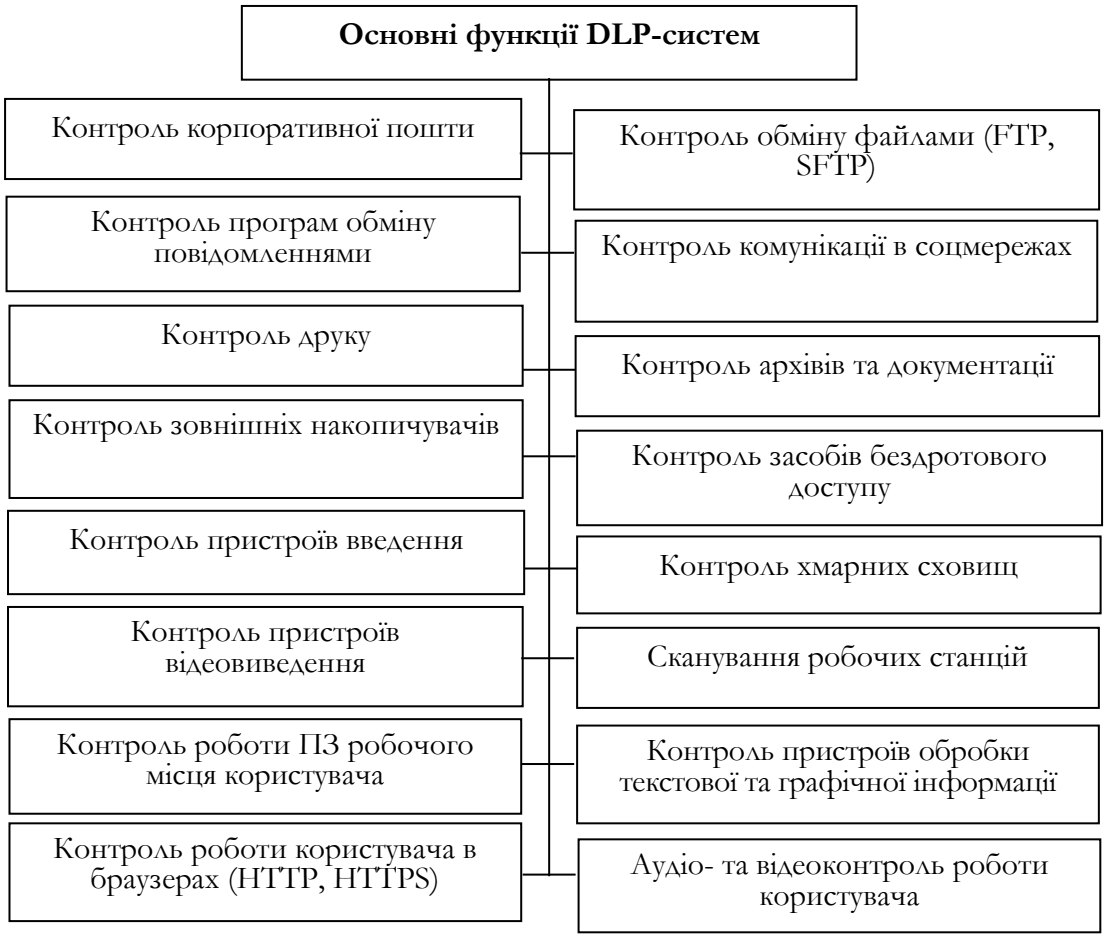

Рис. 1. Основні функції DLP-систем.

–Контроль зовнішніх накопичувачів. DLP-система розпізнає і фіксує під'єднаний до робочого місця пристрій (наприклад, накопичувач USB або DVD). У разі відповідного налаштування система здатна зашифрувати всі дані на заданих пристроях, зробити копію всієї інформації, що на них зберігається, або тільки файлів, які зчитуються або записуються. Цей модуль є корисним, оскільки значна частина витоків відбувається шляхом копіювання важливої інформації на переносні носії.

–Контроль пристроїв введення. Найчастіше це keylogger клавіатури і миші, які можуть фіксувати в базі даних DLP всі натискання на клавіатуру і рухи миші користувача. Найбільш просунуті DLP-системи при цьому надають можливість аналізувати визначені словоформи, забезпечують спрацьовування на них і оповіщення оператора DLP в консолі або електронною поштою.

