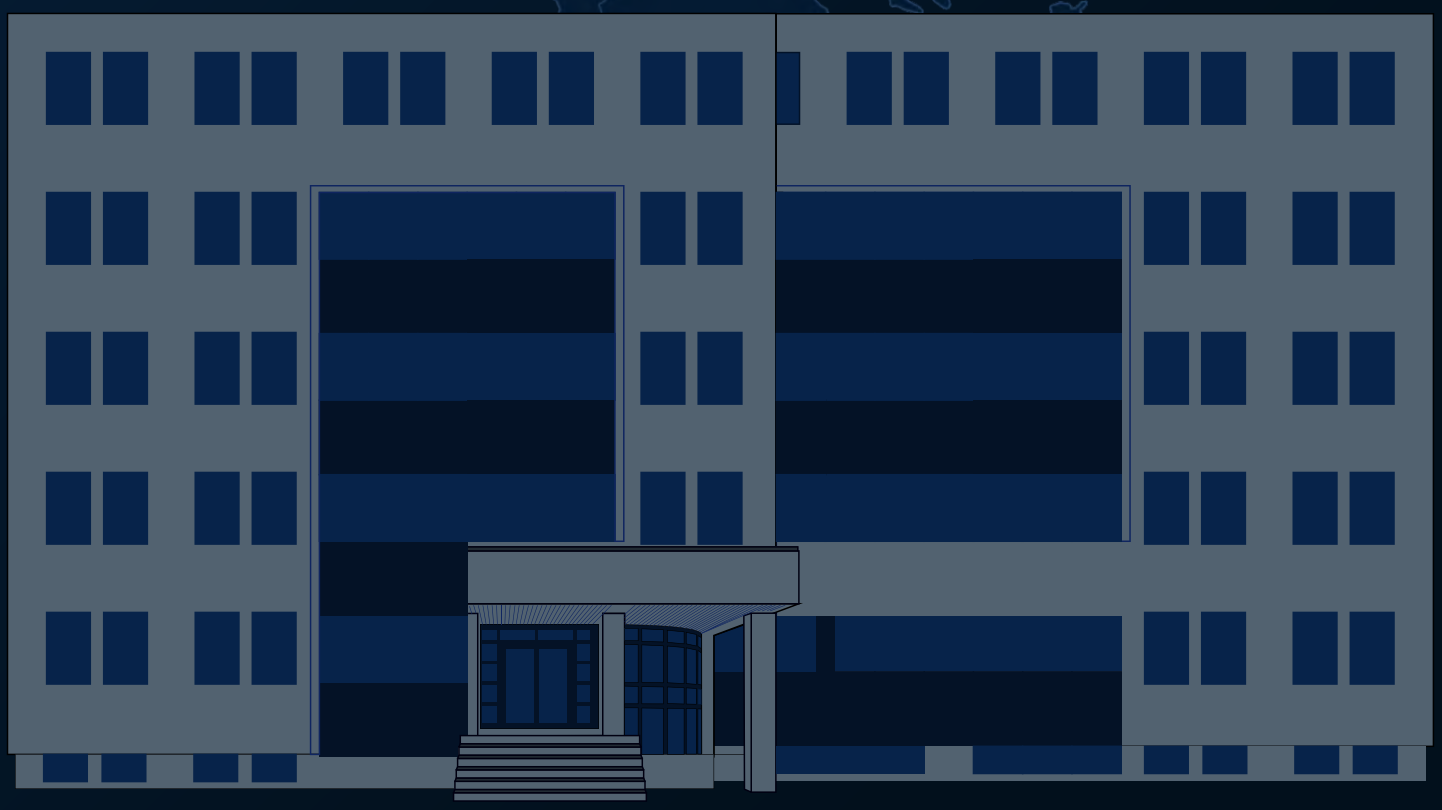
АГЕНЦИЈА ЗА НАЦИОНАЛНА БЕЗБЕДНОСТ

БЕЗБЕДНОСНА ПРОЦЕНКА

ЗА 2027 ГОДИНА



ПОСВЕТЕНИ НА БЕЗБЕДНОСТА
ВЕРНИ НА ДРЖАВАТА

АГЕНЦИЈА ЗА НАЦИОНАЛНА БЕЗБЕДНОСТ

Издавач:
Агенција за национална безбедност на Република Северна Македонија

Уредник
м-р Бојан Христовски

ISBN:
978-608-67632-0-6

Печати:
Зашатитно друштво печатница - Графо Пром, ул. Димитар Влахов бр. 3, Битола

Тираж:
100 примероци

Скопје, 2026

Пријави безбедносна закана

АГЕНЦИЈА ЗА НАЦИОНАЛНА БЕЗБЕДНОСТ

БЕЗБЕДНОСНА ПРОЦЕНКА

ЗА 2027 ГОДИНА

Публикација од јавен карактер за препознавање на ризиците и заканите во РС Македонија

Публикација не содржи класифицирани информации, лични податоци, податоци за конкретни извори на информации, оперативни методи, тековни предмети, информации што би можеле да ја загрозат националната безбедност или да предизвикаат штета во работењето на Агенцијата. Содржината е концепирана на начин што овозможува информираност заради превенција и препознавање на ризиците од страна на јавноста.

