ПОВЕДЕНЧЕСКИ АНАЛИЗ И ОЦЕНКА НА РИСКА ОТ ВЪТРЕШНИ ЗАПЛАХИ ЧРЕЗ СРЕДСТВАТА НА MICROSOFT EXCEL

Бора Неджиб

Редовен докторант, катедра „Информатика“, Икономически университет – Варна

Резюме: *Вътрешните заплахи за информационната сигурност произтичат от лица с легитимен достъп до организационните ресурси, което затруднява тяхното откриване чрез традиционни механизми за защита, основани на сигнатури и фиксирани правила. В статията са анализирани възможностите на Microsoft Excel за предварителна обработка, анализ и визуализация на данни за потребителска активност в контекста на откриването на вътрешни заплахи. Разработен е прототипен аналитичен модел върху синтетичен набор от логови данни, който включва обогатяване на записите чрез корелация с потребителски профили, трансформация на времеви атрибути, оценяване на риска чрез логически правила и интерактивна визуализация чрез обобщени таблици, сегментатори и информационно табло. Резултатите показват, че Microsoft Excel може да се използва като достъпна среда за proof-of-concept решения, обучение и предварителен анализ, като същевременно са очертани ограниченията на подхода спрямо специализираните SIEM и UEBA платформи и възможностите за надграждане чрез методи на машинно обучение.*

Ключови думи: *вътрешни заплахи, поведенчески анализ, оценка на риска, Microsoft Excel, визуализация на данни, информационно табло, UEBA, SIEM, информационна сигурност*

Bora Nedzhib

PhD Student, Department of Informatics, University of Economics – Varna

Abstract: *Insider threats to information security originate from individuals with legitimate access to organizational resources, which makes them difficult to detect through traditional protection mechanisms based on signatures and fixed rules. The article analyzes the capabilities of Microsoft Excel for preprocessing, analysis and visualization of user activity*

data in the context of insider threat detection. A prototype analytical model is developed on a synthetic log dataset, including record enrichment through correlation with user profiles, transformation of time attributes, risk scoring through logical rules, and interactive visualization using pivot tables, slicers and a dashboard. The results show that Microsoft Excel can serve as an accessible environment for proof-of-concept solutions, training and preliminary analysis, while the limitations of the approach compared to specialized SIEM and UEBA platforms and the opportunities for extension through machine learning methods are outlined.

Keywords: *insider threats, behavioral analysis, risk assessment, Microsoft Excel, data visualization, dashboard, UEBA, SIEM, information security*

Увод

Развитието на информационните технологии и дигитализацията на организационните процеси водят до непрекъснато увеличаване на обема от данни, генерирани от потребителската активност, достъпа до ресурси и обмена на информация. Същевременно нараства и значението на киберсигурността като основен фактор за защитата на организационните информационни активи. В този контекст вътрешните заплахи за информационна сигурност се утвърждават като съществен риск за организациите, тъй като произтичат от лица с легитимен достъп до системите и данните. Специфична особеност на този тип заплахи е, че те често се проявяват в рамките на привидно нормална потребителска дейност, което затруднява тяхното своевременно откриване и налага комплексен подход към управлението на вътрешния риск (Skorich, Manning 2025).

Вътрешните заплахи могат да произтичат както от злонамерени действия, така и от непреднамерени грешки, водещи до изтичане на информация, злоупотреба с привилегии или нарушаване работата на информационните системи. Това налага използването на аналитични подходи, поведенчески анализ и методи за откриване на аномалии. Съществено значение имат предварителната обработка и визуализацията на данни, тъй като логовете и записите от събитията обикновено са с голям обем и разнообразна структура (Kent, Souppaya 2006).

Microsoft Excel предоставя функционалности за структуриране, филтриране, анализ и визуализация на данни. Чрез електронни таблици, обобщени таблици (Pivot Tables), условно форматиране, графики и интерактивни информационни табла

(Dashboards) може да се реализира среда за предварителен анализ на потребителска активност и визуализация на индикатори за риск. Практическото приложение на Microsoft Excel позволява разработването на аналитични модели и proof-of-concept (POC) решения. Под POC се разбира подход за валидиране, при който чрез прототип, демонстрация или експеримент се оценява осъществимостта, техническата валидност и приложимостта на дадена концепция в контролирана среда (Gillis, Pratt 2023). Такива решения могат да бъдат използвани в научноизследователски контекст и при експериментален анализ на поведенчески модели (Alexander, Kusleika 2022).

Обект на изследване в настоящата статия са офис приложенията и техните възможности за обработка и визуализация на данни в контекста на информационната сигурност, а **предметът** на изследване са подходите за предварителна обработка и визуализация на данни чрез Microsoft Excel при модели за откриване на вътрешни заплахи.

Целта на статията е да се анализират възможностите на Excel за обработка, анализ и визуализация на данни при модели за откриване на вътрешни заплахи, както и да се демонстрира приложението им чрез примерен аналитичен модел.

За постигане на поставената цел са формулирани следните **задачи:**

1) Да се разгледат основните характеристики на вътрешните заплахи в информационните системи;
2) Да се анализира ролята на предварителната обработка на данни за откриване на вътрешни заплахи;
3) Да се изследват възможностите на Microsoft Excel за обработка и визуализация на данни;
4) Да се анализират средствата за динамичен анализ чрез обобщени таблици (Pivot

5) Да се разработи примерен аналитичен модел за оценка и визуализация на риск.

Представеният модел е част от изследване, насочено към разработване на интелигентен модел за откриване на вътрешни заплахи чрез поведенчески анализ и машинно обучение, като има ролята на предварителен етап за структуриране и визуална интерпретация на данни за потребителско поведение.

1. Вътрешни заплахи и анализ на данни в информационните системи – теоретични аспекти

1.1. Същност и характеристики на вътрешните заплахи

Съвременните организации функционират в условията на висока зависимост от информационни системи, цифрови ресурси и мрежова инфраструктура, което превръща информационната сигурност в ключов елемент от организационната устойчивост. Наред с външните кибератаки все по-съществено значение придобиват вътрешните заплахи, тъй като те произлизат от потребители с легитимен достъп до организационните ресурси и познаване на вътрешните процеси, политики и механизми за защита (Cappelli et al. 2012).