–Контроль пристроїв відеовиведення. За наявності відповідних налаштувань система дозволяє з необхідною періодичністю проводити знімки монітора користувача із записом їх в базу DLP для подальшого перегляду й аналізу оператором.

–Контроль роботи ПЗ робочого місця користувача. Модуль здійснює фіксацію початку і закінчення використання користувачем певного ПЗ, що дозволяє отримати уявлення про активність користувача й оцінити ефективність його роботи. Таким чином, сучасна DLP-система є надійним засобом моніторингу й оцінки ефективності роботи персоналу.

–Контроль роботи користувача в браузерах (HTTP, HTTPS). Система фіксує всі сайти, які відвідував користувач, і час, проведений на кожному з них. Завдяки такому моніторингу можна встановити відсоток часу, коли працівник займається позаробочими справами у робочий час, і відстежити його деструктивні наміри.

–Контроль обміну файлами (FTP, SFTP). Модуль проводить запис копій файлів, переданих користувачем, і фіксує адреси одержувачів.

–Аудіо- та відеоконтроль діяльності користувача. Модуль аудіоконтролю дозволяє вести запис з мікрофону, підключеного до робочого місця користувача (наприклад, такого, який знаходиться в web-камері), за заданим розкладом або в центрі онлайн-контролю. Модуль відеоконтролю забезпечує відеозапис з камери, підключеної до робочого місця. Найчастіше обидва модулі використовуються спільно, забезпечуючи прослуховування і відеоспостереження за роботою працівника.

Як показав огляд основних функцій DLP-систем, крім свого основного завдання, пов'язаного із запобіганням витокам інформації, вони добре підходять для вирішення завдань щодо здійснення контролю дій персоналу, зокрема контролю використання робочого часу та робочих ресурсів, спілкування працівників про деструктивні наміри чи дії на шкоду організації, правомірності дій співробітників з інформаційними активами тощо.

Загалом використання DLP-системи дозволяє:

– виявити слабкі місця в безпеці до настання інциденту інформаційної безпеки;

– сформувати доказову базу і створити можливості для проведення розслідування інцидентів;

– забезпечити застосування санкцій до осіб, винних у витоку конфіденційної інформації;

– оптимізувати використання робочого часу персоналу;

– підвищити ефективність роботи підрозділу інформаційної безпеки за рахунок автоматизації роботи працівників щодо виявлення та реагування на інциденти інформаційної безпеки;

– здійснювати бізнес-розвідку з метою визначення ступеня лояльності працівників організації;

– мінімізувати економічні й репутаційні збитки за рахунок зниження ризиків витоку конфіденційної інформації з організації;

– покращити бізнес-процеси організації.

Системи контролю доступу (Access Control). Контроль доступу є одним із способів запобігання інсайдерським атакам. У загальному розумінні контроль доступу – це процес надання або відхилення конкретних запитів: 1) на отримання та використання інформації та пов'язаних з нею послуг з обробки інформації; та 2) для входу до конкретних фізичних приміщень [14]. Контроль доступу - це техніка безпеки, яка регулює, хто або що може переглядати або використовувати ресурси в обчислювальному середовищі. Існує два типи контролю доступу: фізичний та логічний. Фізичний контроль доступу обмежує доступ до будівель, приміщень та фізичних IT-активів. Логічний контроль доступу обмежує з'єднання з комп'ютерними мережами, системними файлами та даними.

Контроль доступу включає процеси ідентифікації й автентифікації особи та визначення рівня її доступу до інформаційних ресурсів системи на основі політики та процедур, встановлених організацією. Контроль доступу - це механізм, що має дві складові:

– автентифікацію, яка показує, ким є користувач і підтверджує наявність у нього певних повноважень на доступ до системи. Іншими словами представлення деякої комбінації того, що користувач знає (логіна, пароля), має (магнітної картки чи токена) і ким він є (наприклад, біометричні дані). У багатьох випадках також розглядають четвертий критерій - місце перебування користувача.

–авторизацію, яка визначає, чи достатньо у користувача облікових даних, щоб надати йому запитуваний тип доступу.

Система контролю доступу одночасно надає користувачеві достатні привілеї для виконання необхідних завдань, обмежуючи доступ відповідно до набору правил. Правила базуються на принципах найменших привілеїв (чим менше привілеїв надається користувачеві, тим краще), ескалації (дозволяє користувачеві додавати певні права) та розподілу обов'язків.