Содржина

Воведен збор на директорот на Агенцијата за национална безбедност

Почитувани,

Пред Вас е првата публикација на Агенцијата за национална безбедност која ги оценува ризиците и заканите за државата во 2026 година и вклучува проекција, односно безбедносна проценка за развојот на потенцијалните ризици во 2027 година.

Со објавувањето на оваа публикација, Агенцијата за национална безбедност прави дополнителен чекор кон транспарентноста и партнерството со јавноста. Целта на јавното информирање не е да предизвикаме страв и неизвесност, туку да изградиме општество кое може успешно да се справи со безбедносните предизвици на модерното време.

Користејќи некласифицирани информации што Агенцијата може јавно да ги сподели, нудиме разбирлив приказ на безбедносните предизвици што можат да влијаат врз државата, институциите, економијата и врз секојдневниот живот на граѓаните. Истовремено, најважниот придонес од публикацијата е запознавањето на јавноста со безбедносните појави и феномени во насока на препознавање и поттикнување севкупна општествена активност за нивно спречување.

Националната безбедност не е задача само на една институција. Таа зависи од координацијата на државните органи, одговорноста на приватниот сектор, професионалноста на медиумите, академската експертиза, но најважно и непобитно – од внимателното однесување на секој граѓанин. Информирани, будни и свесни граѓани се одговорни чинители во државниот безбедносен апарат преку активно учество во зачувувањето на националната безбедност. Раното препознавање на ризиците, навременото пријавување на сомнителните појави и проверката на информациите, се важен дел од целокупната отпорност. Безбедноста ја остваруваме со заеднички стремежи.

Современите предизвици, ризици и закани се динамични и променливи. Некои се јасно видливи и лесно препознатливи, додека хибридните закани се одвиваат прикриено.Тие се изразени преку тајно делување на државни и недржавни чинители, напади во сајбер-просторот насочени кон прибирање чувствителни информации, кампањи за ширење дезинформации, економски притисоци и злоупотреба на новите технологии. Нивната најзначајна карактеристика е меѓусебната поврзаност, при што сајбер-нападот може да биде проследен со дезинформации, криминалната активност може да прерасне во средство за влијание, а општествената поларизација може да биде искористена за поткопување на довербата во институциите, што е една од најчестите цели на хибридните закани.

Во вакви услови на комплексна регионална и глобална безбедносна констелација, Агенцијата останува посветена на професионализмот, законитоста, политичката неутралност и почитувањето на човековите права. Во соработка со домашните институции, НАТО и партнерските безбедносно-разузнавачки служби, продолжуваме навремено да ги откриваме и да ги проценуваме заканите остварувајќи ја нашата превентивна улога во безбедносниот систем.

Верувам дека оваа публикација ќе биде мотив за соработка и градење доверба. Информирано општество е отпорно општество, а кредибилитетот се гради со професионално работење, отчетност и транспарентност.

За Агенцијата за национална безбедност, довербата на граѓаните не е опција, туку императив. Безбедноста веќе не се крие зад институционален молк. Со оваа прва јавна публикација, ги уриваме бариерите и јасно покажуваме дека граѓаните се темелот на нашата сила.

Директор на Агенција за национална безбедност
м-р Бојан Христовски

Цел и опфат

Оваа проценка ги прикажува најзначајните безбедносни трендови забележани во 2026 година и веројатните правци на нивниот развој во 2027 година. Публикацијата е наменета за граѓаните, институциите, деловната и академската заедница и за медиумуите. Проценката претставува аналитички продукт заснован на достапни податоци, трендови и споредба на повеќе извори. Ризикот се менува во зависност од геополитичката констелација, намерите и капацитетите на актерите, ранливоста на системот и од ефективноста на превентивните мерки.