Според Андреев (2026) заплахата представлява потенциална причина за нежелано събитие, което би могло да навреди на организацията, като може да произхожда както от външни, така и от вътрешни фактори. В контекста на информационната сигурност особено значение имат вътрешните заплахи, които произтичат от действията или бездействията на служители, подизпълнители или други лица с легитимен достъп до организационните ресурси. Тези действия могат да бъдат както умишлени, така и непреднамерени. Умишлените вътрешни заплахи обикновено са свързани със злоупотреба с привилегии, кражба на информация, саботаж или нерегламентирано разпространение на чувствителни данни. Непреднамерените действия най-често произтичат от човешки грешки, недостатъчна осведоменост или неспазване на организационните политики за сигурност (IBM 2024).

Една от основните характеристики на вътрешните заплахи е сложността при тяхното идентифициране. За разлика от традиционните външни атаки, при които често се наблюдават ясно изразени индикатори за компрометиране, сценариите за вътрешни заплахи обикновено се осъществяват чрез валидни потребителски акаунти и формално легитимни действия в рамките на предоставените права за достъп. Това значително затруднява разграничаването между нормална и потенциално рискова активност и налага използването на аналитични подходи, основани на поведенчески анализ, корелация на събития и откриване на аномалии.

В организационната практика вътрешните заплахи могат да бъдат идентифицирани чрез различни поведенчески индикатори, сред които необичайно време за достъп до системите, прекомерни файлови операции, достъп до нетипични ресурси, промени в потребителските привилегии или използване на неоторизирани устройства.

Самостоятелно подобни действия невинаги представляват инцидент по сигурността, но тяхното комбиниране и анализ в контекста на потребителското поведение позволява откриване на потенциални отклонения от нормалната оперативна активност.

Според IBM (2024) вътрешните заплахи могат да бъдат разграничени в три основни категории – злонамерени вътрешни лица, небрежни служители и компрометирани потребителски акаунти. Злонамерените вътрешни лица целенасочено извършват действия с цел извличане на облага или нанасяне на щети на организацията. При компрометираните акаунти легитимните идентификационни данни се използват от външен атакуващ, докато при небрежните служители рискът е свързан основно с човешки грешки и недостатъчна култура по информационна сигурност. От гледна точка на извършените действия Cappelli et al. (2012) разграничават три основни типа злонамерени инциденти – саботаж на информационните системи, кражба на интелектуална собственост и измама.

Нарастващият обем от данни, генерирани в информационните системи, създава предпоставки за прилагане на аналитични подходи при откриване на вътрешни заплахи. Логовете от системи за достъп, файлови операции, мрежова активност и потребителски действия съдържат значителен обем информация относно поведението на потребителите и позволяват идентифициране на отклонения спрямо установените модели на активност. Това определя и нарастващата роля на поведенческия анализ като средство за откриване на потенциално рисково поведение в организационната среда.

1.2. Поведенчески анализ и модели за откриване на аномалии

Традиционните механизми за защита в информационната сигурност обикновено се основават на предварително дефинирани правила, сигнатури и фиксирани прагови стойности. Макар този подход да е ефективен при разпознаването на известни заплахи и утвърдени модели на атака, неговите възможности са ограничени при откриването на нетипични поведенчески отклонения, които не съответстват на предварително зададени сценарии. Поради това в съвременните системи за информационна сигурност все по-широко приложение намират подходите, базирани на поведенчески анализ и откриване на аномалии (Brumfield 2025), които позволяват идентифициране на потенциални рискове чрез анализ на отклоненията от установените модели на активност.

За разлика от механизмите, които разчитат на сигнатурни модели или предварително дефинирани такива за разпознаване на заплахи, поведенческият анализ се

фокусира върху отклоненията от нормалното поведение на потребителите. Чрез наблюдение и анализ на потребителската активност могат да бъдат идентифицирани действия, които се различават от установените модели на работа и потенциално представляват риск за сигурността. Поведенческият анализ се утвърждава като един от основните подходи за откриване на вътрешни заплахи, тъй като позволява идентифициране на аномалии, които трудно могат да бъдат установени чрез традиционните методи, базирани на сигнатури (Sarker et al. 2020).

В практиката широко приложение намират системите от типа User and Entity Behavior Analytics (UEBA) – технология за откриване на киберзаплахи, основана на поведенчески анализ на потребители, устройства, приложения и други обекти в информационната среда. Основната задача на този подход е навременното разпознаване на целенасочени атаки и вътрешни заплахи. За целта UEBA системите използват статистически и поведенчески модели, както и модели на машинно обучение за анализ на потребителската активност и оценка на риска (Kaspersky Lab n.d.). Тези системи обработват големи обеми от логови данни, системни събития и мрежова информация, като анализират поведението на потребителите във времето и идентифицират аномалии спрямо установените модели на активност (Cisco 2026).

Съществено предимство на UEBA подходите е възможността за автоматизирано откриване на поведенчески отклонения без необходимост от предварително дефинирани сигнатури. Това позволява идентифициране както на злонамерени действия, така и на потенциално рисково поведение, което не съответства на предварително известни сценарии за атака. Въпреки това, ефективността на подобни системи остава силно зависима от качеството на входните данни, контекстната интерпретация на потребителската активност и надеждността на използваните аналитични модели.

Наред с предимствата си, UEBA системите имат и определени ограничения, свързани с необходимостта от значителни обеми исторически данни, вероятност от фалшиво положителни резултати и сложност при интерпретацията на поведенческите отклонения. Поради тази причина процесите по структуриране, филтриране и нормализация на логовата информация имат съществено значение за надеждността на аналитичните резултати.

В процеса по обработка и анализ на подобен тип информация съществено значение имат средствата за структуриране, филтриране и визуализация на данните. Предварителната обработка на логовите записи позволява по-ефективно организиране на информацията и подпомага процеса по идентифициране на зависимости и

поведенчески отклонения. В научни изследвания и демонстрационни аналитични модели често се използват инструменти като Microsoft Excel за предварителна обработка, агрегиране и визуално представяне на данните преди интеграцията им в по-сложни аналитични среди.