Система контролю доступу інтегрована в IT-середовище організації і може містити різні типи програмного забезпечення та технологій контролю доступу, які можуть бути в приміщенні, хмарі або на гібриді обох. Програмні засоби управління доступом можуть включати програми для звітування та моніторингу; інструменти управління паролями; засоби забезпечення контролю доступу; сховища ідентифікаторів; інструменти забезпечення політики безпеки. Одним із прикладів програмного забезпечення, яке включає більшість перелічених вище інструментів, є Microsoft Active Directory (AD). Серед інших постачальників продуктів для управління доступом є IBM, Idaptive та Okta.

Програмне забезпечення контролю доступу може містити також модулі, які виконують функції забезпечення контролю доступу до захищених зон об'єкта, збору інформації з камер спостереження, встановлених в приміщеннях і на прохідній, ведення обліку робочого часу. Водночас, враховуючи актуальні запити з боку кінцевих користувачів виробники систем контролю доступу просувають програмні продукти, які містять нові функції, зокрема використання мобільних облікових даних і додатків, безперебійного доступу і відстеження руху, розробку зрозумілих для користувача інтерфейсів, реалізацію настроюваних панелей моніторингу і поведінкової аналітики за

рахунок інтеграції програмного забезпечення управління доступом з ПЗ для відеоспостереження.

Як відзначалося, важливою функцією систем контролю доступу є облік робочого часу, завдяки чому є можливість забезпечити контроль за тривалістю роботи персоналу, що в подальшому допоможе прорахувати ефективність праці цілих відділів або конкретних людей. Постійний моніторинг робочого часу значно підвищує загальну продуктивність праці працівників організації, оскільки вони будуть витрачати менше часу на перерви й рідше відволікатися від робочих завдань, допомагає більш ефективно планувати робоче навантаження і прогнозувати точні терміни виконання завдань, а також забезпечує покращення інформаційної безпеки.

Розробники, намагаючись відповідати новим вимогам ринку в умовах пандемії COVID-19, пропонують рішення, які дозволяють запобігти проходу гостей без захисної маски, ідентифікувати особу в масці на обличчі, виконувати функції відстеження стану здоров'я. Так, за необхідності, система може бути оснащена термодатчиком і контролювати температуру тіла всіх відвідувачів.

Значною популярністю користуються системи нового покоління, які базуються на мобільних технологіях, наприклад NFC (Near field communication), яка є стандартом обміну даними на короткі дистанції до 10 см. NFC зв'язок працює між двома пристроями за умови, що обидва пристрої в активному режимі. Тому користувач легко може використовувати свій смартфон з NFC замість безконтактних карт і брелків. Крім цього, такі системи використовують різноманітні високоточні біометричні засоби розпізнавання обличчя, сітківки ока й дозволяють контролювати пересування працівників без використання перепусток чи магнітних карток [15].

Стеження за правомірним і дозволеним в організації використанням комп'ютерів та Інтернету за допомогою такої системи також входить в облік робочого часу. Завдяки цій функції керівні особи можуть визначити, як багато часу співробітники витрачають на марне блукання в мережі Інтернет, а також в разі потреби заблокувати ресурси, які створюють перешкоди продуктивності праці.

Системи аналітики поведінки користувачів та IT-об'єктів (UBA/UEBA). Загроз інформаційній безпеці організації з кожним роком стає все більше, вони стають більш витонченими і продуманими, а самі порушники – розумнішими. У такому світі контролювати і реагувати на інциденти інформаційної безпеки стає все складніше і дорожче. Тому перед індустрією інформаційної безпеки стоїть безліч завдань щодо автоматизації процесів визначення та реагування на внутрішні загрози. Одним із засобів вирішення таких завдань є системи аналітики поведінки користувачів (User Behavior Analytics - UBA).

Немає нічого нового у використанні аналітики для захисту даних та запобігання витоків. Міжмережеві екрани, наприклад, аналізують вміст пакетів та інші метадані для виявлення та блокування доступу зловмисників. Антивірусне програмне забезпечення постійно сканує файлові системи на наявність шкідливих програм, шукаючи фрагменти коду та інші ознаки зараження файлу.