Области опфатени со проценката

Стратешка проценка на безбедносната средина, вклучително и на актуелните геополитички случувања, вооружените конфликти, регионалната стабилност

Организиран криминал, коруптивни влијанија и нелегални финансиски текови

Странски разузнавачки активности и влијанија

Сајбер-закани и злоупотреба на новите технологии

Хибридни закани, дезинформации, когнитивни операции и манипулација со информации

Заштита на критичната инфраструктура и на економската, енергетската и истражувачката безбедност

Насилен екстремизам, радикализација и тероризам

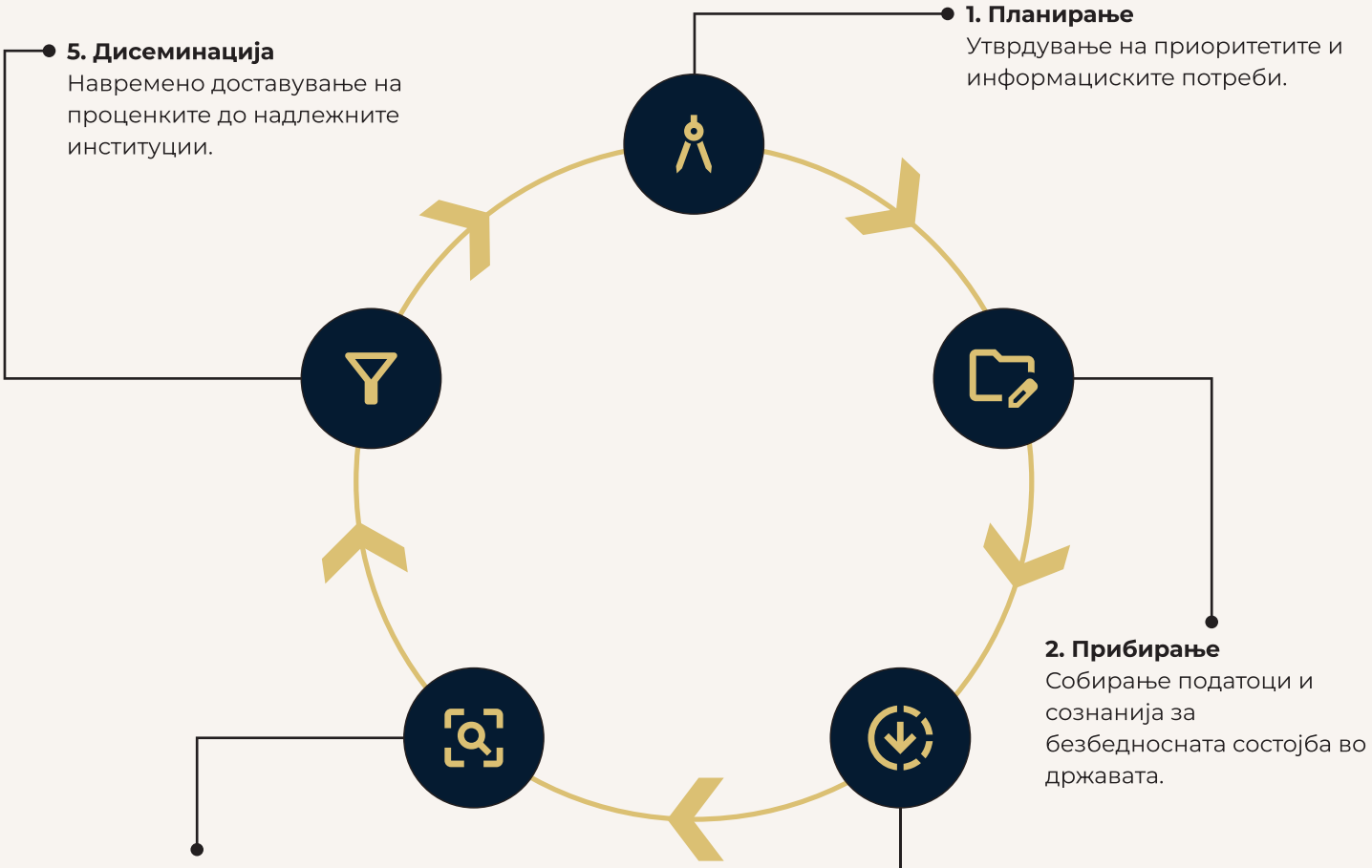
Транснационални миграциски движења

За Агенцијата за национална безбедност

Како дел од реформата на безбедносно-разузнавачкиот систем, со донесување на Законот за Агенција за национална безбедност беше основана Агенцијата за национална безбедност како самостоен орган на државната управа која започна со работа на 1 септември 2019 година. Со донесување на Законот, престана да постои поранешната Управа за безбедност и контраразузнавање како орган во состав на Министерството за внатрешни работи.

Агенцијата придонесува за заштита на националната безбедност, независноста, суверенитетот, уставниот поредок и основните слободи и права на човекот и граѓанинот. Во рамките на законски утврдените надлежности, Агенцијата постапува самостојно, професионално и непристрасно, без влијание од политичките партии.

Агенцијата има превентивна улога во системот за националната безбедност и собира, обработува, анализира, проценува, разменува, чува и заштитува податоци и информации со цел откривање и спречување закани и ризици по националната безбедност.