Възможности на Microsoft Excel за обработка и визуализация на данни при анализ на вътрешни заплахи

Предварителна обработка и обогатяване на данни в Microsoft Excel

Съвременните офис приложения все по-често се използват за обработка и анализ на данни, като разширяват приложението си извън традиционната административна дейност. Microsoft Excel е широко използвано приложение за електронни таблици, прилагано за автоматизация на офис процеси и създаване на бизнес приложения, като с времето неговите функционалности непрекъснато се разширяват (Сълов и др. 2019). Приложението предоставя възможности за структуриране, филтриране, агрегиране и визуализация на данни чрез електронни таблици, логически функции и аналитични инструменти. Макар да не е предназначено за обработка на големи обеми данни в реално време, Excel е подходящ за изграждане на демонстрационни аналитични модели и среди за предварителен анализ.

В рамките на настоящото изследване Microsoft Excel е използвано като среда за предварителна обработка и анализ на данни, свързани с потребителската активност и потенциални вътрешни заплахи. За целите на разработката чрез скрипт е генериран синтетичен набор от данни, който не съдържа реална организационна информация или лични данни. Наборът включва 200 събития, извършени от 30 потребители в 8 отдела за периода от 10.02.2025 г. до 04.03.2025 г., като 50 от събитията са в почивни дни. В данните са заложени сценарии на рисково поведение, като многократни неуспешни опити за вход, достъп до файлове с висока чувствителност, трансфер на големи обеми данни, използване на USB устройства, отдалечен достъп и активност извън работно време. Всяко събитие е маркирано с очаквано ниво на риска (RiskLabel), като 48 от събитията са с ниво High или Critical, което позволява последваща проверка на резултатите от модела.

За нуждите на анализа е създаден първичен демонстрационен набор от данни (Raw_Data), съдържащ синтетични записи за потребителска активност и системни събития. Таблицата включва атрибути като идентификатор на събитие, времеви маркер, потребителски идентификатор, организационна роля, тип действие, устройство, IP адрес

и статус на операцията (вж. Фиг. 1). Данните са организирани в структуриран табличен формат, позволяващ автоматизирано разширяване на диапазоните при добавяне на нови записи и улесняващ последващото използване на аналитични функции и механизми за визуализация.

	A	B	C	D	F	J	K	M	N	O	P	Q	R
1	EventID	Timestamp	UserID	Department	ActionType	DeviceType	LoginStatus	Location	WorkHours	SessionDurationMin	FailedAttempts24h	PrivilegeLevel	RiskLabel
2	E1001	2/10/25 8:12	U101	Sales	Login	PC	Success	Office	Yes	5	0	Admin	Low
3	E1002	2/10/25 8:45	U102	HR	Open	PC	Success	Office	Yes	12	0	User	Low
4	E1003	2/10/25 9:03	U103	IT	Download	PC	Success	Office	Yes	3	0	Admin	Medium
5	E1004	2/10/25 9:31	U104	Finance	Delete	PC	Success	Office	Yes	8	1	Admin	High
6	E1005	2/10/25 10:00	U105	Marketing	Login	USB	Failed	Remote	No	0	3	User	High
7	E1006	2/10/25 10:22	U106	Sales	Download	PC	Success	Office	Yes	15	0	User	Low
8	E1007	2/10/25 11:15	U107	IT	Open	Remote	Success	VPN	Yes	9	0	Admin	Low
9	E1008	2/10/25 12:04	U108	Legal	Delete	PC	Success	Office	Yes	4	2	User	High
10	E1009	2/10/25 13:20	U109	R&D	Download	PC	Success	Office	Yes	70	0	Admin	Medium

Фиг. 1. Първичен набор от логови данни (Raw_Data)
Източник: Разработка на автора

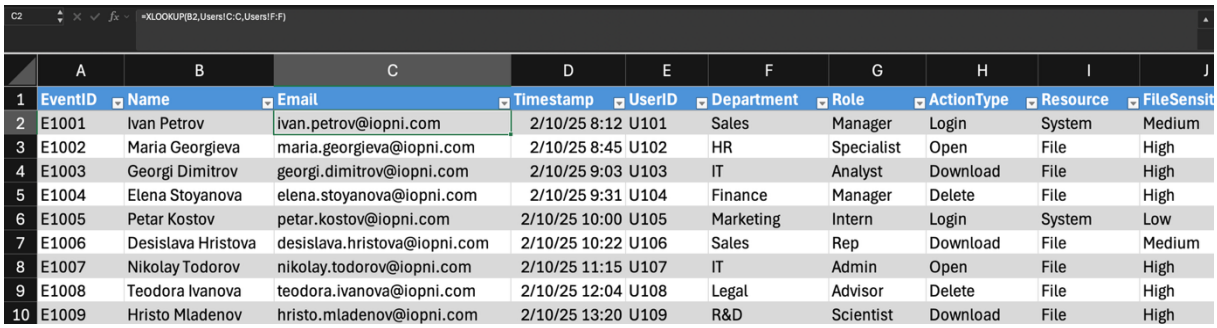
За обогатяване на логовите записи е създадена допълнителна таблица „Users“, съдържаща информация за потребителските профили и организационните роли. В нея са включени атрибути като име на служител, отдел, длъжност, служебен имейл адрес и ниво на достъп. Информацията от таблицата се използва за изграждане на контекст при анализа на потребителската активност и за корелация между логовите събития и организационната структура. При създаването на потребителските профили са използвани текстови функции на Microsoft Excel за автоматично генериране на стандартизирани служебни имейл адреси. С функциите LOWER() и SUBSTITUTE() се осъществява преобразуване на текста в унифициран формат, подходящ за последваща обработка и анализ (вж. Фиг. 2).

	A	B	C	D	E	F	G	H	I
1	UserID	Gender	Name	Department	Role	Email	NormalWorkStart	NormalWorkEnd	AccessLevel
2	U109	M	Hristo Mladenov	R&D	Scientist	hristo.mladenov@iopni.com	10:00	19:00	High
3	U105	M	Petar Kostov	Marketing	Intern	petar.kostov@iopni.com	10:00	18:00	Low
4	U119	M	Valentin Popov	R&D	Lead	valentin.popov@iopni.com	10:00	18:00	High
5	U101	M	Ivan Petrov	Sales	Manager	ivan.petrov@iopni.com	9:00	18:00	High
6	U103	M	Georgi Dimitrov	IT	Analyst	georgi.dimitrov@iopni.com	9:00	18:00	High
7	U104	F	Elena Stoyanova	Finance	Manager	elena.stoyanova@iopni.com	9:00	18:00	High
8	U107	M	Nikolay Todorov	IT	Admin	nikolay.todorov@iopni.com	9:00	18:00	High
9	U110	M	Vladimir Stoev	Sales	Director	vladimir.stoev@iopni.com	9:00	18:00	High
10	U112	M	Plamen Yordanov	IT	Security	plamen.yordanov@iopni.com	9:00	18:00	High

Фиг. 2. Таблица с потребителски профили (Users)
Източник: Разработка на автора

След структуриране на първичните данни е приложено обогатяване на информацията чрез функцията XLOOKUP(), която извлича данни за съответния потребител от таблицата на потребителите. По този начин към всеки логов запис се добавя контекстна информация, свързана с организационната роля, отдела и нивото на достъп на потребителя. Използването на подобен механизъм за корелация позволява

изграждане на по-пълна картина относно потребителското поведение и подпомага анализа на потенциално рискови действия. Чрез комбиниране на логовите записи с организационна информация се създават условия за по-прецизна интерпретация на поведенческите отклонения и оценяване на риска. На Фиг. 3 е визуализиран пример за използваната функция XLOOKUP().



	A	B	C	D	E	F	G	H	I	J
1	EventID	Name	Email	Timestamp	UserID	Department	Role	ActionType	Resource	FileSensit
2	E1001	Ivan Petrov	ivan.petrov@iopni.com	2/10/25 8:12	U101	Sales	Manager	Login	System	Medium
3	E1002	Maria Georgieva	maria.georgieva@iopni.com	2/10/25 8:45	U102	HR	Specialist	Open	File	High
4	E1003	Georgi Dimitrov	georgi.dimitrov@iopni.com	2/10/25 9:03	U103	IT	Analyst	Download	File	High
5	E1004	Elena Stoyanova	elena.stoyanova@iopni.com	2/10/25 9:31	U104	Finance	Manager	Delete	File	High
6	E1005	Petar Kostov	petar.kostov@iopni.com	2/10/25 10:00	U105	Marketing	Intern	Login	System	Low
7	E1006	Desislava Hristova	desislava.hristova@iopni.com	2/10/25 10:22	U106	Sales	Rep	Download	File	Medium
8	E1007	Nikolay Todorov	nikolay.todorov@iopni.com	2/10/25 11:15	U107	IT	Admin	Open	File	High
9	E1008	Teodora Ivanova	teodora.ivanova@iopni.com	2/10/25 12:04	U108	Legal	Advisor	Delete	File	High
10	E1009	Hristo Mladenov	hristo.mladenov@iopni.com	2/10/25 13:20	U109	R&D	Scientist	Download	File	High

Фиг. 3. Използване на XLOOKUP() за обогатяване на данните
Източник: Разработка на автора

След структуриране и обогатяване на информацията е приложена предварителна обработка на времевите атрибути, включително дата, час и ден от седмицата. За тази цел са използвани вградените функции в Excel – INT(), HOUR() и TEXT(), които извличат и нормализират времевите характеристики на логовите записи. Получените данни позволяват идентифициране на активности, извършени извън стандартното работно време, което представлява често използван индикатор при анализ на вътрешни заплахи. За стандартно работно време е прието от понеделник до петък от 08:00 до 18:00 ч., а събитията извън него се маркират чрез функцията IF():

$$= IF(OR(HOUR(B2) < 8, HOUR(B2) >= 18, WEEKDAY(B2,2) > 5), "Yes", "No")$$

Подобен подход позволява автоматизирано откриване на поведенчески отклонения, които могат да бъдат разглеждани като индикатори за потенциално рискова активност. При оценката на риска моделът използва и индивидуалното работно време на всеки служител от таблица Users, като за извънработна се приема активност преди началото или след края на работния му ден, както и в почивни дни. Въпреки опростения

характер на подобен модел, той демонстрира приложимостта на логическите функции при изграждане на базови механизми за анализ на потребителско поведение.

След предварителна обработка на данните е внедрен механизъм за оценяване на риска чрез логически функции и предварително дефинирани правила. Според IBM (2026) оценката на заплахата (Threat Score) представлява числова стойност, използвана в киберсигурността за количествено определяне на нивото на риск, свързан с дадено събитие, обект или актив. В разработения модел за всяко събитие се изчислява поведенческа оценка на риска (BehavioralRiskScore) като сума от точките по осем индикатора (вж. Таблица 1). Точките се определят чрез функциите IF(), IFS() и MIN(), като MIN() ограничава приноса на неуспешните опити за вход до 25 точки, а максималната възможна оценка е 115 точки.

Таблица 1

Индикатори и точкуване в модела за оценка на риска

Индикатор	Условие	Точки
Извънработно време	Извън индивидуалното работно време или в почивен ден	20
Чувствителност на файла	High/Medium/Low	10/5/1
Обем на трансфера	≥ 100 MB/10-99 MB/под 10 MB	15/5/1
Неуспешни опити за вход	5 точки за опит, най-много 25 (MIN)	0 – 25
Ниво на привилегии	Admin/User	10/2
Тип устройство	USB/Remote/друго	15/10/2
Локация	Remote/друга	10/1
Продължителност на сесията	Над 60 минути	10

Източник: Разработка на автора

Нивото на риска се определя чрез функцията IFS() въз основа на сумарната оценка: под 20 точки – Low, от 20 до 39 точки – Medium, от 40 до 69 точки – High, и 70 и повече точки – Critical:

$$= IFS(AQ2 < 20, "Low", AQ2 < 40, "Medium", AQ2 < 70, "High", TRUE, "Critical")$$

Класификацията и оценяването на риска чрез логически функции са представени на Фиг. 4. Макар подобен подход да не може да замени специализираните системи за управление на информация и събития за сигурност (SIEM), представляващи решения за идентифициране и адресиране на потенциални заплахи и уязвимости преди тяхното въздействие върху бизнес процесите (IBM n.d.), той предоставя подходяща среда за демонстрационни изследвания, предварителен анализ и визуализация на данните.

	A	B	AI	AJ	AK	AL	AM	AN	AO	AP	AQ	AR
1	EventID	Timestamp	AfterHours Flag	SensitiveAccess Score	Transfer Risk	FailedLogin Risk	PrivilegedAcces sRisk	Device Risk	Location Risk	SessionAn omaly	Behavioral RiskScore	ThreatLevel
2	E1001	2/10/25 8:12	1	5	1	0	10	2	1	0	39	Medium
3	E1003	2/10/25 9:03	0	10	5	0	10	2	1	0	28	Medium
4	E1004	2/10/25 9:31	0	10	1	5	10	2	1	0	29	Medium
5	E1007	2/10/25 11:15	0	10	1	0	10	10	1	0	32	Medium
6	E1008	2/10/25 12:04	0	10	1	10	2	2	1	0	26	Medium
7	E1009	2/10/25 13:20	0	10	15	0	10	2	1	0	38	Medium
8	E1012	2/10/25 15:10	0	10	1	0	10	10	1	0	32	Medium
9	E1018	2/10/25 19:15	1	10	1	0	2	2	1	0	36	Medium
10	E1020	2/10/25 20:45	1	1	1	0	10	2	1	0	35	Medium

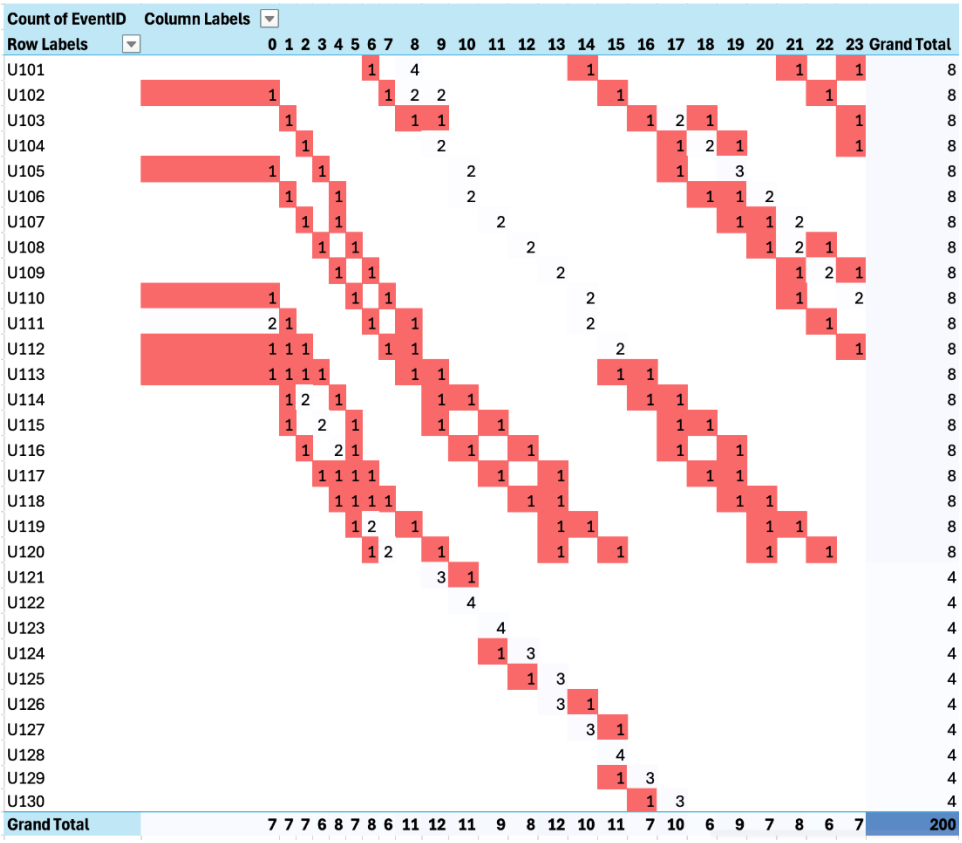
Фиг. 4. Класификация и оценяване на риска чрез логически функции
Източник: Разработка на автора

Представените механизми за обогатяване, трансформация и оценяване на данните показват, че чрез стандартни функции на Microsoft Excel може да бъде изграден базов процес за предварителна обработка на логови записи. Получените атрибути и оценки на риска формират основата за последващия агрегиран анализ и визуализация на потребителската активност.

Анализ и визуализация на данни чрез обобщени таблици и интерактивни информационни табла

Обобщените таблици в Microsoft Excel са използвани като основен инструмент за агрегиране, групиране и анализ на данните, свързани с потребителската активност и потенциалните вътрешни заплахи. Чрез тях се обобщават записи от големи обеми логове и се извършва визуализиране на зависимости между различни показатели, използвани при поведенческия анализ.

В разработения модел обобщените таблици се използват за анализ на потребителската активност по часове от денонощието, отдели и нива на риска (вж. Фиг. 5 и Фиг. 6). Това позволява идентифициране на високорискови потребители, както и откриване на поведенчески отклонения при работа с информационната система. С възможностите за групиране, филтриране и динамично обновяване на информацията в Excel се прилага интерактивен анализ, при който данните се актуализират автоматично при промяна на избраните критерии. Този подход улеснява интерпретацията на информацията и подпомага ранното идентифициране на потенциални вътрешни заплахи.



Count of EventID	Column Labels																							
Row Labels	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	Grand Total
U101							1		4						1							1		1	8
U102	1							1	2	2						1							1		8
U103		1							1	1							1	2	1					1	8
U104			1							2								1	2	1				1	8
U105	1			1							2							1		3					8
U106		1			1						2								1	1	2				8
U107			1	1								2								1	1	2			8
U108				1	1								2								1	2	1		8
U109					1	1								2								1	2	1	8
U110	1					1	1								2							1		2	8
U111	2	1					1		1						2								1		8
U112	1	1	1					1	1							2								1	8
U113	1	1	1	1					1	1						1	1								8
U114		1	2		1					1	1						1	1							8
U115		1		2		1				1		1						1	1						8
U116			1		2	1					1		1					1		1					8
U117				1	1	1	1					1		1					1	1					8
U118					1	1	1	1					1	1						1	1				8
U119						1	2		1					1	1						1	1			8
U120							1	2		1				1		1					1		1		8
U121										3	1														4
U122											4														4
U123												4													4
U124												1	3												4
U125													1	3											4
U126														3	1										4
U127															3	1									4
U128																4									4
U129																1	3								4
U130																	1	3							4
Grand Total	7	7	7	6	8	7	8	6	11	12	11	9	8	12	10	11	7	10	6	9	7	8	6	7	200

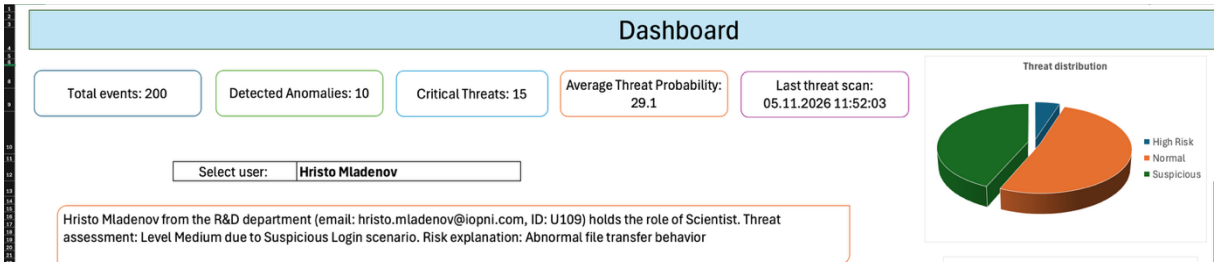
Фиг. 5. Разпределение на потребителската активност по часове от денонощието чрез обобщени таблици
Източник: Разработка на автора

Count of UserID	Column Labels				
Row Labels	Critical	High	Low	Medium	Grand Total
Finance	1	5	5	13	24
HR	1	6	5	16	28
IT	5	22	2	11	40
Legal		9	1	10	20
Marketing		10	4	6	20
Operations	3	6	1	2	12
R&D	2	12	1	5	20
Sales	3	14	8	11	36
Grand Total	**15**	**84**	**27**	**74**	**200**

Фиг. 6. Разпределение на събитията по отдели и нива на риска чрез обобщени таблици
Източник: Разработка на автора

В рамките на разработения модел е изградено интерактивно информационно табло (Dashboard), предназначено за визуализация и анализ на данните, свързани с вътрешни заплахи в информационни системи (вж. Фиг. 7). Чрез използване на диаграми, условно форматиране и графични индикатори се осъществява визуално представяне на

основните показатели за риск и потребителска активност. Освен поведенческата оценка на риска, таблото показва и вероятност за вътрешна заплаха (InsiderThreatProbability), изчислена като средна стойност от поведенческата оценка и оценка на отклонението от обичайния обем на трансфер на данни, като 10 събития със z-стойност над 2,5 са маркирани като аномалии.



Фиг. 7. Интерактивно информационно табло (Dashboard)
Източник: Разработка на автора

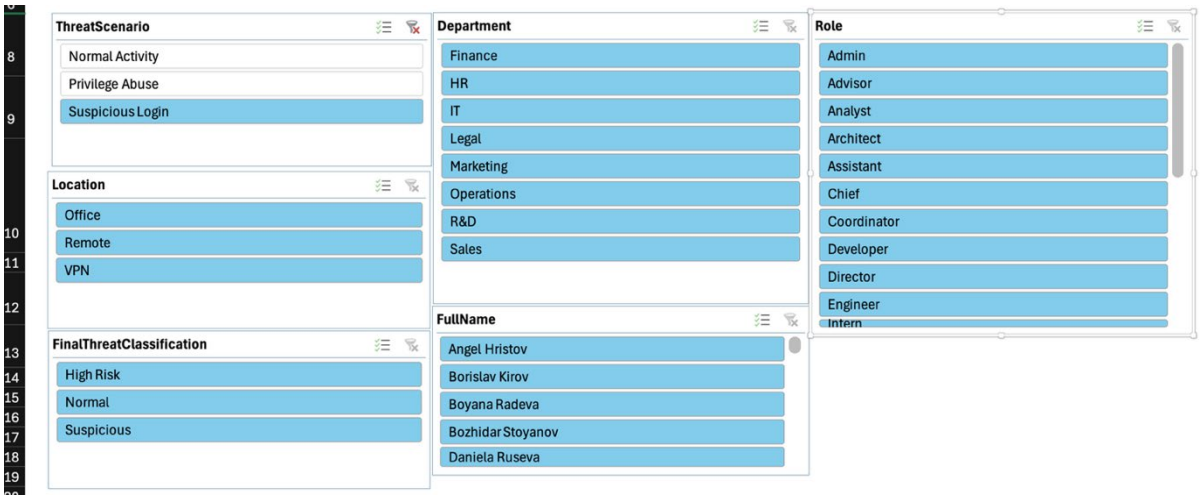
За целите на интерактивния анализ са използвани механизми за динамично филтриране и автоматично обновяване на визуалните елементи. Чрез функционалността за проверка на данни (Data Validation) е осигурен избор на конкретен потребител, при който информацията в информационното табло се актуализира автоматично (вж. Фиг. 8). В конзолата нивото на заплахата се представя и чрез условна числова стойност (Low – 20, Medium – 50, High – 75, Critical – 95), използвана единствено за целите на визуализацията.

Threat Investigation Console

Name	Department	email	Role	UserID	Threat level	Threat scenario	Risk Explanation	Threat score
Iva Kostadinova	IT	iva.kostadinova@iopni.com	Developer	U130	Medium	Normal Activity	Normal behavioral pattern	50
Plamen Yordanov	IT	plamen.yordanov@iopni.com	Security	U112	Medium	Normal Activity	Normal behavioral pattern	50

Фиг. 8. Threat Investigation Console в информационното табло
Източник: Разработка на автора

Интерактивните сегментатори (Slicers), показани на Фиг. 9, позволяват бързо филтриране и групиране на информацията по различни критерии, което подпомага анализа и визуализацията на данните. Комбинирането на обобщени таблици, динамични сегментатори и визуални елементи позволява изграждане на интерактивна аналитична среда за проследяване на потребителската активност и идентифициране на поведенчески аномалии.



Фиг. 9. Интерактивни сегментатори (Slicers) за динамично обновяване на информацията
Източник: Разработка на автора

Осъщественият подход демонстрира възможностите на Microsoft Excel за изграждане на интерактивна аналитична среда, подходяща за предварителна обработка, визуализация и анализ на данни в контекста на модели за откриване на вътрешни заплахи. Въпреки ограниченията на платформата при работа с големи обеми данни и липсата на специализирани механизми за обработка в реално време, Excel предоставя достатъчно функционалности за изграждане на демонстрационни аналитични модели и proof-of-concept среди за научни изследвания и обучителни цели.

3. Реализация на примерен модел за откриване на вътрешни заплахи

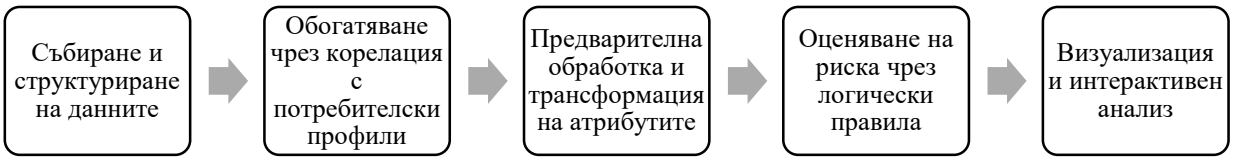
В рамките на настоящото изследване е приложен примерен аналитичен модел за обработка, анализ и визуализация на данни, свързани със сценарии на вътрешни заплахи, чрез използване на офис приложението Excel. Разработеният модел комбинира механизми за предварителна обработка на данни, логически правила за оценяване на риска и интерактивни средства за визуален анализ на потребителското поведение. Използваният подход има демонстрационен и изследователски характер и цели да покаже възможностите на офис приложенията за изграждане на базова аналитична среда при анализ на вътрешни заплахи.

Аналитичен модел за поведенчески анализ и оценяване на риска

Разработеният аналитичен модел представлява последователен процес за събиране, обработка, обогатяване и анализ на данни, свързани с потребителската активност в информационна система. Основната му цел е идентифицирането на

поведенчески индикатори, които могат да бъдат асоциирани с потенциални вътрешни заплахи.

Архитектурата на модела обхваща няколко основни етапа като събиране и структуриране на данните, обогатяване на логовете чрез корелация с потребителски профили, предварителна обработка и трансформация на атрибутите, оценяване на риска чрез логически правила, както и визуализация и интерактивен анализ на резултатите (вж. *Фиг. 10*). По този начин се формира базов модел за поведенчески анализ, при който различни характеристики на потребителската активност се комбинират с цел формиране на обобщена оценка на риска.



Фиг. 10. Архитектура на аналитичния модел
Източник: Разработка на автора

Моделът прилага корелационен подход, при който действия, които поотделно не представляват съществен риск, при комбиниране с други индикатори от Таблица 1 формират обобщена оценка на риска (Threat Score), използвана за класификация на потребителската активност по нива на заплаха.

Оценяването на риска е изпълнено чрез логически зависимости и предварително дефинирани прагови стойности, които моделират принципите на системите за откриване на вътрешни заплахи. В този контекст по-високото ниво на риск се асоциира с натрупване на множество поведенчески отклонения, а не с единични събития. Това позволява по-балансирана интерпретация на активността и намалява вероятността нормални оперативни действия да бъдат неправилно класифицирани като инцидент по сигурността.

Разработеният модел не цели изграждане на прецизна математическа или статистическа система за оценка на риска, а има за цел да демонстрира концептуален подход за внедряване на базов аналитичен механизъм чрез използване на офис приложения и логически правила. В реални организационни среди подобни модели обикновено се надграждат чрез методи на машинно обучение, статистически анализ и UEBA платформи, които позволяват динамична адаптация към поведението на потребителите и спецификата на организационната среда.

Като част от информационното табло е внедрена Threat Investigation Console, предназначена за обобщено представяне на основните показатели за риск, нивото на заплаха и поведенческите индикатори за конкретен потребител. Подобен подход е характерен за центровете за сигурност (Security Operations Center – SOC), насочени към откриване, реагиране и предотвратяване на заплахи чрез обединяване на технологиите и операциите по киберсигурност (Scapicchio et al. n.d.), както и за UEBA платформите, при които визуализацията и интерактивният анализ са ключов елемент при мониторинга и разследването на инциденти.

Прилагането на модела върху синтетичен набор от данни класифицира 27 събития с ниско (Low), 74 със средно (Medium), 84 с високо (High) и 15 с критично ниво на риска (Critical). Събития с ниво High или Critical са установени при 28 от 30-те потребители, като най-голям е броят им в отдел IT (27 от 40 събития, от които 5 критични), следван от отделите Sales (17) и R&D (14). При сравнение със заложените в данните етикети моделът класифицира като High или Critical 37 от 48-те рискови събития (77%), включително всичките 5 събития с критичен етикет. Същевременно 30 от 107-те събития с нисък етикет са класифицирани като високорискови, което показва, че статичните прагове водят до относително голям брой фалшиво положителни резултати и обосновава необходимостта от надграждане на модела чрез методи на машинно обучение.

. Ограничения и възможности за надграждане на модела

Въпреки осъществените функционалности, разработеният модел има ограничения, свързани с използваната технологична среда и демонстрационния характер на изследването. Microsoft Excel предоставя средства за обработка, структуриране и визуализация на данни, но не е предназначено за обработка в реално време, а обемът на анализираните данни е ограничен до 1 048 576 реда на работен лист. Стандартните функции на приложението не включват алгоритми за машинно обучение, въпреки че тази възможност вече е налична чрез Python в Excel (Microsoft n.d.). Допълнително ограничение е зависимостта от предварително дефинирани логически правила и статични прагови стойности при оценката на риска. Макар подходът да позволява изграждане на базов механизъм за оценяване на риска, той не осигурява достатъчна адаптивност към динамично променящо се потребителско поведение и организационен контекст.

Съществено ограничение е и използването на синтетичен набор от данни, генериран с демонстрационна и изследователска цел. Макар подобен подход да позволява моделиране на различни сценарии и интегриране на аналитични механизми

без използване на реална организационна информация, той не може напълно да възпроизведе сложността и динамиката на реалните корпоративни среди.

При реални системи за откриване на вътрешни заплахи обикновено се използват специализирани SIEM и UEBA платформи, които осигуряват автоматизирана корелация на събития, обработка на данни в реално време и прилагане на алгоритми за машинно обучение. Подобни системи използват статистически и поведенчески модели за откриване на аномалии и могат автоматично да адаптират механизмите за оценяване на риска спрямо променящите се модели на потребителска активност.

В бъдеща разработка моделът може да бъде надграден чрез използване на автоматизирано събиране на логови данни, интеграция със SIEM платформи, UEBA механизми за поведенчески анализ, статистически методи за откриване на аномалии, алгоритми за машинно обучение, обработка на данни в реално време и механизми за прогнозен анализ на рисково поведение. Подобно разширяване би позволило изграждане на по-адаптивна и интелигентна аналитична среда, способна да идентифицира сложни поведенчески зависимости и потенциални вътрешни заплахи в динамична организационна инфраструктура. Пряка възможност за надграждане в рамките на същата среда предоставя Python в Excel (Microsoft 365), който позволява използването на библиотеки като pandas и scikit-learn за статистически анализ и обучение на модели за откриване на аномалии директно върху данните в работната книга.

За по-ясно позициониране на разработения модел спрямо специализираните решения е изготвено сравнително представяне на основните характеристики на разгледаните технологии (вж. Таблица 2).

Таблица 2

Сравнение между Microsoft Excel, SIEM и UEBA решения за анализ на вътрешни заплахи

Характеристика	Microsoft Excel	SIEM	UEBA
Цена	Ниска	Висока	Висока
Лесно внедряване	Да	Частично	Частично
Работа в реално време	Не	Да	Да
Машинно обучение	Ограничено	Ограничено	Да
Подходящо за обучение и POC	Да	Да	Да
Подходящо за корпоративна среда	Ограничено	Да	Да

Източник: Разработка на автора

Сравнението показва, че Microsoft Excel не може да замени специализираните SIEM и UEBA решения в корпоративна среда, но е подходящ като нискобюджетна и

лесно достъпна среда за обучение, прототипиране и предварителен анализ. Това определя и ролята на разработения модел като начален етап, който може да бъде надграден чрез специализирани платформи и методи на машинно обучение.

Заключение

Възможностите на Microsoft Excel за обработка, анализ и визуализация на данни показват, че офис приложенията могат да служат не само за административни дейности, но и като достъпна среда за разработване на базови аналитични модели в областта на информационната сигурност. Чрез разработения примерен модел беше демонстрирано приложението на стандартните функционалности на Excel при обработка на логове, анализ на потребителска активност и визуализация на индикатори за риск, свързани с вътрешни заплахи.

Разработената аналитична среда, включваща структурирани данни, логически функции, обобщени таблици и интерактивни табла, потвърждава възможностите на офис приложенията за изграждане на аналитични и proof-of-concept решения. Въпреки ограниченията при работа с големи обеми данни и системи в реално време, Excel е подходящ за обучение, научни изследвания и разработване на модели за поведенчески анализ.

Приложен върху синтетичен набор от 200 събития, моделът класифицира като високорискови 77% от заложените рискови събития, включително всички критични, но при относително висок дял фалшиво положителни резултати. Разгледаният подход демонстрира основните етапи при обработка, анализ и интерпретация на данни за потребителско поведение и може да послужи като основа за разработване на интелигентни модели за откриване на вътрешни заплахи чрез машинно обучение.

Използвана литература

Андреев, Е. Киберсигурност и дигитална устойчивост: архитектури, методи и образователни практики. Варна: Стено, 2026. ISBN 978-619-241-440-5.

Сълов, В., Т. Атанасова, Н. Филипова, С. Парушева, П. Петров, С. Сълова, Л. Тодоранова, О. Маринова. Информатика. Варна: Наука и икономика, 2019.

Alexander, M., D. Kusleika. Microsoft Excel 365 Bible. Indianapolis: Wiley, 2022.

Brumfield, C. What is anomaly detection? Behavior-based analysis for cyber threats [online]. CSO Online, 2025 [viewed 02.06.2026]. Available from:

https://www.csoonline.com/article/3822459/what-is-anomaly-detection-behavior-based-analysis-for-cyber-threats.html.

Cappelli, D., A. Moore, R. Trzeciak. The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud). Boston: Addison-Wesley, 2012.

Cisco. What is User and Entity Behavior Analytics (UEBA)? [online]. Cisco, 2026 [viewed 18.05.2026]. Available from: https://www.cisco.com/c/en/us/products/security/what-is-ueba.html.

Gillis, A. S., M. Pratt. What is a proof of concept (POC)? [online]. TechTarget, 2023 [viewed 24.05.2026]. Available from: https://www.techtarget.com/searchcio/definition/proof-of-concept-POC.

IBM. What is insider threat? [online]. IBM, 2024 [viewed 24.05.2026]. Available from: https://www.ibm.com/topics/insider-threats.

IBM. X-Force Threat Score FAQs [online]. IBM, 2026 [viewed 24.05.2026]. Available from: https://www.ibm.com/docs/en/cloud-paks/cp-security/1.11.0?topic=insights-x-force-threat-score-faqs.

IBM. What is security information and event management (SIEM)? [online]. IBM, n.d. [viewed 24.05.2026]. Available from: https://www.ibm.com/think/topics/siem.

Kaspersky Lab. UEBA (User and Entity Behavior Analytics) [online]. Kaspersky Lab, n.d. [viewed 24.05.2026]. Available from: https://encyclopedia.kaspersky.com/glossary/ueba/.

Kent, K., M. Souppaya. Guide to Computer Security Log Management. NIST Special Publication 800-92. Gaithersburg: National Institute of Standards and Technology, 2006. Available from: https://doi.org/10.6028/NIST.SP.800-92.

Microsoft. Open-source libraries and Python in Excel [online]. Microsoft, n.d. [viewed 05.11.2026]. Available from: https://support.microsoft.com/en-us/excel/python/open-source-libraries-and-python-in-excel.

Sarker, I., A. Kayes, S. Badsha, H. Alqahtani, P. Watters, A. Ng. Cybersecurity data science: an overview from machine learning perspective. – In: *Journal of Big Data*. 2020, Vol. 7, No. 1, Article 41. ISSN 2196-1115. Available from: https://doi.org/10.1186/s40537-020-00318-5.

Scapicchio, M., A. Downie, M. Finio. What is a security operations center (SOC)? [online]. IBM, n.d. [viewed 04.11.2026]. Available from: https://www.ibm.com/think/topics/security-operations-center.

Skorich, P., M. Manning. Insider Threat: A Systemic Approach. London: Routledge, 2025.