Натомість UBA-система фокусується на діяльності користувача: запущені програми, мережева активність і найбільш важливі файли, до яких здійснюється доступ. Аналітика поведінки користувачів - це відстеження, збір і оцінка призначених даних і дій користувачів з використанням систем моніторингу.

Оскільки інсайдерські загрози найважче виявити і потенційно вони є найбільш шкідливими, UBA є цінним інструментом для виявлення підозрілої поведінки користувачів, що може свідчити про крадіжку даних, шахрайство або інші зловмисні дії.

ISSN 2663 - 4023

До найпоширеніших видів загроз, які може виявити UBA, належать:

–крадіжка даних: викрадення особистих або конфіденційних даних організації;

–перевищення привілеїв: зміна облікових даних доступу;

–зловживання привілейованим обліковим записом: неналежне використання дозволів на доступ;

–компрометація облікових даних: приховане захоплення облікових записів у зловмисних цілях;

–аномальна поведінка: доступ до зовнішніх доменів, віддалений доступ до ресурсів з високими привілеями, незвичні тривалість входу в систему, час або місце розташування.

Крім UBA-систем засоби поведінкової аналітики включають ПЗ для аналітики поведінки користувачів та IT-об’єктів (User&Entity Behavior Analytics - UEBA), оскільки предметом поведінкової аналітики може бути не тільки будь-яка людина, але й машина, яка взаємодіє з організацією, системою, платформою чи продуктом. UEBA-системи за допомогою алгоритмів машинного навчання і статистичного аналізу масивів даних про користувачів та IT-об’єкти (кінцеві станції, сервери, комутатори, додатки, системи зберігання даних і мережевого трафіку тощо) будують моделі їх поведінки і визначають відхилення від цих моделей як у режимі реального часу, так і в минулому.

Джерелами даних для UBA/UEBA можуть бути файли журналів серверних і мережевих компонентів, систем безпеки, локальні журнали з кінцевих станцій, дані з систем автентифікації і навіть зміст листування користувачів у соціальних мережах, месенджерах і поштою.

Незважаючи на те, що формально UBA і UEBA відносяться до одного класу систем, вони мають низку відмінностей. Так, в UEBA-системах передбачено профілювання та аналіз IT-об’єктів, можливість своєчасно реагувати на компрометацію активів та об'єктів інфраструктури, вирішувати проблеми не тільки внутрішніх витоків конфіденційних даних, але і зовнішніх атак, спрямованих на систему. Крім того, системи UEBA найчастіше поставляються в рамках платформи і використовують дані інших систем, у той час, як UBA зазвичай реалізовані у вигляді окремих рішень під певні завдання і можуть самостійно функціонувати без інтеграції з іншими рішеннями.

Системи UBA/UEBA архітектурно вирішують 4 основні завдання:

–збір даних з усіх можливих доступних джерел: брандмауерів, антивірусів, системних журналів, журналів подій, пристроїв, систем виявлення й запобігання вторгненням;

–нормалізація та зберігання потрібних даних в одному місці. Під нормалізацією розуміють структурований процес організації даних у таблиці так, що він зберігає взаємозв'язок між даними;

–аналіз зібраних даних з метою виявлення аномальної поведінки користувача чи об’єкта шляхом її порівняння з нормою;

–звітування про нетипову поведінку користувачів у разі її виявлення [16].

На рис. 2. представлена схема архітектури UBA/UEBA-систем.

