ИНФОРМАТИКА И КОМПЮТЪРНИ НАУКИ
INFORMATICS AND COMPUTER SCIENCES

ИЗПОЛЗВАНЕ НА ИЗКУСТВЕН ИНТЕЛЕКТ ЗА АНАЛИЗ И КАТЕГОРИЗАЦИЯ НА КИБЕРАТАКИ ЧРЕЗ РАЗПОЗНАВАНЕ НА ПОВЕДЕНЧЕСКИ МОДЕЛИ

Мирослав Стефанов
Университет по библиотекознание и информационни технологии

Резюме: *Докладът представя детайлен анализ на текущото състояние на киберсигурността в България, като се фокусира върху оценката на риска от кибератаки, които засягат или се извършват върху български IP адреси. Изследването разглежда различни подходи и инструменти за събиране и анализ на данни, включително оперативен мониторинг в реално време, използването на honeypot системи, както и анализ чрез Jupyter Notebook и Python, които подпомагат изчерпателния анализ на информацията. Изследването се базира на подход, който включва обобщаване на метаданните, използвани в анализа, и методите за откриване на кибератаки, като подчертава важността на географското местоположение, методите на нападение и тяхната последователност във времето. Анализът подчертава интензивността и разпространението на кибернападенията в страната, както и значителното разнообразие и потенциалната нестабилност на тези атаки. Основната част от анализа представя ключови статистически данни относно кибератаките, които показват активността и широтата на киберзаплахите в страната, включително дескриптивен анализ и клъстерен анализ на нападенията. Разглеждат се корелационни анализи за изучаване на свързването между кибератаките и различни географски региони, както и времевия анализ за откриване на дългосрочни тенденции. Използвайки визуализационни инструменти като 3D бар графика и линейна графика, предоставя подробно представяне на корелациите и промените по време, докато boxplot и KS тест за пригодено сравняване се използват за оценка на разпределението и нормалността на данните. Докладът представя общ поглед за киберсигурността в България, като използва разнообразни методи и инструменти за събиране и анализ на данни с цел идентифициране на ключовите тенденции и потенциалните рискове от кибератаките. Изводите подчертават важността на непрекъснатото мониториране и анализ на кибератаките за откриването на тенденции и бързо реагиране. Важно е да се разработят цели и стратегии за киберзащита, като се вземат предвид регионални, икономически и технологични фактори, които могат да повлияят на киберсигурността. Докладът предлага препоръки за бъдещи изследвания, включително установяването на дългосрочни модели и разработването на прогнозни модели, които да предвидят изменения в тактиките на нападателите и да предложат ефективни превантивни стратегии.*

Ключови думи: *киберсигурност, кибератаки, тенденции, корелационен анализ, времеви серии*

ВЪВЕДЕНИЕ

В настоящата епоха на глобализация и технологично развитие киберсигурността е от съществено значение за националната и корпоративната сигурност. Процесите на цифровизация и увеличаване на зависимостта от интернет технологиите променят начина, по който обществото функционира, като увеличават рисковете от кибератаки. Тези атаки не само представляват заплаха за личните данни на хората, но могат да имат дългосрочни икономически и социални последствия, което подчертава необходимостта от по-ефективни мерки за киберсигурност. В този контекст държавите, включително България, стоят пред предизвикателството да изградят и приложат стратегии за защита срещу все по-сложните и често срещани кибератаки.

България е страна с активно развиваща се информационна и комуникационна инфраструктура (ИКТ) и това я изправя пред нуждата да засилва своите способности в областта на киберсигурността, за което е от решаващо значение да се проучи рискът от кибератаки, които засягат или се извършват върху български IP адреси.

1. МЕТОДОЛОГИЯ НА ИЗСЛЕДВАНЕТО

МЕТОДИ ЗА АГРЕГИРАНЕ НА МЕТАДАННИ

Извършването на оперативен мониторинг в реално време е от съществено значение за ефективното откриване на кибератаки, затова оперативният мониторинг играе ключова роля. Използването на honeypot системи е от съществено значение за засичането на всеки неоторизиран опит за достъп, което гарантира постоянно наблюдение на мрежовата активност. Следващата стъпка е ефективното агрегиране и централизация на събраните данни, които са необходими за аналитичен преглед и оценка. За да бъде осигурена неприкосновеността и надеждността на данните, важно е да бъдат въведени строги мерки за сигурност, които гарантират защита и поверителност на информационните потоци.

МЕТОДИ ЗА АНАЛИЗ И ИНСТРУМЕНТАРИУМ

Аналитичният процес в изследването е организиран чрез използване на езици и платформи, които са широко приложими в сферата на научните изследвания, като Jupyter Notebook и Python. Jupyter Notebook осигурява интерактивност и детайлен анализ на данните. В процеса на анализа се използват различни Python библиотеки: Pandas за ефективно манипулиране и анализ на данните, Matplotlib и Seaborn за интуитивна графична визуализация (Hunter 2007), както и Scikit-learn за прилагане на разширени статистически модели и алгоритми за машинно обучение (Pedregosa 2011).

ОПИСАНИЕ, ИЗТОЧНИЦИ И ПРЕДСТАВИТЕЛНОСТ НА МЕТАДАННИТЕ

В рамките на нашето научно изследване проведохме процедури за стандартизиране на метаданните и последваща валидация, с които да откриваме всякакви аномалии и изключения, които биха могли да окажат влияние върху достоверността на аналитичния процес. Нашият статистически анализ включва инструментариум от различни изчисления за

централната тенденция и разпръснатост – средни стойности, медиани, моди, стандартни отклонения и екстремални стойности. Тези метрики ни помагат да имаме по-пълна представа за разпределението на данните.