Надлежности

- Откривање и спречување шпионажа, странско разузнавачко дејствување и други прикриени активности насочени против државните интереси
- Откривање и спречување насилен екстремизам, радикализација, тероризам и негово финансирање
- Откривање и спречување сериозни и организирани криминални активности што можат да ја загрозат државата, финансиската безбедност, човештвото или меѓународното право
- Заштита на носители на високи државни функции и објекти од стратешко значење за државата
- Проценување хибридни, сајбер, економски, енергетски, технолошки и на информациски закани и ризици
- Вршење безбедносни проверки и поддршка на системот за заштита на класифицираните информации
- Други активност поврзани со безбедносни закани и ризици за националната безбедност
- За прашања од значење за националната безбедност, Агенцијата навремено ги информира државниот врв и надлежните државни органи и разменува информации со домашните и странските партнерски служби

Агенцијата не ги смета за безбедносна закана политичките, верските, медиумските, академските или граѓанските активности. Предмет на безбедносен интерес можат да бидат единствено конкретни дејства поврзани со шпионажа, прикриено странско влијание, организиран криминал, корупција, саботажа, насилен екстремизам и тероризам или други активности што претставуваат безбедносна закана.

Меѓуинституционална и меѓународна соработка

Со цел зајакнување на соработката со другите институции, како и заради навремена размена на информации и податоци, Агенцијата за национална безбедност има склучено меморандуми за соработка со повеќе државни органи и високообразовни институции.

Справувањето со современите безбедносни закани бара сеопфатен и координиран пристап и соработка на национално и меѓународно ниво. Агенцијата учествува во националните механизми за координација, соработува со министерствата, органите на државната управа, јавните претпријатија, единиците на локалната самоуправа и со други правни лица, а преку билатерални и мултилатерални канали разменува безбедносно-релевантни информации со партнерски служби, НАТО-алијансата и со други регионални и меѓународни безбедносни форуми.

Јавни показатели за обемот на работа

Со цел рано предупредување и спречување активности поврзани со безбедносни закани и ризици, Агенцијата изготвува разузнавачки информации за внатрешно и надворешно информирање врз основа на оперативни извештаи.

Во текот на една година, Агенцијата во просек спроведува околу 20.000 безбедносни проверки по барање на надлежни државни органи, од кои дел се заради утврдување безбедносни пречки при издавање безбедносен сертификат за пристап до класифицирани информации.

Улога на Агенцијата за национална безбедност

Агенцијата за национална безбедност има клучна улога во изготвувањето безбедносни проценки, раното предупредување и во превенцијата од ризици и закани по националната безбедност. Преку навремено детектирање на потенцијалните опасности, Агенцијата работи на минимизирање на ризиците пред тие да прераснат во закани од поширок размери. За таа цел, Агенцијата редовно доставува релевантни и навремени информации до надлежните органи.

Правна рамка

Агенцијата при извршување на работите од своја надлежност постапува во согласност со Уставот на Република Северна Македонија, законите и со ратификуваните меѓународни договори.

Основен закон со кој се уредува основањето, целта, надлежностите, начинот на работа, организацијата и раководењето, условите и постапката за спроведување на мерките за тајно собирање на податоци и информации, правата и обврските на работниците, контролата и надзорот на Агенцијата за национална безбедност е Законот за Агенција за национална безбедност.

Правната рамка на Агенцијата за национална безбедност ја сочинуваат и подзаконските акти донесени врз основа на Законот за Агенција за национална безбедност, како и интерните прописи и процедури за постапување при вршење на работите од надлежност на Агенцијата.

При вршење на работите од својата надлежност, Агенцијата постапува и согласно:

- **Законот за следење на комуникациите -** претставува правна рамка во која се утврдени условите и постапката за спроведување на мерките за следење на комуникациите заради заштита на интересите на безбедноста на државата, вклучувајќи ги и мета податоците.

- **Законот за класифицирани информации -** со оглед на тоа што најголем дел од податоците со кои располага Агенцијата се определени со степен на класификација.

- **Законот за заштита на личните податоци -** при вршење на работите од своја надлежност Агенцијата собира, обработува и користи лични податоци.

- Агенцијата во вршење на работите постапува и применува и други **прописи од областа на работните односи, финансии и јавни набавки, слободен пристап до информации од јавен карактер** итн.

Основни начела на постапување

Законитост	Секоја мерка и активност мора да има јасна правна основа и да биде спроведена од овластени лица.
Неопходност и пропорционалност	Интензитетот на мерката мора да биде соодветен на природата и сериозноста на ризикот.
Политичка неутралност	Агенцијата не смее да дејствува во интерес на политичка партија или против законска политичка активност.
Заштита на правата	Почитувањето на човековите права и приватноста е составен дел од законитото и професионалното работење.
Заштита на информациите	Класифицираните и личните податоци се чуваат, користат и споделуваат само под законски утврдени услови.
Контрола и надзор	Работењето се одвива под надзор на собраниските тела и други органи, судска и обвинителска контрола, како и преку внатрешната контрола на Агенцијата.