ISSN 2663 - 4023

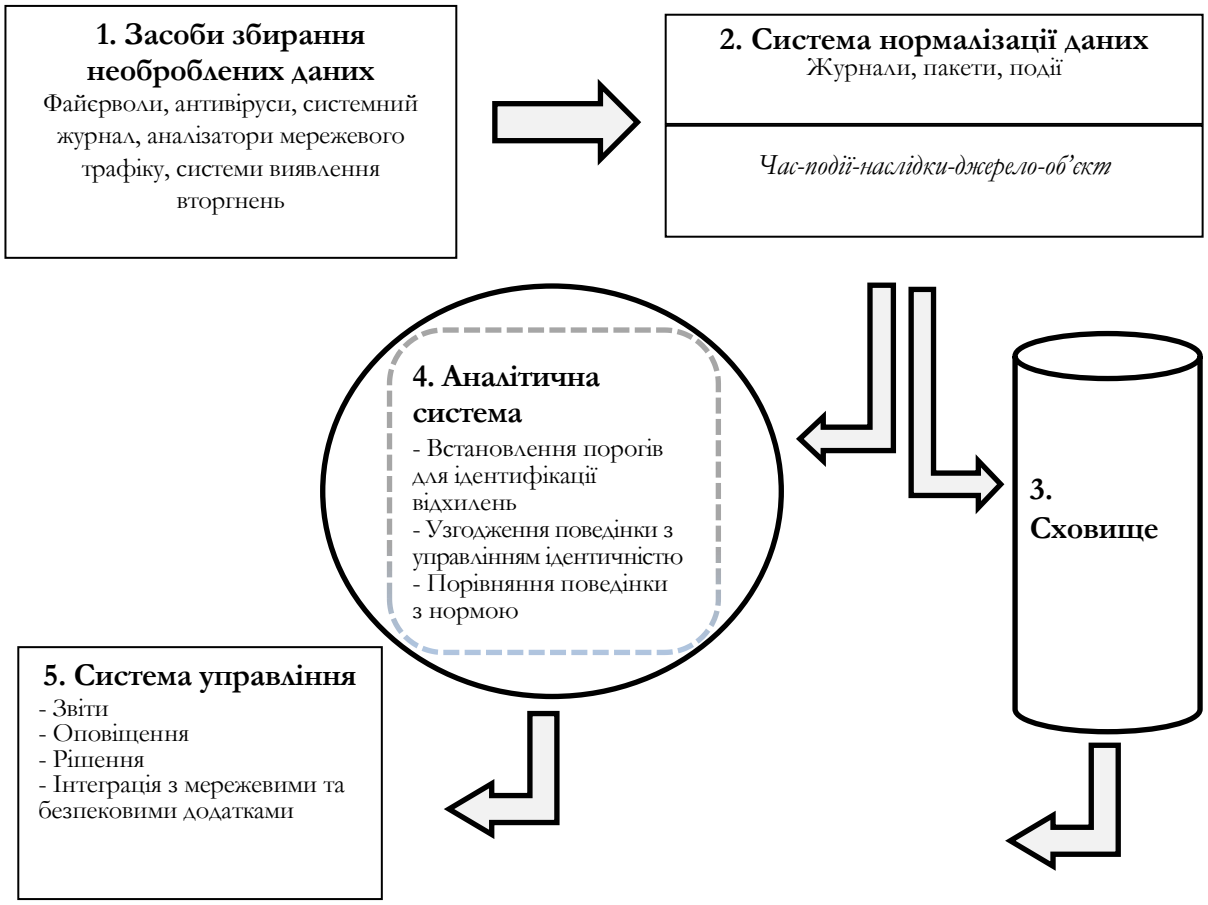

Рис. 2. Архітектура UBA/UEBA систем.

Як видно з наведеної схеми, головним компонентом UBA/UEBA є аналітична система, і у випадку аналізу поведінки користувачів така система застосовує машинне навчання. Алгоритми машинного навчання беруть зібрані дані та визначають закономірності, щоб передбачити ймовірність того, що діяльність користувачів є зловмисною.

Поведінковий аналіз для виявлення зловмисних дій користувачів, який здійснюється аналітичною системою, є послідовністю таких етапів:

1) збирання системою всієї доступної інформації (усі можливі журнали, записи, профілі тощо), щоб сформувати шаблон поведінки користувачів і «навчити» систему;

2) визначення поведінкового шаблону і встановлення набору порогових значень, щоб ідентифікувати, коли поведінка переходить із нормальної в зловмисну (ці пороги становлять відсоток ймовірності, наприклад, 95%);

3) встановлення ймовірності реалізації зловмисної діяльності на основі порівняння отриманої інформації про порушення інформаційної безпеки, яке відбулося в системі, з поведінковим шаблоном. Якщо відсоток ймовірності перевищує встановлене порогове значення, подається сигнал тривоги [16].