- **Мрежа от honeypot системи**

В контекста на настоящото изследване извлечената информация произтича от разширена мрежа от honeypot системи, стратегически разположени в множество урбанизирани агломерации. Тези системи са стратегически разположени в различни общини и институции и имитират различни уязвимости в мрежовата инфраструктура. Целта на тяхното приложение е да служат като средство за привличане и регистриране на неоторизиран достъп и злонамерени действия, предоставяйки данни за поведението и методите на нападателите.

- **Описание на методите за разпознаване на кибератаки**

Главните параметри при идентификацията на киберинциденти включват географското местоположение на нападателите (определено чрез IP адресите), последователността на атаките във времето, използваните методи и вектори на атака (включително сканиране на портове, експлоатация на известни уязвимости) и събраните метаданни, описващи всяко действие.

- **Представителност на данните – период, обем, локации**

Представителността на данните се основава на информация за дневния брой кибератаки и свързаните с тях уникални IP адреси, произлизащи от български източници. Анализът включва данни за едногодишен период, които са разделени на месечни интервали, за да бъде по-лесно обработване и визуализиране на тенденциите.

1. РЕЗУЛТАТИ И АНАЛИЗ НА КАРТИНАТА НА КИБЕРСИГУРНОСТТА В БЪЛГАРСКИЯ НАЦИОНАЛЕН ДОМЕЙН

2.1. Основни статистически данни

- **Дескриптивен анализ**

Анализът на статистическите данни за кибератаките, които са извършени от или на български IP адреси, предоставя важна информация за характера и обема на такива инциденти (вж. Таблица 1). Изследванията показват, че обемът на атаките средно на ден достига до около 162 454 извършени от 89 на брой уникални български IP адреси. Тези данни показват активността и разпространеността на кибератаките в страната. Стандартното отклонение от 108 135 подчертава значителната нестабилност и вариация на дневната активност. Това е сигнал за непостоянство в атаките или за периоди на по-агресивна активност, което е съществено за разбирането на динамиката на киберпрестъпленията и подчертава сериозността и мащаба на киберзаплахите, които засягат региона.

Таблица 1. Анализ на статистически данни на кибератаки със среден брой IP адреси

Изчисление	Стойност
Среден брой дневни атаки	162 454
Среден брой уникални IP адреси на ден	89
Общ брой атаки на ден	1 620 178

Също така средният брой на уникалните български IP адреси, които участват в атаките, е около 89 на ден, със стандартно отклонение от 32, което предполага наличието на известно разнообразие в броя на активните източници на атаки (вж. Таблица 2). Това ни дава представа за големината и за размера на мрежата на атакуващите в рамките на страната.

Стандартното отклонение на дневните атаки от 108 135 и броят на уникалните IP адреси на ден от 32, както и значителното стандартно отклонение от 1 130 543 на общия брой атаки показват високата вариативност и потенциалната нестабилност на страната. Тези колебания в данните за деня могат да сигнализират за различни модели на атаки, които могат да бъдат предизвикани от различни фактори, включително времеви периоди, технически уязвимости и човешки фактори.

Таблица 2. Анализ на статистически данни на кибератаки със стандартно отклонение

Изчисление	Стойност
Стандартно отклонение на дневни атаки	108 135
Стандартно отклонение на уникални IP адреси на ден	32
Стандартно отклонение на общ брой атаки на ден	1 130 543

В рамките на проведеното изследване броят на регистрираните кибератаки за определен ден възлиза приблизително на 1 620 178, с огромно стандартно отклонение от 1 130 543. Този висок индекс подсказва, че има голямо колебание и възможност за големи кибератаки. Откритото съотношение на атаките, които произхождат от IP адреси в България и които представляват около 10.03% от общия брой атаки за деня, подчертава значимата роля, която тези адреси играят в киберсигурността на държавата.

Тази статистика е изключително важна за научния анализ, като предоставя съществени данни относно броя и честотата на кибератаките, свързани с IP адресите в България, както и тяхната връзка с общия обем на международните кибератаки (вж. Таблица 3). Това ни дава

възможност да разберем по-добре локалните модели на кибернападения и тяхната роля в широкия спектър от киберзаплахи.

Анализът на данните разкрива важни характеристики на кибератаките, извършени от български IP адреси. Високото съотношение на атаките спрямо адресите, което достига средно до 1822.71 атаки за всеки адрес, подчертава тенденцията за концентрация на атаките в ръцете на ограничен брой нападатели. Това дава основание да се предположи, че има съществуващи активни кибератакуващи групи, които оперират в рамките на страната.

Таблица 3. Честота на кибератаки от български IP адреси

Показател	Стойност	Описание
Съотношение на българските атаки към българските IP адреси	1822.71	Средно за всеки български IP адрес са извършени около 1822 атаки
Средно съотношение на българските атаки към общия брой атаки	10.03	Средно българските атаки представляват около 10.03% от всички атаки на ден

Средното съотношение на българските атаки спрямо общия брой на атаките, което е около 10.03%, предоставя основа за изследване на влиянието на местните кибератаки в контекста на глобалните киберзаплахи. Този показател подкрепя заключението, че българските източници на атаки са значима част от общата киберактивност и въздействат не само на национално, но и на международно ниво.

Във връзка със споменатата концентрация и значителния обем на общите атаки е изключително важно да се проучат кибератаките от български IP адреси, за да се разработят целенасочени стратегии за киберзащита (Brown 2018). За да се справим ефективно с тези видове атаки, трябва подробно да разберем мотивите, методите и технологиите, които използват нападателите.

- **Клъстерен анализ на кибератаките**

Извършеният анализ предоставя детайлна статистика за три различни клъстера, които представляват групи от кибератаки, сортирани въз основа на различни характеристики, като честотата и източника на атаките. Анализът на тези данни предоставя ценна информация относно моделите, шаблоните и обхвата на кибератаките, фокусирайки се върху ролята на българските IP адреси в този процес (вж. Таблица 4).

Таблица 4. Клъстерен анализ на кибератаки

Показател	Клъстер 1	Клъстер 2	Клъстер 3
Среден брой атаки	1 087 073	6 140 481	2 075 983
Минимален брой атаки	0	4 222 992	1 060 602
Максимален брой атаки	2 310 624	7 559 298	5 701 032
Стандартно отклонение на атаки	468 478	1 281 068	781 073
Среден брой БГ IP	72.64	112.83	112.51
Минимален брой БГ IP	0	85	70
Максимален брой БГ IP	140	143	157
Стандартно отклонение на БГ IP	27.48	28.42	20.59

Клъстер 1 се характеризира с най-ниския среден брой атаки – 1 087 073, което предполага, че този клъстер включва по-малко агресивни или по-рядко срещани форми на кибератаки (Smith & Jones 2017). Наблюдението за минимален брой атаки, равен на нула, предполага периоди на намаляваща активност или пълна липса на такива, докато максималният регистриран обем от 2 310 624 и ниското стандартно отклонение от 468 478 подчертават стабилността в разпределението на атаките в този клъстер. Средният брой засечени IP адреси в България, участвали в атаките, е относително нисък – 72.64, с минималното стандартно отклонение от 27.48, което предполага стабилност и липса на резки пикове в активността.

Клъстер 2 се отличава със значително по-висок среден брой атаки – 6 140 481, което показва, че клъстерът включва много активни атаки или атаки с голям мащаб. Стандартното отклонение на атаките 1 281 068 е значително, което показва, че въпреки високия среден брой атаки, има съществени колебания в тяхната честота (Lee & Kim 2018). Това се свързва с периодични или сезонни кампании. Българските IP адреси също показват високо средно ниво 112.83 и най-голям максимален брой 143, което подчертава значимата роля на българските източници в този клъстер.

Клъстер 3 представлява средният диапазон между първите два клъстера по отношение

на средния брой атаки от 2 075 983. Показва най-голямо разнообразие в обема на атаките, което се отразява в максималния обем от 5 701 032 и стандартното отклонение от 781 073. В този клъстер се включват различни видове атаки или такива, които са повлияни от специфични външни събития. Средният брой на IP адресите в България е подобен на този в Клъстер 1 (112.51), но ниските стойности на стандартно отклонение от 20.59 показват постоянна активност във времето на атакуващите групи в България.

Изследването на големия брой кибератаки, извършени от български IP адреси в определени категории, подчертава необходимостта от по-детайлно познание за регионалните особености на такива инциденти. Важността на тази информация е подчертана в работата на Thompson и неговите колеги (Thompson 2019), които призовават за разширено научно изследване на влиянието на тези атаки върху глобалната киберсигурност. Това ни помага да идентифицираме ключовите аналитични елементи и модели, необходими за наблюдение и предотвратяване на потенциални заплахи, както разискват Rodriguez и Anderson (Rodriguez & Anderson 2020).

2.2. Корелационен анализ по време и събития

След изследване на връзките между кибератаките и различните географски региони, забелязваме силна свързаност в Бургас с корелация от 0.632924, което подсказва значително влияние на географията върху модела на атаките в този регион (вж. Таблица 5). Изглежда, че географското местоположение играе важна роля за киберзаплахите там. Варна и Пловдив, от друга страна, показват по-слаба свързаност с корелации от 0.132300 и 0.082618 съответно, което ни дава основание да предположим, че тези региони не са толкова засегнати от киберзаплахите, обусловени от географията. Интересно е да отбележим и силната корелация над 0.9 за Харманли, София и Велинград, което подсказва концентрираност на атаките или присъствие на специфични заплахи в тези райони.

Таблица 5. Корелационен анализ на събития

Град	Корелация	Сила на връзката
Бургас	0.632924	умерена до силна връзка
Варна	0.132300	слаба връзка
Пловдив	0.082618	много слаба връзка
Харманли	над 0.9	силна връзка
София	над 0.9	силна връзка
Велинград	над 0.9	силна връзка

При корелационен анализ по време става ясно, че има по-силни връзки при използването на седмични и месечни времеви интервали в сравнение с дневните (вж. Таблица 6). Това е индикация за по-ясно дефинирани модели на кибератаки в по-дългосрочен план. Например ДАЕУ показва висока свързаност в трите времеви интервала, което подсказва стабилност и

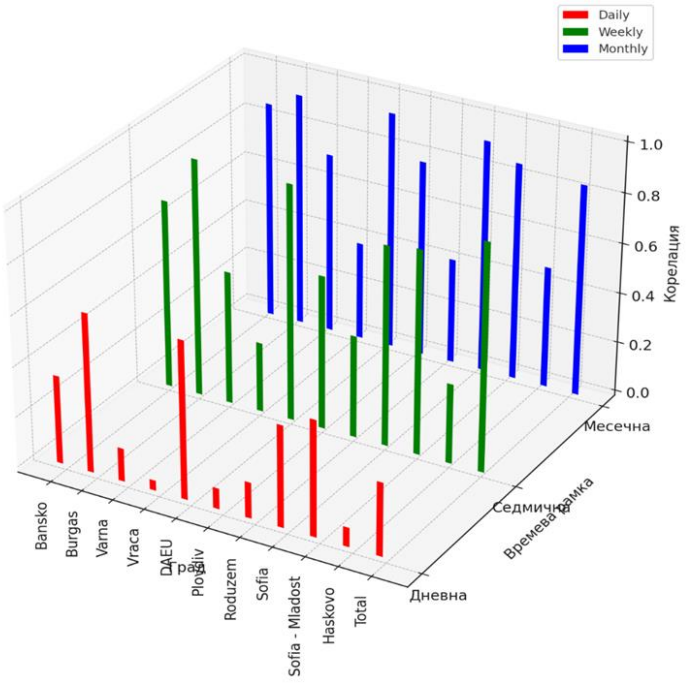
предвидимост в атаките. В същото време градовете Враца и Хасково имат по-ниски стойности на свързаност, особено при дневна база, което означава по-случайни или различни модели на кибератаки.