Контрола, надзор и транспарентност

Имајќи ја предвид природата на работата на Агенцијата за национална безбедност, како и можноста за примена на мерки за тајно собирање на податоци и информации, контролата и надзорот врз работата на Агенцијата обезбедува законито, одговорно и професионално работење како и спречување на можноста од злоупотреби.

Внатрешна контрола

Во рамките на Агенцијата за национална безбедност функционира посебна организациска единица за внатрешна контрола, во чија надлежност се оценка на законитоста, почитување на професионалните стандарди, оценка за почитување на прописите и процедурите за работа, постапување по пријави за судир на интереси и ризици од корупција, предлагање мерки за отстранување неправилности, давање иницијативи за поведување постапки за утврдување дисциплинска одговорност и други работи согласно закон.

Работењето на организациската единица за внатрешна контрола придонесува во зајакнување на институционалниот интегритет, законито работење и јакнење на професионалните стандарди.

Надворешна контрола

Контролата на законитоста на спроведувањето на мерките за тајно собирање на податоци и информации за кои наредба издал судот согласно закон, врши Јавниот обвинител на Република Северна Македонија и судијата на Врховниот суд на Република Северна Македонија кој ја издал наредбата.

Надзор

Надзор над работата на Агенцијата за национална безбедност вршат: Собранието - непосредно и преку надлежни работни тела, Народниот правобранител на Република Северна Македонија, Агенцијата за заштита на лични податоци, Дирекцијата за безбедност на класифицирани информации, Државниот завод за ревизија и Советот за граѓански надзор согласно со Законот за следење на комуникациите како и други органи согласно со закон.

Овие институции вршат надзор над законитоста во работењето, почитување на човековите права, заштита на податоците и правилно користење на јавните средства.

Транспарентност

Агенцијата за национална безбедност има законска обврска заради транспарентно информирање и комуникација со јавноста на својата интернет-страница да објавува податоци и информации кои се од значење за работата на Агенцијата, јавно достапни годишни извештаи, јавни огласи за вработување во Агенцијата и друго. Агенцијата може и непосредно да ја информира односно извести јавноста за одредени безбедносни појави и случаи.

Во изминатиот период беше редизајнирана интернет-страницата www.anb.gov.mk која редовно се ажурира со новости поврзани со работењето и активностите на Агенцијата. Агенцијата редовно објавува и документи поврзани со буџетот, завршни сметки и јавни набавки.

Агенцијата за национална безбедност има редовна комуникација со медиумите во поглед на прашања кои се од интерес на јавноста, без притоа да се наруши доверливоста на информациите и податоците со кои располага.

Безбедносно опкружување

Глобално и регионално опкружување

Меѓународната безбедносна средина и натаму ќе биде обележана со силна геополитичка конкуренција, како војната во Украина, нестабилноста на Блискиот Исток, економските и енергетските притисоци, брзиот технолошки развој и сè помалку ј сна. Држ ви е, разуз авачките лужби, ор аниз циите другите вл ј телни групи сè почестата у отреба на ибр- идни редства Г аницата меѓу м рот, поли ичката и еконо ската к нкуренција и т ориот конфликт с анува сè често ги остваруваат своите цели преку комбинација од дипломатски, економски, информативни, сајбер и разузнавачки активности. Западниот Балкан останува чувствителен на политички тензии, етнонационалистички наративи, странско влијание, организиран криминал и миграциски притисоци. Настаните во една држава можат брзо да предизвикаат политички, економски, информативни или безбедносни последици и во соседните земји. Република Северна Македонија ја задржува својата геостратешка важност како транзитен коридор и членка на НАТО-алијансата. Тоа ја зголемува нејзината регионална улога, но и интересот на различни државни и недржавни субјекти за влијание врз домашните процеси.

Во ваквата сложена глобална безбедносна средина во насока на слабеење и поткопување на единството во Алијансата, тероризмот, како и Руската Федерација остануваат главни закани по безбедноста, а Народна Република Кина претставува системски предизвик.

Хибридни закани и манипулација со информации

Хибридните закани претставуваат координирана употреба на повеќе различни средства, како што се дезинформации, сајбер-напади, економски притисоци, корупција, прикриено финансирање, дејствување преку локални посредници и злоупотреба на културни, историски или идентитетски прашања. Во 2027 година се очекува зголемување на ризикот од употреба на вештачка интелигенција за создавање уверливи синтетички содржини кои можат да се користат за дезинформирање и дискредитација односно нарушување на довербата во институциите.