На думку експертів провідної дослідницької компанії у сфері IT Gartner, технології UBA/UEBA стають все більш надійними та цінними, їх ширше впроваджують у діяльність із забезпечення інформаційної безпеки як у процесі заміни застарілих інструментів, так і в ході вдосконалення комплексних безпекових рішень за рахунок

розробки додаткових функцій поведінкової аналітики. Також фахівці прогнозують, що до 2022 року основні методи й технології поведінкової аналітики будуть впроваджені у 80% рішень із виявлення загроз та встановлення пріоритетності інцидентів [17].

Можливості поведінкової аналітики UBA/UEBA застосовують у цілому ряді технологій безпеки, таких як SIEM (Security Information and Event Management), IDPS (Intrusion Detection and Prevention Systems) та інших, доповнюючи і розширюючи їх функціонал, сприяючи створенню комплексних практично всеохоплюючих рішень з безпеки ІТ. Так, серед виробників SIEM-систем багато використовують інструменти UEBA, зокрема Dell Technologies, IBM, FireEye, McAfee та інші. Для прикладу можна навести розробки QRadar SIEM від IBM [18] та Analytics-Driven SIEM від Splunk Solutions [19], які містять компоненти моніторингу й аналізу діяльності користувачів.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

З огляду на зростаючий вплив людського чинника на стан захищеності інформаційних систем та ресурсів організації стоять перед необхідністю активно запобігати і протидіяти загрозам інформаційній безпеці з вини персоналу. Використання традиційних засобів захисту таких, як антивіруси, міжмережеві екрани, системи запобігання вторгненням не забезпечують цілковитий захист від внутрішніх порушників, що обумовлює необхідність застосування комбінованих та системних інструментів контролю діяльності користувачів.

Для ефективного захисту своїх активів і вчасного виявлення інсайдерських загроз організаціям варто впроваджувати технології моніторингу й аналізу поведінки користувачів, які можуть бути як окремими програмними продуктами, так і компонентами комплексних рішень з інформаційної безпеки. Поширеними засобами, які виконують функції контролю й аналізу діяльності користувачів, є системи запобігання втраті даних, контролю доступу й аналізу поведінки користувачів.

У перспективі планується дослідити можливості використання технологій моніторингу й аналізу поведінки користувачів як інструментів інформаційно-аналітичної діяльності у сфері забезпечення інформаційної безпеки організації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 *Data Breach Investigations Report*. (2020). Verizon. https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf
2 *15 Alarming Cyber Security Facts and Stats*. Cybint. https://www.cybintsolutions.com/cyber-security-facts-stats/
3 Бурячок, В. Л., Толубко, В. Б., Хорошко, В. О., & Толюпа, С. В. (2015). *Інформаційна та кібербезпека: соціотехнічний аспект : підручник*. ДУТ.
4 Башинська, І. О. (2014). *Основні порушники та загрози інформаційної безпеки промислових підприємств. Problems of social and economic development of business*.
5 Живко, З. Б. (2019). *Сучасні методи забезпечення надійності персоналу : навчальний посібник у схемах і таблицях*. ЛьвДУВС.
6 Elmrabit, N., Yang, S.-H., Yang, L. (2015). Insider threats in information security categories and approaches. https://www.researchgate.net/publication/283503171_Insider_threats_in_information_security_categories_and_approaches
7 Markus, K., Pihelgas, M., Wojtkowiak, J., Trinberg, L., Osula, A.-M. (2018). Insider Threat Detection Study. *Cooperative Cyber Defence Centre of Excellence.* https://ccdcoe.org/uploads/2018/10/Insider_Threat_Study_CCDCOE.pdf
8 Mazzarolo, G., Jurcut, A. (2019). Insider threats in Cyber Security: The enemy within the gates. https://arxiv.org/ftp/arxiv/papers/1911/1911.09575.pdf

9 Balakrishnan, B. (2021). Insider Threat Mitigation Guidance. *SANS Institute*. https://www.sans.org/reading-room/whitepapers/monitoring/insider-threat-mitigation-guidance-36307
10 Common Sense Guide to Mitigating Insider Threats. Sixth Edition: Technical Report #CMU/SEI-2018-TR-010. *Carnegie Mellon University. Software Engineering Institute. CERT National Insider Threat Center*. https://apps.dtic.mil/sti/pdfs/AD1084084.pdf
11 Insider Threat Best Practices Guide. Second Edition. *SIFMA. Sidley Austin LLP.* https://www.nationalinsiderthreatsig.org/itrmresources/Insider%20Threat%20Best%20Practices%20Guide%202nd%20Edition%20--%20SIFMA.pdf
12 *Data loss prevention - Glossary | CSRC.* NIST Computer Security Resource Center | CSRC. https://csrc.nist.gov/glossary/term/data_loss_prevention
13 Прохоров, С. (2016). DLP в структуре информационной безопасности предприятия. https://lib.itsec.ru/articles2/in-ch-sec/dlp-v-strukture-ib-predpriyatiya
14 Lutkevich, B. (2020). Access control. https://searchsecurity.techtarget.com/definition/access-control
15 *All About Access Control*. Everything covered from definition, types, to features and how-tos. https://www.supremainc.com/en/hub/insights-access-control.asp
16 *UEBA (User and Entity Behavior Analytics) for when traditional Cyber Security can't protect your network.* Northforge Innovations. https://gonorthforge.com/ueba/
17 Sadowski, G., Litan, A., Bussa, T., Phillips, T. (2018). Market Guide for User and Entity Behavior Analytics. *Gartner Inc*. https://www.cbronline.com/wp-content/uploads/dlm_uploads/2018/07/gartner-market-guide-for-ueba-2018-analyst-report.pdf
18 *IBM QRadar SIEM. IBM Security : White Paper.* IBM Corporation. https://www.ibm.com/downloads/cas/RLXJNX2G
19 *The Seven Essentials of an Analytics-Driven SIEM : White Paper.* Splunk. https://www.bwdigitronik.ch/application/files/6915/8081/0492/the-seven-essential-capabilities-of-analytics-driven-siem.pdf

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (13), 2021
ISSN 2663 - 4023

Tetyana M. Muzhanova
Ph.D. in Public Administration, Associate Professor, Associate Professor of Information Security and Cyber Security Department
State University of Telecommunications, Kyiv, Ukraine
ORCID ID: 0000-0002-7435-0287
muzanovat@gmail.com

Svitlana V. Lehominova
Doctor of Economics, Professor, Head of Information Security and Cyber Security Department
State University of Telecommunications, Kyiv, Ukraine
ORCID ID: 0000-0002-4433-5123
chiarasvitlana77@gmail.com

Yuriy M. Yakymenko
Ph.D. in Military Science, Associate Professor, Associate Professor of Information Security and Cyber Security Department
State University of Telecommunications, Kyiv, Ukraine
ORCID ID: 0000-0002-6848-852X
yakum14@ukr.net

Iryna V. Mordas
Ph.D. in Economics, Associate Professor, Associate Professor of the Department of Public Policy of the Educational and Scientific Institute of Public Administration and Public Service
Taras Shevchenko National University of Kyiv, Ukraine
ORCID ID: 0000-0002-2908-7555
mordas_iv@ukr.net

TECHNOLOGIES OF USER ACTIVITIES MONITORING AND ANALYSIS IN PREVENTING INSIDER THREATS OF INFORMATION SECURITY OF AN ORGANIZATION

Abstract. The increase in the number of information security incidents related to personnel activities, the frequency of which has almost doubled in the last two years, has led organizations to use effective technologies that prevent and counteract internal threats to information security. An important role in this context belongs to the tools of monitoring and analysis of user activity. According to experts, in the coming years, such technologies will be implemented in 80% of solutions to identify threats and prioritize information security incidents.

The article reveals the essence and analyzes the functionality of several systems that monitor and analyze employee behavior, including Data Loss Prevention (DLP), Access Control, Analysis of User Behavior and IT objects (UBA / UEBA).

The authors establish that the DLP system monitors and reports on user attempts to transmit confidential information by monitoring mail and web traffic, wireless access, external storage, input/output devices, user workstation software, audio and video surveillance of its activities, etc.

Access control tools perform, in particular, the functions of monitoring access and movement of a person in protected areas of the object, collecting information from surveillance cameras, keeping records of working time. In the context of a pandemic, solutions have been developed that allow identifying a person in a mask on the face, to perform the functions of monitoring health.

Analysis of the functional characteristics of UBA / UEBA behavioral analytics systems showed that they not only solve the problem of collecting data from all possible available sources (software and hardware, logs, user correspondence, etc.), but also analyze the collected data and report atypical user behavior in case of its detection.

The article notes that behavioral analytics is used in a number of security technologies, such as Security Information and Event Management system, Intrusion Detection and Prevention System, and others, complementing and expanding their capabilities, helping to create comprehensive information security solutions.

The authors recommend organizations to use tools for monitoring and analyzing the user activities in different combinations or as part of integrated Information Security Management solutions to achieve the appropriate information security level in the face of growing threats from personnel.

Key words: information security of an organization; internal threats to information security of an organization; Data Loss Prevention (DLP); Access Control; User Behavior Analytics (UBA).

REFERENCES

1 *Data Breach Investigations Report*. (2020). Verizon. https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf
2 *15 Alarming Cyber Security Facts and Stats*. Cybint. https://www.cybintsolutions.com/cyber-security-facts-stats/
3 Buriachok, V. L., Tolubko, V. B., Khoroshko, V. O., & Toliupa, S. V. (2015). *Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt : pidruchnyk.* DUT
4 Bashynska, I. O. (2014). *Osnovni porushnyky ta zahrozy informatsiinoi bezpeky promyslovykh pidpryiemstv. Problems of social and economic development of business*.
5 Zhyvko, Z. B. (2019). *Suchasni metody zabezpechennia nadiinosti personalu : navchalnyi posibnyk u skhemakh i tablytsiakh.* LvDUVS.
6 Elmrabit, N., Yang, S.-H., Yang, L. (2015). Insider threats in information security categories and approaches. https://www.researchgate.net/publication/283503171_Insider_threats_in_information_security_categories_and_approaches
7 Markus, K., Pihelgas, M., Wojtkowiak, J., Trinberg, L., Osula, A.-M. (2018). Insider Threat Detection Study. *Cooperative Cyber Defence Centre of Excellence.* https://ccdcoe.org/uploads/2018/10/Insider_Threat_Study_CCDCOE.pdf
8 Mazzarolo, G., Jurcut, A. (2019). Insider threats in Cyber Security: The enemy within the gates. https://arxiv.org/ftp/arxiv/papers/1911/1911.09575.pdf
9 Balakrishnan, B. (2021). Insider Threat Mitigation Guidance. *SANS Institute*. https://www.sans.org/reading-room/whitepapers/monitoring/insider-threat-mitigation-guidance-36307
10 Common Sense Guide to Mitigating Insider Threats. Sixth Edition: Technical Report #CMU/SEI-2018-TR-010. *Carnegie Mellon University. Software Engineering Institute. CERT National Insider Threat Center*. https://apps.dtic.mil/sti/pdfs/AD1084084.pdf
11 Insider Threat Best Practices Guide. Second Edition. *SIFMA. Sidley Austin LLP*. https://www.nationalinsiderthreatsig.org/itrmresources/Insider%20Threat%20Best%20Practices%20Guide%202nd%20Edition%20--%20SIFMA.pdf
12 *Data loss prevention - Glossary | CSRC*. NIST Computer Security Resource Center | CSRC. https://csrc.nist.gov/glossary/term/data_loss_prevention
13 Prokhorov, S. (2016). DLP v strukture ynformatsyonnoi bezopasnosty predpryiatyia. https://lib.itsec.ru/articles2/in-ch-sec/dlp-v-strukture-ib-predpriyatiya
14 Lutkevich, B. (2020). Access control. https://searchsecurity.techtarget.com/definition/access-control
15 *All About Access Control*. Everything covered from definition, types, to features and how-tos. https://www.supremainc.com/en/hub/insights-access-control.asp
16 *UEBA (User and Entity Behavior Analytics) for when traditional Cyber Security can't protect your network.* Northforge Innovations. https://gonorthforge.com/ueba/
17 Sadowski, G., Litan, A., Bussa, T., Phillips, T. (2018). Market Guide for User and Entity Behavior Analytics. *Gartner Inc.* https://www.cbronline.com/wp-content/uploads/dlm_uploads/2018/07/gartner-market-guide-for-ueba-2018-analyst-report.pdf
18 *IBM QRadar SIEM. IBM Security : White Paper*. IBM Corporation. https://www.ibm.com/downloads/cas/RLXJNX2G
19 *The Seven Essentials of an Analytics-Driven SIEM : White Paper.* Splunk. https://www.bwdigitronik.ch/application/files/6915/8081/0492/the-seven-essential-capabilities-of-analytics-driven-siem.pdf