Таблица 6. Корелационен анализ по време

Град	Дневна корелация	Седмична корелация	Месечна корелация
Банско	0.3511	0.7515	0.8701
Бургас	0.6329	0.9457	0.9337
Варна	0.1323	0.5313	0.7232
Враца	0.0403	0.2786	0.3921
ДАЕУ	0.6295	0.9404	0.9483
Пловдив	0.0826	0.6133	0.7851
Рудозем	0.1432	0.4080	0.4215
София	0.4051	0.7968	0.9272
София – Младост	0.4621	0.8138	0.8684
Хасково	0.07696	0.3192	0.4858
Total (общо)	0.2921	0.9073	0.8454

2.3. Триизмерна бар графика (3d bar chart)

Този тип графика представлява аналитичен инструмент, използван за визуализиране на корелационните коефициенти между кибератаките и различни географски региони в рамките на различни времеви рамки – дневна, седмична, месечна (вж. фиг. 1). Тази графика осигурява детайлно представяне на вариативността и сравненията на корелациите във всяка времева перспектива и за всеки изследван град, което дава възможност за по-дълбоко разбиране на динамиката на кибератаките и тяхното разпределение в различните региони.



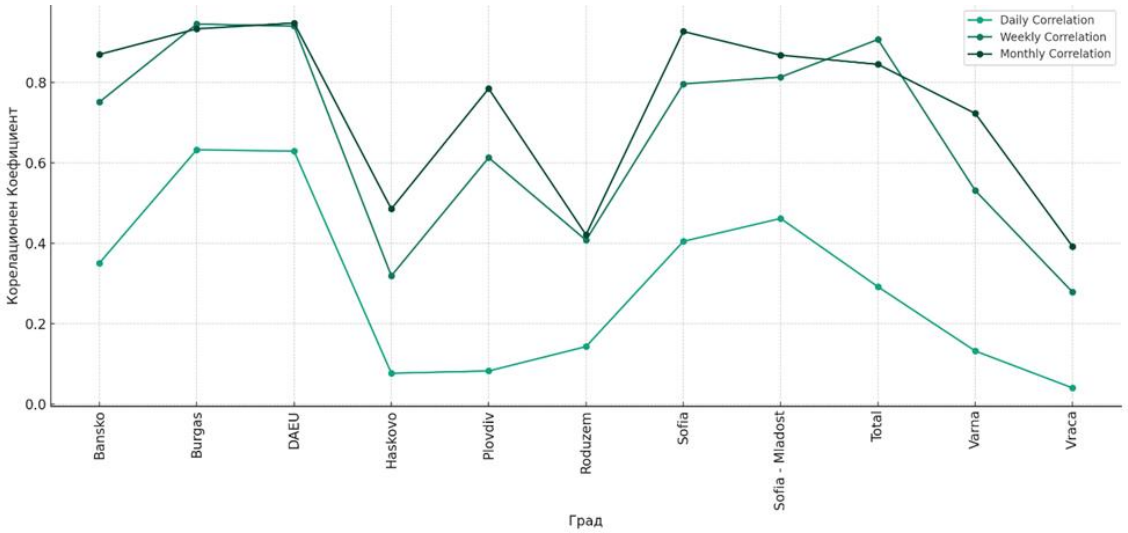
Фиг. 1. Триизмерна графика на корелациите между BG Attack и BG IP

Графиката показва корелационните коефициенти между броя на атаките, извършени от български IP адреси (BG Attack), и броя на уникалните български IP адреси (BG IP) за всяка времева рамка (дневна, седмична, месечна) по отношение на всеки град. Триизмерните барове позволяват визуализация на различията в корелациите през различните времеви периоди и градове, като се вижда, че в общия случай корелациите са по-високи за месечните данни в сравнение с дневните и седмичните. Това отразява по-стабилни дългосрочни взаимодействия между активностите на атаките и наличието на локални атакуващи източници.

2.4. Линейна графика (line chart)

Промените в корелационните коефициенти през времето за всеки град могат да се представят чрез времеви редове, които показват как връзката между кибератаките и географските региони се променя (вж. фиг. 2). Този анализ е полезен за откриване на дългосрочни тенденции и потенциални причини за вариации в киберсигурността, които могат да бъдат свързани с изменения в социално-икономическите условия, технологичното развитие или политическите стратегии за сигурност.

Графичното представяне като линейни графики позволява да видим корелационните коефициенти за всеки град отделно и да направим сравнение между различни градове. Това е особено полезно при откриването на необичайни или изключителни събития, които влияят на киберсигурността в определена област.



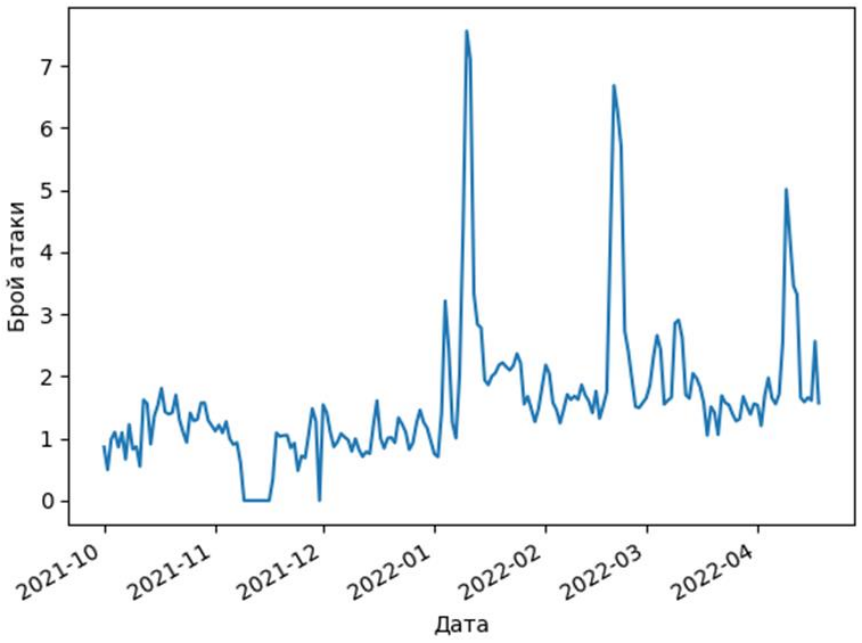
Фиг. 2. Промяна на корелационни коефициенти през времето по градове

Промяна на корелациите във времето: графиката показва, че за повечето градове има по-голяма свързаност в седмични и месечни периоди в сравнение с дневните. Това подсказва за стабилността на отношенията в по-дългосрочен план. Например в градове като Бургас и ДАЕУ високите корелации подчертават последователността на атаките, свързани с местни източници.

Сравнение между градовете: различията в корелациите между градовете могат да отразяват уникални локални условия, които оказват влияние върху киберсигурността. Столицата София и нейните райони като „Младост“ показват значителни корелационни стойности, което подкрепя идеята за интензивна киберактивност в тези райони.

Тенденции и модели: Откритите тенденции могат да бъдат използвани за идентифициране на потенциални рискови фактори или за разработване на адаптивни модели за реагиране на кибератаки. Аномалиите или необичайните събития могат да бъдат изследвани, като се отклоняват от общия модел.

- **Диаграма на динамиката на дневните атаки**



Фиг. 3. Динамика на дневните атаки

На представената графика е изобразена динамиката на дневните кибератаки за периода от ноември 2021 г. до април 2022 г. (вж. фиг. 3). Наблюдава се голяма промяна в количеството на нападенията, като се отбелязват няколко високи върха, които указват периоди на интензивност в кибератаките.

В началото на наблюдавания период броят на атаките остава относително стабилен и нисък, което сочи за период на нормална киберактивност или ефективно предотвратяване на атаките. Впоследствие се наблюдава серия от остри възходи в броя на атаките, които достигат своите върхни точки през месеците декември и февруари, последвани от април. Тези пикове могат да са резултат от специфични кампании на кибератаки, масирано разпространение на вредоносен софтуер или други координирани злонамерени действия.

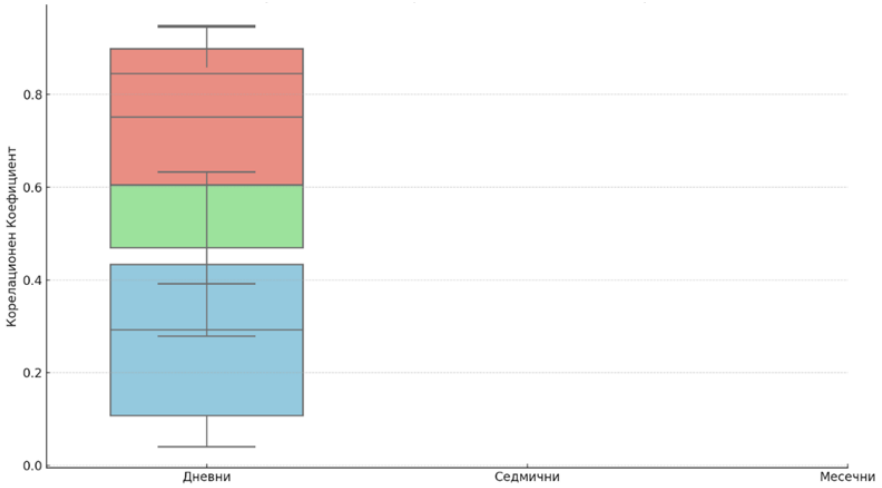
Значителните пикове в броя на атаките също могат да отразяват сезонни тенденции или събития с висока стойност на целите, като празнични периоди или големи търговски събития, по време на които се увеличава броят на онлайн транзакциите и потенциално – уязвимостите за кибератаки.

Общият анализ на графиката подчертава значението на непрекъснатия мониторинг и анализ на кибератаките за идентифицирането на потенциални модели и реагирането в реално време. Също така осигурява ценни данни за изследванията в областта на киберсигурността, които могат да допринесат за разработването на предвидими и превантивни мерки за справяне с бъдещи заплахи.

2.5. Boxplot диаграма

Представената графика е боксплот (boxplot) или кутийна диаграма, която илюстрира разпределението на уникалните IP адреси, участващи в кибератаките на дневна база (вж. фиг. 4). Графиката сама по себе си показва междуквартилния размах (между първия и третия квартил), където се съдържа централната половина от данните, а линията в средата на кутията отразява медианата на разпределението.

От графиката се вижда, че медианата е около 89 уникални IP адреса на ден, но има и дни с много по-висока активност, което се показва от аутлайърите в диаграмата.



Фиг. 4. Boxplot диаграма на корелационни коефициенти за различните времеви рамки

Боксплотът на графиката илюстрира разпределението на корелационните коефициенти между броя на кибератаките от български IP адреси (BG Attack) и броя на уникалните български IP адреси (BG IP) за дневни, седмични и месечни времеви рамки. Този вид визуализация е изключително полезен за оценка на вариабилността на данните и идентифицирането на изключения (аутлайъри).

Дневни данни: Наблюдаваме по-широк спектър на корелационни стойности с медиана, която е по-ниска от тази на седмичните и месечните данни. Това показва, че дневните връзки между BG Attack и BG IP могат да бъдат по-променливи, което отразява дневните флуктуации в кибератаките.

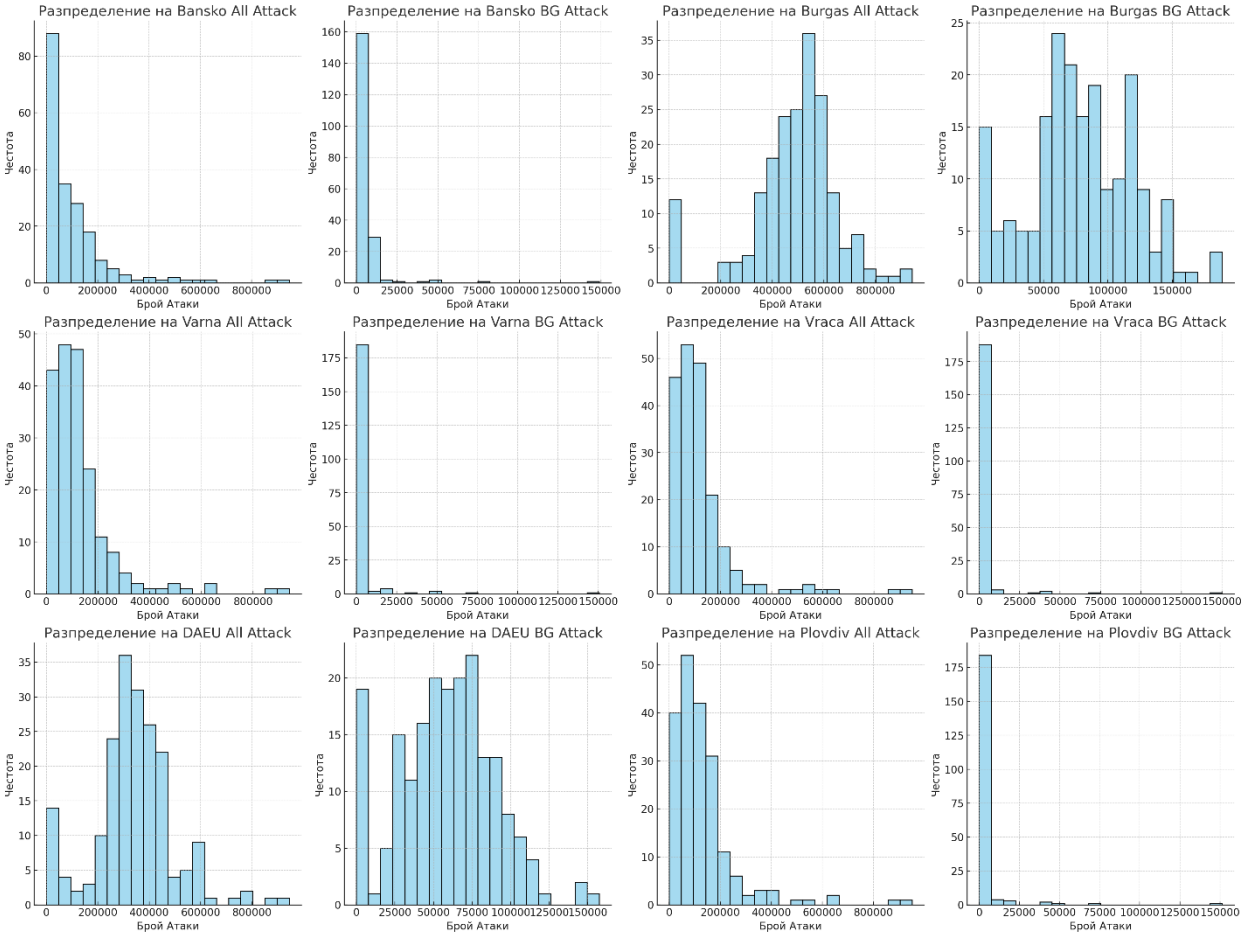
Седмични данни: Седмичните данни показват по-висока медиана и по-малка вариация в сравнение с дневните данни, което предполага, че седмичните връзки са по-стабилни и предвидими.

Месечни данни: Месечните данни се отличават с най-високата медиана и най-слабата вариация, подчертавайки значението на дългосрочната връзка между BG Attack и BG IP.

2.6. KS тест за пригодност

Kolmogorov–Smirnov test (K–S test или KS test) за пригодност е статистически тест, който

се използва за сравняване на емпирично разпределение на извадка с очакваното (референтно) разпределение (вж. фиг. 5). Създадените хистограми предоставят информация за разпределението на атаките за избраните колони. В таблицата са показани KS статистиката и P-стойностите за всяка колона, което ни помага да оценим нормалността на разпределението на данните за атаки.



Фиг. 5. KS тест за пригодност

Ненормално разпределение: за много от колоните (като **Bansko BG Attack**, **Varna BG Attack**, и **Vraca BG Attack**) статистиката на KS е висока, а P-стойността е много ниска (по-малка от 0.05), което показва, че разпределението на атаките значително се различава от нормалното разпределение.

Възможно нормално разпределение: за други колони (като **Burgas BG Attack** и **DAEU BG Attack**) P-стойността е по-висока (по-голяма от 0.05), което означава, че данните не се различават значително от нормално разпределение.

2.7. Описание на картината на киберсигурността

На националния домейн

Графиката представлява корелационна матрица, която илюстрира степента на взаимовръзка между различни видове кибератаки, регистрирани от определени географски точки (вж. фиг. 6). Корелационната матрица използва координати на цветове, за да покаже силата и посоката на връзката между две променливи. Тук е използвана цветова скала от червено до бяло, където:

- Тъмночервено представлява силна положителна корелация (близо до 1).
- Бяло представлява нулева корелация (близо до 0).
- Тъмносиньо представлява силна отрицателна корелация (близо до -1).

От корелационната матрица може да направим следните изводи:

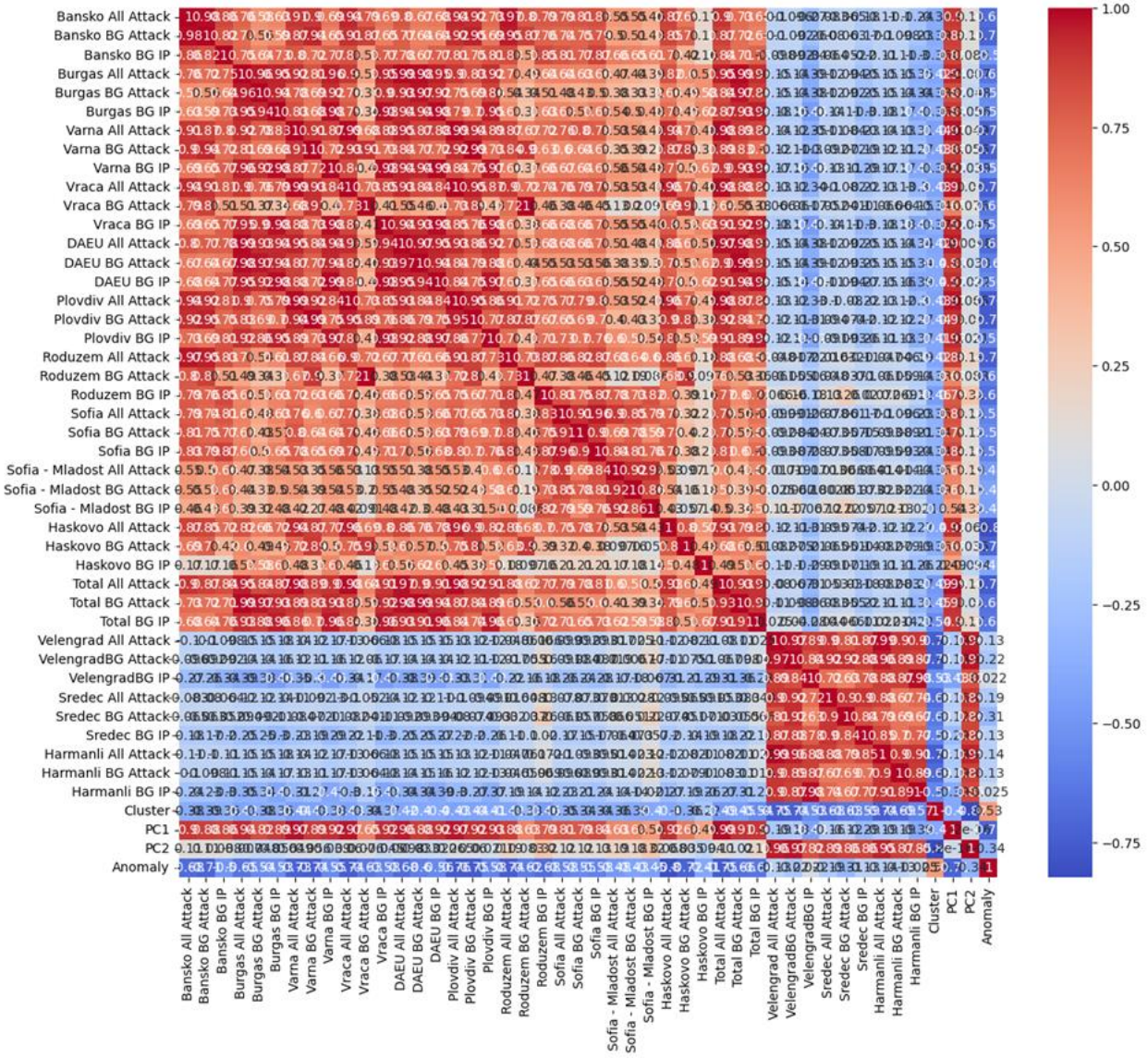
Силни положителни корелации: високи положителни стойности (тъмночервено) по диагонала показват, че всяка променлива е перфектно корелирана със себе си, което е очаквано. Освен това високите стойности между различни атаки и IP адреси в един и същи град или област показват, че колкото повече атаки се извършват, толкова повече уникални IP адреси се използват.

Умерени до високи корелации между градовете: някои видове атаки имат висока положителна корелация помежду си, което показва, че те се случват едновременно или че са резултат от сходни уязвимости или тактики на нападателите. Например високите положителни стойности в някои редове и колони могат да индикират, че определен тип атака се появява едновременно в множество географски региони, което би могло да покаже координирана атака или глобална киберзаплаха.

Различия в корелационните стойности: различията в корелационните стойности между различните градове и общия брой атаки могат да предполагат, че някои региони имат различно поведение при атаките. Например някои могат да имат по-синхронизирани атаки, докато други – по-независими или случайни модели на атаки.

Интерес представляват и включените компоненти за главни (PC1 и PC2), които предполагат, че има основни фактори или оси на вариация, които обясняват голяма част от наблюдаваните данни. Включването на метрика за аномалии в долната част на матрицата също е ключово, тъй като показва потенциалната способност на модела да идентифицира изходящи данни, които могат да представляват нестандартни или неочаквани атаки.

Корелационната матрица е мощен инструмент за визуализация, който помага да се идентифицират потенциални връзки между различни променливи и може да служи като основа за по-нататъшен анализ, като каузален анализ или разработване на модели за предвиждане на атаките.



Фиг. 6. Корелационна матрица на характеристиките

Анализът на динамиката на дневните атаки, както е показано на графиката, предоставя ценна информация за честотата и интензивността на кибератаките във времето. Според изследване на Sharma и Panigrahi вариациите в броя на атаките могат да бъдат обвързани със сезонни тенденции или глобални събития, които влияят на поведението на нападателите (Sharma & Panigrahi 2012). Допълнително значителните върхове, наблюдавани в графиката, могат да отразяват специфични кампании на кибератаки или разпространението на нови видове вредоносен софтуер, както е отбелязано от Alazab et al. (Alazab, Venkatraman & Watters 2013). Важно е да се отбележи, че такива анализи могат да помогнат на организациите да подобрят своите отбранителни стратегии и да разработят по-адаптивни мерки за реагиране на заплахи в реално време.

ИЗВОДИ

Научният анализ на хистограмите и други графични методи представлява фундаментален подход за изследване на динамиката и моделите на кибератаките, позволявайки детайлно разбиране и формиране на хипотези относно причините за разпределението на атаките. Такива методи са особено полезни за идентифицирането на повишена киберактивност по време на значими национални празници, както е наблюдавано в България, където се регистрира висока честота на атаки в деня на националния празник. Това подчертава важността на специализирани стратегии за превенция на кибератаките особено в периоди с предвидимо увеличение на киберактивността.

Анализът разкрива също така, че определени региони като Варна и Рудозем са „горещи точки“ за кибератаки, подчертавайки необходимостта от разработване на регионално адаптирани стратегии за киберсигурност. Наблюдаваните времеви вариации и сезонни модели изискват допълнителен анализ за оптимизиране на отбранителните стратегии, като се вземат предвид регионални и икономически фактори, които могат да влияят на честотата и интензивността на атаките.

По-тесните интерквартилни интервали (IQR) за седмичните и месечните данни подчертават стабилността на кибератаките във времето, изисквайки внимателен мониторинг и анализ за идентифициране на потенциални аномалии или специфични събития, които могат да предизвикат извънредни атаки.

Научното изследване, включващо данни от honeypot системите, подчертава многостранния характер на кибератаките и подкрепя необходимостта от прецизен анализ и интерпретация на събраните данни. Това включва разработването на динамични и адаптивни подходи, които интегрират реално времеви данни и машинно обучение за справяне с постоянно променящата се природа на киберзаплахите, както и създаването на регионално адаптирани стратегии за сигурност, базирани на корелационни анализи.

Бъдещите изследвания трябва да се фокусират върху установяването на дългосрочни модели и разработването на прогностични модели, които могат да предвиждат изменения в тактиките на атакуващите и да предложат превантивни стратегии. Важно е също така да се включат социално-икономически и психологически фактори за пълното разбиране на мотивите зад кибератаките, което ще спомогне за разработването на комплексни образователни и правни стратегии за справяне с киберзаплахите. Такъв холистичен подход ще допринесе за задълбочено разбиране на киберпространството и ще спомогне за разработването на интегрирани решения за сигурност, като по този начин се повиши защитата срещу кибератаките във всички аспекти на обществото.

REFERENCES
Alazab, M., S. **Venkatraman** & P. **Watters** (2013). Cybercrime: The case of Obfuscated Malware. Global Security, Safety, and Sustainability & e-Democracy, pp. 99–109.
Brown, A. (2018). Statistical Methods for Cybersecurity Analysis. *Journal of Cybersecurity Technology, vol. 2, no. 1, pp. 34–45.*
Hunter, J. D. (2007). Matplotlib: A 2D Graphics Environment. *Computing in Science & Engineering 9.03.2007, pp. 90–95.*
Lee S., & B. **Kim** (2018). Large-Scale Cyber Attack Detection Using Advanced Analytics. *International Journal of Information Security, vol. 19, no. 2, pp. 123–135.*
Pedregosa, F., et al. (2011). Scikit-learn: Machine Learning in Python. *Journal of Machine Learning Research, no. 12, pp. 2825–2830.*
Rodriguez, C. & T. **Anderson** (2020). Strategies for Preventing Cyber Incidents: An Analytical Approach. *Journal of Cyber Policy, vol. 5, no. 1, pp. 76–89.*
Sharma, P. & P. K. **Panigrahi** (2012). A detailed analysis of cybersecurity trends and its impact on cybersecurity policy formulation and implementation. In: *Proceedings of the International Conference on Data Engineering and Communication Technology (pp. 223–231).* Springer, Singapore.
Smith, J. & M. **Jones** (2017). Cybersecurity: The Evolving Nature of Cyber Threats and Attack Patterns. *Journal of Network Security, vol. 15, no. 3, pp. 112–120.*
Thompson, R., et al. (2019). Assessing the Regional Impact of Cyber Attacks in a Global Context. *Security Journal, vol. 32, no. 4, pp. 242–256.*

USING ARTIFICIAL INTELLIGENCE TO ANALYZE AND CATEGORIZE CYBER ATTACKS THROUGH BEHAVIORAL PATTERN RECOGNITION

Abstract: *The article presents a detailed analysis of the current state of cybersecurity in Bulgaria, focusing on assessing the risk of cyberattacks that affect or are carried out on Bulgarian IP addresses. Various approaches and tools are studied for data collection and analysis, including real-time operational monitoring, the use of honeypot systems, and analysis through Jupyter Notebook and Python, which support the comprehensive analysis of information. The research is based on an approach that includes summarizing the metadata used in the analysis and the methods for detecting cyberattacks, highlighting the importance of geographic location, methods of attack, and their sequence over time. The analysis emphasizes the intensity and spread of cyberattacks in the country, as well as significant diversity and potential instability of these attacks. The main part of the analysis presents key statistical data regarding cyberattacks, showing the activity and breadth of cyber threats in the country, including descriptive analysis and cluster analysis of the attacks. Correlation analyses are examined to study the connection between cyberattacks and different geographic regions, as well as time analysis for detecting long-term trends. Using visualization tools such as 3D bar charts and line charts provides a detailed representation of the correlations and changes over time, while boxplot and KS test for fitting comparison are used to assess the distribution and normality of the data. The article provides an overall view of cybersecurity in Bulgaria, using various methods and tools for data collection and analysis, with the aim of identifying key trends and potential risks from cyberattacks. The conclusions underline the importance of continuous monitoring and analysis of cyberattacks to detect trends and respond quickly. It is important to develop goals and strategies for cyber defense, taking into account regional, economic, and technological factors that can affect cybersecurity. The article offers*

recommendations for future research, including establishing long-term models and developing forecasting models that can predict changes in attackers' tactics and offer effective preventative strategies.

Keywords: *cybersecurity, cyber attacks, trends, correlational analysis, time series*

Miroslav Stefanov, PhD candidate
University of Library Studies and Information Technologies
E-mail: m.stefanov@unibit.bg