Внатрешни општествени и институционални фактори

И покрај проценката за стабилна и мирна безбедносна состојба во државата, сепак политичката поларизација, поттикнувањето недоверба во институциите, коруптивните ризици, економската несигурност и чувствителните меѓуетнички и меѓуверски прашања можат да бидат злоупотребени за создавање тензии и поделби. Постоењето на различни политички, верски, етнички или општествени ставови само по себе не претставува безбедносна закана, а ризикот се зголемува кога овие прашања намерно се манипулираат со цел ширење омраза, поттикнување насилство, продлабочување на поделбите, блокирање на институциите или намалување на довербата во демократските процеси.

Принцип на отпорност

Националната отпорност претставува способност на државата и општеството навреме да ги препознаат заканите, да ги намалат постојните слабости и да го зачуваат функционирањето на институциите и основните услуги вклучително и во услови на криза. Таа подразбира брз и координиран одговор, ефикасно справување со последиците и што побрзо враќање во нормална состојба.

Безбедносна терминологија

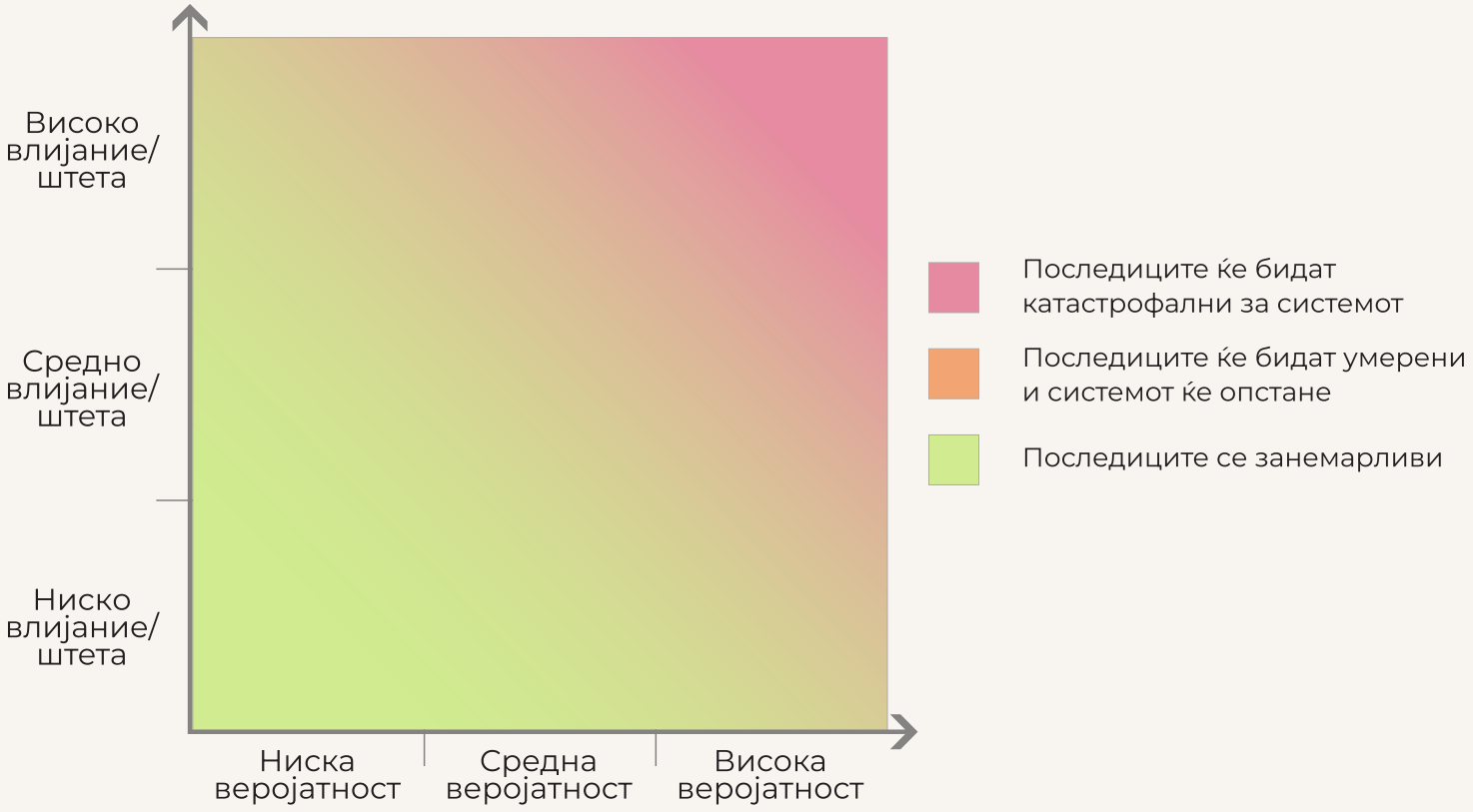
Безбедносен феномен - во безбедносната терминологија го означува секој поединечен настан, процес, појава или состојба во општеството што има потенцијал да влијае врз безбедноста и служи како појдовна точка.

Безбедносен предизвик - комплексна, долгорочна и често непредвидлива состојба или тренд што го принудува безбедносниот систем да се прилагодува, да развива нови стратегии и да ги менува воспоставените практики. За разлика од директната закана, која е моментална и има јасен непријател, безбедносниот предизвик е поширок феномен кој нема секогаш намерна заднина, но долгорочно ја тестира отпорноста на државите и организациите.

Безбедносен тренд - претставува индикатор дали ризиците од појавата или заканата ќе се намалат, ќе останат стабилни или ќе се зголемат.

Безбедносна појава - означува поврзани настани, процеси или однесувања на државни и/или недржавни актери во континуитет, што би можеле да влијаат на вообичаените општествени текови или безбедноста на граѓаните и државата.
Безбедносните појави во општеството се градираат според нивниот интензитет, зачестеност и географски/социјален опсег.

Безбедносен ризик – претставува веројатност одредена безбедносна појава или феномен да предизвика штета, загуба или загрозување на луѓето, имотот, информациите или државата. Ризикот секогаш содржи елемент на неизвесност и се пресметува како комбинација од два фактори: веројатност (колку е реално да се случи) и последица (колку големо влијание/штета ќе предизвика).



Безбедносна закана - е непосредна, конкретна намера и активност за нанесување штета на одредена цел. Истата е составена од намера, план, подготовка и изведување. За разлика од безбедносниот ризик кој претставува веројатност, директната закана веќе постои, таа е насочена и бара итна реакција.

Степенот на заканата се одредува според намерата и капацитетот на противникот.

- **Висока закана** - Јасна намера и целосен капацитет на противникот. Нападот е многу веројатен или веќе е во тек.
- **Средна закана** - Постои капацитет за напад или постои општа намера, но нема индиции за непосреден напад. Противникот сè уште собира ресурси или чека прилика.
- **Ниска закана** - Нема сознанија за намера, а капацитетите на потенцијалниот противник се минимални и безопасни.

Безбедносна проценка - претставува структуриран и методолошки процес на анализа на моментални безбедносни индикатори на одреден настан, општествен процес или појава во насока на предвидување на импликациите и развојот на состојбите во иднината. При проценувањето се зема предвид дека настаните со големо влијание најчесто имаат мала веројатност, но доколку се случат, можат да предизвикаат сериозни и долготрајни последици. Терористички акт, голем сајбер-инцидент или подолготраен прекин на електроенергетскиот систем се релативно ретки појави, но можат значително да го нарушат функционирањето на институциите, економијата и секојдневниот живот на граѓаните. Поради тоа, проценката не се заснова само на зачестеноста на настаните, туку и на можните последици, со цел да се обезбеди континуирана подготвеност за превенција, навремено реагирање и справување и попречување на безбедносни ризици и закани.

Фактори на отпорност

	Членството во НАТО и развиената сојузничка размена на информации
	Европската интеграција и усогласувањето со европските безбедносни стандарди и регионална соработка
	Активното граѓанско општество, независните медиуми и академската заедница
	Развојот на националната рамка за сајбер-безбедност и механизмите за одговор на инциденти
	Зголемената јавна свест за дезинформации, измами и дигитална заштита

Безбедносна проценка за потенцијалните ризици по националната безбедност во 2027 година

И покрај индикаторите поврзани со ефектите од геополитичките и безбедносни случувања на меѓународно и на регионално ниво, но и на домашните безбедносни општествено-политички и економско-социјални предизвици, безбедносната состојба во Македонија во текот на 2027 година се проценува дека ќе биде мирна и стабилна, а нивото на закана по националната безбедност ќе остане ниско.

Сложеното и динамично безбедносно опкружување имплицира зголемен број меѓусебно поврзани ризици и закани по националната безбедност. Сепак, проценката е дека државните институции располагаат со соодветни човечки, технички и организациски капацитети и механизми за нивно навремено и координирано детектирање преку редовна размена на информации, со цел откривање, спречување и ограничување на можните последици врз земјата. Имајќи ги предвид геопозицинираноста, како и заштитните механизми кои ги предвидува членството во НАТО-алијансата, веројатноста од директна и конвенционална воена закана врз Република Северна Македонија останува ниска, а главните безбедносни закани најверојатно ќе се одвиваат прикриено, преку сајбер-напади, дезинформации, разузнавачки активности, операции на влијание, економски и технолошки зависности, организиран криминал, корупција и искористување на постојните општествени поделби. Целта на споменатите малициозни активности е намалување на довербата во институциите, влијание врз јавното мислење и процесите на одлучување, предизвикување економска штета и нарушување на функционирањето на државните системи.

Проценка е дека сајбер-заканите ќе бидат меѓу најчестите и најдинамичните безбедносни ризици, заедно со онлајн-измамите, манипулативните информативни кампањи и активностите на организираните криминални групи. Ризикот од нив произлегува од широката зависност на институциите, компаниите и граѓаните од дигиталните технологии и информациските системи. Најголеми последици би можеле да предизвикаат системски сајбер-напади насочени кон критични информациски системи и инфраструктура, особено доколку доведат до прекин на основни услуги, компромитирање чувствителни државни информации или нарушување на функционирањето на институциите. Посебен ризик претставува можноста сајбер-нападите да се комбинираат со други форми на безбедносно и хибридно дејствување. Сајбер-просторот може да се користи за неовластено прибирање информации, нарушување или прекин на системи, ширење дезинформации, влијание врз јавноста и поддршка на пошироки операции насочени кон институциите и процесите на одлучување.

Странските држави, нивните разузнавачки служби, организации или поединци што дејствуваат во нивен интерес можат истовремено да користат локални посредници, медиуми и онлајн-платформи, економски инструменти и сајбер-средства за да влијаат врз јавноста, институциите или процесите на одлучување. Истовремено, организираните криминални групи можат паралелно да перат пари, да корумпираат службени лица, да користат шифрирани комуникации и да обезбедуваат финансиска, логистичка или техничка поддршка на други злонамерни актери. На тој начин, криминалните, разузнавачките, економските, информативните и сајбер-заканите можат меѓусебно да се надополнуваат и да создадат посложени безбедносни предизвици.
Поради тоа, заканите не се разгледуваат и третираат изолирано, туку преку интегриран и координиран институционален одговор заснован врз навремена размена на информации, јасна поделба на надлежностите, заедничка проценка на ризиците и усогласено преземање превентивни мерки заради рано предупредување.

Контраразузнавање

Странското разузнавачко дејствување претставува континуиран и сериозен безбедносен ризик. Разузнавачкиот интерес и странското влијание е насочено кон политичките и безбедносните стратешки определби на државата на внатрешен и надворешен план, процесот на европската интеграција, одбраната, енергетиката, критичната инфраструктура, телекомуникациите, финансискиот сектор, јавните набавки, новите технологии и сензитивни лични или класифицирани податоци.

Форми на разузнавачко дејствување:

Градење на однос со лица, развивање човечки извори и агентурна мрежа со пристап до класифицирани информации

Финансиска поддршка, посредници, прокси-компании и други форми на прикривање на вистинскиот ентитет

Сајбер-шпионажа, компромитирање уреди и комуникациски системи

Користење на територијата на државата за спроведување активности насочени кон трети земји или сојузнички интереси

Користење дипломатски, деловни, академски, медиумски или НВО статус како покритие разузнавачки активности

Прибирање информации преку внатрешни лица, искористување на незадоволство, финансиски проблеми или недоволна безбедносна култура

Прикриено влијание врз јавни политики, одлуки, медиумски наративи или општествени групи

Проценка за 2027 година

Се проценува дека разузнавачките служби и нивните прокси-актери што делуваат во интерес на други држави во 2027 година ќе покажуваат континуиран интерес за Република Северна Македонија. Нивните активности се очекува да бидат насочени кон прибирање сензитивни информации и преку хибридни начини на делување да се обидат да остварат влијание врз важни одлуки, нарушување на работата и угледот на државните институции. Посебен ризик ќе претставуваат активностите во кои разузнавачкото дејствување ќе се комбинира со сајбер-напади, економски притисоци, дезинформации, обиди за компромитирање лица и институции.

Приоритети

- Континуирано зајакнување на безбедносните проверки и проценување на ризикот
- Засилување на капацитетите за заштитата од внатрешни ризици и неовластен пристап
- Подигнување на контраразузнавачката свест во институциите и стратешките јавни приватни партнерства
- Заштита на истражувања, технологија, интелектуална сопственост и сензитивни податоци, комуникациски мрежи и критична инфраструктура
- Брза размена на информации со домашни и сојузнички партнерски служби
- Попречување хибридни активности од трети земји кои се насочени кон создавање на општествена поларизација, слабеење на капацитетите и забавување на евроинтегративните процеси на државата
- Навремено откривање координирани кампањи за влијание и сајбер-активности
- Утврдување на изворите на финансирање и откривање на прокси-актери
- Подобрување на медиумската писменост и нивото на отпорност на граѓаните и локалните заедници
- