

## ПОВЕДЕНЧЕСКИЯТ АНАЛИЗ В КРИТИЧНАТА ИНФРАСТРУКТУРА (ВЛИЯНИЕТО НА COVID-19)

Тиана Калеева<sup>1</sup>  
e-mail: [t.kaleeva@unwe.bg](mailto:t.kaleeva@unwe.bg)

### Резюме

*Целта на статията е да представи поведенческия анализ като инструмент за подобряване на сигурността, като се акцентира върху ролята му при обекти от критичната инфраструктура. Въз основа на документален и сравнителен анализ се разглеждат различни технологии и програми, основани на поведенческия анализ, като по този начин се илюстрират освен механизмите на функциониране и ползите от тяхното внедряване, така и тенденциите на развитие в тази област. Посочени са различни предизвикателства за поведенческия анализ, причинени от влиянието на COVID-19 кризата. Представени и предложени са възможни решения за тяхното преодоляване, като се имат предвид финансовите и ресурсни фактори.*

**Ключови думи:** сигурност, критична инфраструктура, поведенчески анализ, COVID-19

**JEL:** M14, L20

### Увод

Съвременният модерен и развит свят както множество възможности, така води след себе си и редица рискове и опасности. Усъвършенстването на технологиите, мобилността и комуникацията може да се разгледа едновременно като положителна промяна, но и като повишена несигурност. За да се реагира своевременно срещу заплахите за сигурността на даден обект и безопасността на лицата, намиращи се на територията му, се налага търсенето и въвеждането на адекватни и също толкова модерни инструменти и технологии.

Пример за такъв иновативен подход е поведенческия анализ. Необходимостта от изучаването му и търсенето на възможности за неговото внедряване е породено от следния изследователски проблем: *нуждата от откриване и прилагане на програми, основани на поведенчески анализ, които да спомогнат за навременната реакция спрямо дадените заплахи и да повишат сигурността, особено на обекти от критичната инфраструктура.*

---

<sup>1</sup> Докторант, катедра „Национална и регионална сигурност“, УНСС

Статията изтъква ролята на поведенческия анализ в сигурността на критичната инфраструктура, представя различни технологии, базирани на анализа на невербалната комуникация, посочва различни предизвикателства, които COVID-19 кризата води след себе си в тази област и предлага решения за тяхното преодоляване.

За постигане на поставената цел, в статията се прилагат документален и сравнителен анализ. Първият се използва, за да се извърши преглед, изследване и интерпретация на наличната информация за изучаваната област, като се анализират различни публични и неклаифицирани документи, свързани с темата. Вторият се прилага по отношение на различните видове програми, основани на поведенческия анализ, за да се извърши съпоставка между тях, да се изследват добрите практики от чуждия опит в областта и да се отправят предложения за тяхното внедряване.

### **Ролята на поведенческия анализ в сигурността**

От втората половина на миналия век все повече внимание се обръща на невербалната комуникация в лицето на поведенческия анализ. Той е фундаментален инструмент в разбирането на човешкото поведение. Невербалната комуникация е външно отражение на емоционалното състояние на даден човек. Всеки един жест и движение могат да бъдат ценен показател за емоцията, която той/тя изпитва в конкретен момент.

Редица специалисти в тази област провеждат експерименти и анализи за интерпретиране на човешкото поведение и нагласи, осъществяват се все повече обучения за разпознаване на враждебното намерение и се разработват и въвеждат различни технологии с цел повишаване на сигурността.

Наблюдават се подобрения в капацитета и възможностите за прилагане на изкуствен интелект и роботика към чувствителни за сигурността среди, като по този начин се предоставя неинвазивна възможност за идентификация на заплахите, прогнозиране на престъпни действия, разпознаване на лъжи и незаконни намерения, включително и да се разкрие наличието на болестно състояние чрез топлинен видео анализ.

В основата на поведенческия анализ е идеята, че вътрешното емоционално състояние на даден човек предизвиква физически и видими промени, които могат да се идентифицират от компютърните сензори и да се обработят като тревожни сигнали в зависимост от създадените алгоритми за тази цел. Приема се, че опасният индивид проявява поведенчески черти, които са различни от нормалните. Те могат да се поставят в две категории – микро и макро.

Лицевите изражения, биометричните показатели, температурата, изпотяването, липсата на очен контакт или необичайната „привъзраност“ към вещи от ръчния багаж спадат към микро групата. Макро групата, от друга

страна, включва по-изявени движения като целенасочено прикриване на лицето или цялото тяло (Blum, 2020).

Пол Екман, виден психолог и анализатор на емоциите и на невербалните жестове, провежда редица проучвания и експерименти и стига до заключението, че има седем универсални лицеви изражения (гняв, отвращение, страх, изненада, щастие, тъга, безразличие), които са характерни за всички хора, дори и те да са с различна култура едни от други или с езикови различия (Paul Ekman Group, n.d.).

Това откритие води до идеята, че всички хора проявяват еднотипни лицеви черти в резултат на дадена емоция, както и идентичен език на тялото, следователно поведенческият анализ може да се използва, за да се определи не само емоционалното състояние на дадено лице, но и неговото/нейното намерение. Прилагането на анализа би имало ключова роля при идентифицирането на враждебно или съмнително поведение.

Екман стига до извода, че масовите устройства като „психологически стрес анализатор“, „гласов анализатор“, „гласов стрес мониторинг“ и други не са особено ефективни, защото улавят стреса, а не измамното поведение. Затова той изследва и разработва няколко технологии за детекция на съмнително поведение, сред които е тренажорът за разпознаване на микроизраженията.

Микроизраженията са мимики с много кратка продължителност в порядъка на една четвърт до половин секунда. Могат да се появят в опит за умишлено прикриване на чувства и емоции или несъзнателно като защитен механизъм. Въз основа на това Екман създава инструмент за обучение Micro Expression Training Tool, включващ модули за сравнение на контрастни емоции и микроизражения с цел обучение и усъвършенстване анализирането на невербалните знаци, който се използва от различни заинтересовани лица, включително служители от Министерство на вътрешната сигурност на САЩ, австралийската федерална полиция и други (Екман, 2011).

Невербалните сигнали като ключови за комуникацията между хората, са и от голяма важност при идентифицирането на враждебно или съмнително поведение. Способността да се интерпретират тези сигнали и прикрити жестове, може да се окаже решаващ фактор в повишаването на сигурността, особено за уязвими обекти с повишено ниво на престъпност или струпване на голяма маса от хора.

## **Поведенческият анализ и критичната инфраструктура**

По своята същност критичната инфраструктура може да се определи като елемент, система или части от нея, намиращи се в една страна, които са от основно значение за поддържането на жизненоважни обществени функции, здравето, безопасността, сигурността, икономическото или

социалното благосъстояние на населението, и чието нарушаване или унищожаване би имало значителни последици за дадената страна в резултат на невъзможността да се запазят тези функции.

В съвременното общество критичната инфраструктура е от изключителна важност за нормалното протичане на икономическите, политически, социални, културни и дори екологични аспекти на развитието на една страна. „Усъвършенстването на защитата на критичната инфраструктура се отнася до нейното непрекъснато развиване и перманентно подобряване. Сигурността на защитата означава гарантирането на по-голяма безопасност и неуязвимост. Стабилността на защитата се свързва с релевантно поддържане и укрепване на обектите на инфраструктурата“ (Гечкова, 2017).

Характерен пример за ролята на поведенческия анализ в сигурността е летищната инфраструктура като част от критичната инфраструктура. Като място със струпване на голяма маса от хора и множество от логистични елементи, осигуряването на неговата безопасност е от голяма важност.

За 2019 г. 4,5 млрд. пътници са използвали въздушния транспорт, което е с 3,6% повече от 2018 г. Съгласно докладът на Международната организация за гражданска авиация от 2019 г. броят на излитанията е 38,3 млн., с 1,7% повече от предходната година. Съотношението на приходите от пътниците към пропътуваните километри също бележи ръст с 4,9%, възлизащи на 8 686 млрд.

Наравно с тези данни докладът показва и че са регистрирани 47 акта на незаконна намеса, включващи 2 атаки на самолети в режим на полет, 10 атаки срещу летища или други авиационни съоръжения, 2 атаки с използване на самолети като оръжие, 5 кибератаки, застрашаващи авиационната безопасност, 3 незаконни изземвания на самолети и още 25 атаки, попадащи в категория „други“ (ICAO, 2020).

Непрекъснато увеличаващият се пътнически поток, който по данни на Международния летищен съвет се очаква да достигне 20,9 млрд. през 2040 г. (Airport Council International, n.d.), както и актовете на незаконна намеса, налагат все по-голяма необходимост от повишаване сигурността на летищната инфраструктура и на безопасността на всички лица, намиращи се на територията ѝ.

За осъществяването на това може да се използва поведенческият анализ, който чрез програмите за наблюдение на пътниците да анализира невербалната им комуникация и да идентифицира потенциална опасност от пътници със съмнително или враждебно поведение. По този начин може да се предотврати опасност за летищната инфраструктура и да се повиши сигурността на територията ѝ.

След събитията от 11-ти септември техниките за детекция и анализ на поведението се прилагат успешно в летищната сигурност и правоприлагане

в продължение на много години. През 2011 г. пред Камарата на представителите на САЩ висши служители на Администрацията за транспортна сигурност (АТС) представят независим доклад върху Американската програма за детекция на поведението към АТС, проведено по искане на Дирекция „Държавна сигурност“. Той показва, че персонал, който е обучен да анализира поведението, има 9 пъти по-голяма вероятност да идентифицира лицата с престъпни намерения, отколкото персоналят, който не е преминал такова обучение (Advanced Security & Risk Solutions, n.d.).

Изследваната програма е Screening of Passengers by Observation Techniques (SPOT) и макар да предизвиква множество дебати след представения независим доклад по отношение на ефективността си, подава тласък в посока на въвеждане на поведенческия анализ в сигурността. Друг американски пример за такава програма е Future Attribute Screening Technology (FAST), целяща бързото и обективно идентифициране на съмнителни лица, която е проектирана за използване при контролно-пропускателни пунктове за подпомагане дейността на служителите по сигурността (Homeland Security, 2014).

Израел, от своя страна, също бележи значителни успехи в тази посока. Компанията Suspect Detection Systems (SDS), основана от специалисти в сектора на сигурността, е лидер в технологиите за разпознаване на поведението в борбата с тероризма и предотвратяването на престъпления. Софтуерът COGITO е внедрен в повече от 15 страни и се прилага както от предприятия, така и от правоприлагащи органи, включително за проверка на летища и контролно-пропускателни пунктове и детекция на терористи, нелегални имигранти и контрабандисти (Suspect Detection Systems, n.d.).

Австралийската компания SecureWorx, предоставяща напреднали и модерни услуги за ИТ сигурност, разработва видео базирана технология за поведенчески анализ (Human Behavior Technology). Технологията разпознава субектите, разбира поведението им, идентифицира отклоненията от нормалното поведение и проследява предсказуемостта на поведението. Може да се прилага за разкриване на контрабандни действия, за осигуряване на безопасност на персонала, както и за ранна детекция на групово или индивидуална подозрителна дейност (Greig, 2021).

### **COVID-19 и предизвикателствата пред поведенческия анализ**

Макар поведенческият анализ да се развива непрекъснато, да се търсят различни и иновативни възможности за неговото подобрене и приложение, предизвикателства продължава да има. Адекватният и навременен отговор към тях е от съществена значимост. Пример за такова предизвикателство е именно COVID-19 кризата. Може да се наблюдават няколко аспекта в тази проблематика.

На първо място, предвид ситуацията, е здравето и живота на всеки един индивид. Струпването на голяма маса от хора, характерно за критичната инфраструктура, в ерата на COVID-19 означава по-голям риск от заразяване и разпространяване на вируса. Една от основните и най-често използвана предпазна мярка е носенето на маска.

Маските обикновено покриват долната половина на лицето (най-общо казано устата и носа), като това означава, че за анализ на емоцията остава само горната част (очите и зоната около тях). Това може да доведе до объркване в интерпретацията на изражението, тъй като се наблюдава само една зона от лицето. Фокусирането само върху едната половина на лицето повишава склонността към объркване на едни емоции с други, както и затруднява правилното интерпретиране на лицевите изражения (Arnold, Nestor, Fischer, 2020).

Маските могат и да възпрепятстват разпознаването на вече споменатите микроизражения, които подсказват за скрита или прикрита емоция. Тъй като разпознаването на съмнително и опасно поведение, включително и измамно такова, се извършва основно на базата на микроизраженията, маските могат да затруднят или намалят ефективността на анализа на този ключов компонент на невербалната комуникация (Attia, 2020).

На второ място следва да се отбележи, че макар основно маската за лице да се прилага за предпазване от заразяване, може да се използва и умишлено за прикриване на лицевите изражения. Ако това наистина е намерението за нейното носене, предвид въведените покрай COVID-19 мерки, поставената маска може да не се интерпретира като съмнително поведение, изискващо реакция и допълнителна проверка, както би било в други ситуации.

Тези проблеми налагат въвеждането на нови или приспособяването на вече съществуващите програми въз основа на поведенческия анализ, които да отчитат възможността за умишлено прикрита самоличност или емоция, както и за наличие на скрити лицеви зони и необходимостта от насочване на вниманието върху откритите такива.

Друг важен аспект е именно финансовият. Внедряването на специфична технология за поведенчески анализ изисква значителни ресурси. Според независим одитен доклад от 2013 г. горепосочената програма SPOT за периода 2007 – 2012 г. има калкулирани разходи на стойност 878 млн. щатски долари и повече от 2800 служители, назначени на пълно работно време. Необходимо е като работещи с такава технология, те да преминават и през първоначално и последващо обучение (Department of Homeland Security, 2013), т.е. все елементи от внедряването на такива технологии, които изискват голям ресурс. Затова въвеждането на програми, базирани на пове-

денческият анализ, следва да се извърши като се вземат под внимание необходимите и налични ресурси.

Не на последно място стои и факторът комфорт. Ако отново се разгледа като пример летищната инфраструктура, се наблюдава наличието на множество от пътници, изпращащи и придружаващи лица, както и служители, които се намират на територията ѝ. Тяхната безопасност е от огромно значение, но това не означава, че за да се постигне, се налага да се внесе напрежение, стрес или тревога, причинени от допълнителни проверки и/или контролна дейност.

В епидемиологичната обстановка наличието на допълнителни проверки вече присъства на територията на летищата, затова въвеждането на нови такива, би нарушило известния комфорт за пътуващите. Възможно е да причини и забавяне в целия процес на проверка. Това, от своя страна, може да доведе до недоволство и до враждебно поведение – точно това, което се цели да бъде избегнато и/или навреме идентифицирано.

Програмите, основани на поведенческият анализ, предоставят възможност за улесняване на процеса по контрол и проверка, но в периода на COVID-19 те следва да бъдат адаптирани към новата обстановка, за да успеят да съчетаят комфорта и сигурността в едно.

### **Възможни решения**

Един от възможните подходи, който може да се приложи е изместване на фокуса на поведенческият анализ – наблюдаване поведението на цялото тяло. Според Джо Наваро (бивш агент на ФБР и експерт в невербалната комуникация) често при анализа на невербалната комуникация вниманието се концентрира основно върху лицата на хората, а всъщност трябва да се наблюдава и анализира поведението на цялото им тяло (Navarro, 2020). Това е особено важно днес, след като лицата ни остават скрити зад предпазните маски. Затова приспособяването на анализа към видимите зони на тялото, които издават намерението на лицата, би било от голяма полза при детекцията на съмнително или враждебно поведение.

Друг подход може да се приложи, като се запази фокуса върху лицевите изображения, но се насочи към откритите части на лицето. Очите, визуалния контакт, посоката на гледане, големината на зениците, честотата на мигане, движението на клепачите и веждите и дори бръчиците около очите са проводник на информация, която правилно интерпретирана може да посочи за враждебно, съмнително или измамно поведение.

Неслучайно митническите инспектори в САЩ гледат пътниците право в очите, за да определят честото на мигане, когато питат завърналите се туристи дали имат нещо за деклариране. Ако пътникът започне да мига бър-



зо, вероятно инспекторът ще подложи на проверка багажа му, защото би се усъмнил, че лицето се опитва да прикрие информация. Служителите от правоприлагащите органи също наблюдават темпа на мигане на заподозрения, за да определят дали е виновен или невинен. Според специалисти отклоненият поглед или широко отворените очи могат да са индикация за уплах или чувство на вина. Свитите зеници, от друга страна, на враждебност (Ниренберг, Калеро, Грейсън, 2019).

Положителен пример за технология, концентрирана върху лицевите изразения е софтуерът BioObserver, създаден от компанията Herta. Тя е световен лидер в развитието на решения за лицево разпознаване. Компанията предлага бързи, точни, ясни и ориентирани към крайния потребител решения за видео наблюдение, контрол на достъпа и маркетинговите нужди. Международните ѝ проекти включват платформи за повишаване на сигурността на защитени градове, летища, жп и метро станции, затвори, банки, казина, спортни стадиони, търговски центрове, военни и полицейски приложения. Част от продуктите са насочени и към идентифициране на измамно поведение (Herta, n.d.a).

Софтуерът BioObserver бележи значителна промяна в изследването на човешкото поведение и анализа на лицевото изразение. Базиран на напреднала технология на изкуствен интелект BioObserver автоматично хваща и отбелязва лицевите изразения на човека и микроизразенията му, както и посоката на погледа и ориентацията на главата, за да наблюдава поведенческите черти (като емоционално състояние или нива на внимание). С BioObserver може да се идентифицират микроизразения като „намръщване“, „мигане“ или „повдигане на вежди“. Софтуерът разпознава 7-те базови емоции, както и 18 микроизразения (Herta, n.d.b). Автоматичният анализ може да се извършва както на база записано видео, така и в реално време, което би го направил изключително полезен за обекти от критичната инфраструктура.

Въпреки възможностите, които предоставят технологиите за поведенчески анализ по отношение на идентифицирането на враждебно и съмнително поведение, трябва да се вземе предвид финансовия фактор. Оптималният баланс между ефективни резултати и налични ресурси може да е трудно постижим. Затова следва да се разработва или внедрява технология, която да отговаря на нуждите на конкретната инфраструктура.

Повечето компании, развиващи се в тази сфера, предоставят както по-богати и универсални програми, така и възможност за внедряване само на отделни компоненти, които биха били по-необходими от други спрямо нуждите на дадения обект от критичната инфраструктура. Така едно добро решение може да бъде получено и внедрено на достъпна цена.



Човешкият фактор също е важен и следва да се вземе под внимание. Технологиите, основани на поведенческия анализ, подпомагат процеса по идентификация на съмнително поведение особено при струпването на множество от хора, но това не елиминира необходимостта от служители, които да наблюдават процеса и да се намесят при необходимост. Обучаването им е ключово за ефективното прилагане на програмите за поведенчески анализ, но то също изисква финансови ресурси.

### **Заклучение**

Въпреки че епидемията от COVID-19 затруднява провеждането на поведенчески анализ и по този начин се отразява негативно върху него, то тя сама по себе си предоставя и големи възможности в тази област. Необходимостта от решение, което да е едновременно съобразено с епидемиологичната обстановка, да е ефективно по отношение на детекцията на съмнително, измамно или враждебно поведение, да функционира на територия, част от критичната инфраструктура, без да води до неудобство за лицата, намиращи на нея и без да утежнява времево процеса, води до непрекъснати иновации, подобрения и търсене на най-доброто възможно решение. Макар да звучи като амбициозна задача, почти невъзможна за осъществяване, особено обвързано с финансови ресурси, под една или друга форма това вече се случва. Посочените в статията технологии са доказателство за това. Те са една малка част от вече съществуващите програми в тази област и още по-малка от бъдещите такива.

### **Използвана литература**

- Гечкова, Т. (2017). Приоритизиране на мерките за защита на националната критична инфраструктура (стратегически акценти), Икономически и социални алтернативи, брой 2, с. 68-76, (Gechkova, T., 2017, Prioritizirane na merkite za zashtita na natsionalnata kritichna infrastruktura (strategicheski aktsenti), Ikonomicheski i sotsialni alternativi, broy 2, s. 68-76), available at: <https://www.unwe.bg/alternativi/bg/journalissues/article/11099>
- Екман, П. (2011). Излъжи ме, ако можеш, Изд. Жануа'98, София. (Ekman, P., 2011, Izlazhi me, ako mozhesh, Izd. Zhanua'98, Sofia).
- Ниренберг, Дж., Калеро, Х., Грейсън, Г. (2019). Как да прочетем човека като книга, Изд. Атеа Букс. (Nierenberg, G., Calero, H., Grayson, G., 2019, Kak da prochetem choveka kato kniga, Izd. Atea Buks).

- Advanced Security & Risk Solutions. (n.d.). What is Behavioral Detection? [Online], available at: <http://advancedsecurityandriskolutions.ie/what-is-behaviour-detection/#:~:text=Behaviour%20Detection%20and%20Analysis%20uses%20a%20combination%20of,be%20intent%20on%20criminal%20attack%20on%20your%20business> (accessed 21 March 2021)
- Airport Council International. (n.d.). Smart Security [Online], available at: <https://aci.aero/advocacy/security/smart-security/> (accessed 20 March 2021)
- Arnold, D., Nestor, M., Fischer, D. (2020). “Masking” our Emotions: Botulinum Toxin, Facial Expression and Well-Being in the Age of COVID-19 [Online], available at: [https://www.researchgate.net/publication/342499792\\_Masking\\_our\\_Emotions\\_Botulinum\\_Toxin\\_Facial\\_Expression\\_and\\_Well-Being\\_in\\_the\\_Age\\_of\\_COVID-19](https://www.researchgate.net/publication/342499792_Masking_our_Emotions_Botulinum_Toxin_Facial_Expression_and_Well-Being_in_the_Age_of_COVID-19) (accessed 20 March 2021)
- Attia, P. (2020). Masking emotion in the age of COVID-19 [Online], available at: <https://peterattiamd.com/masking-emotion-in-the-age-of-covid-19/> (accessed 20 March 2021)
- Blum, S. (2020). Behavior Detection Technology: Screening on The Go, Transport Security International [Online], available at: <https://www.tsi-mag.com/behaviour-detection-technology-screening-on-the-go/> (accessed 22 March 2021)
- Department of Homeland Security. (2013). Transportation Security Administration’s Screening of Passengers by Observation Techniques (REDACTED) [Online]. available at: <https://www.oig.dhs.gov/reports/2013-05/transportation-security-administrations-screening-passengers-observation-techniques> (accessed 23 March 2021)
- Greig, C. (2021). SecureWorx Vision-based Human Behavior Technology [Online], available at: [TIC19020-Chris\\_Greig.pdf](TIC19020-Chris_Greig.pdf) (accessed 22 March 2021)
- Herta. (n.d.a) About Herta [Online], available at: <https://hertasecurity.com/company-facial-recognition/about-us/> (accessed 21 March 2021)
- Herta. (n.d.b). BioObserver. Advanced Facial Expression Analysis for The Study of Human Behavior in Videos [Online], available at: <https://hertasecurity.com/advanced-solution-facial-expression-analysis/> (accessed 20 March 2021)
- Homeland Security. (2014). Future Attribute Screening Technology Fact Sheet [Online], available at: <https://www.dhs.gov/publication/future-attribute-screening-technology> (accessed 22 March 2021)
- ICAO. (2020). Annual Report 2019, The World of Air Transport in 2019 [Online], available at: <https://www.icao.int/annual-report-2019/Pages/the-world-of-air-transport-in-2019.aspx#:~:text=According%20to%20ICAO%E2%80%99s%20preliminary%20compilation%20of%20annual%20global,Presentation%20of%202019%20Air%20Transport%20Statistical%20Results%20page> (accessed 20 March 2021)

- Navarro, J. (2020). Former FBI Agent of 25 Years Explains How to ‘Speed-Read’ Body Language – Now That We’re Wearing Face Masks [Online], available at: <https://www.cnbc.com/2020/04/16/retired-fbi-agent-how-to-read-body-language-during-coronavirus-when-wearing-face-masks.html> (accessed 23 March 2021)
- Paul Ekman Group. (n.d.). Universal Facial Expressions [Online], available at: <https://www.paulekman.com/resources/universal-facial-expressions/> (accessed 22 March 2021)
- Suspect Detection Systems. (n.d.). AI driven insider threat detection [Online], available at: <https://www.sds-cogito.com/> (accessed 21 March 2021)

\*\*\*

## THE BEHAVIORAL ANALYSIS IN THE CRITICAL INFRASTRUCTURE (THE INFLUENCE OF COVID-19)

Tiana Kaleeva, PhD Candidate  
Department of National and Regional Security  
Faculty of Economics of Infrastructure  
University of National and World Economy  
*e-mail: t.kaleeva@unwe.bg*

### Abstract

*The aim of the current article is to outline the behavioural analysis as an instrument for improvement of the security, emphasizing on its role in the critical infrastructure locations. Based on documentary and comparative analysis various technologies and programs based on behavioral analysis are being presented, and in this way, illustrates not only their operating mechanisms and benefits but also the development trends in this sphere. Multiple and diverse challenges for the behavioral analysis caused by the impact of the Covid-19 crisis are also presented. Possible solutions for overcoming them are proposed taking into an account the different financial and resource factors.*

**Key words:** security, critical infrastructure, behavioural analysis, Covid-19

**JEL:** M14, L20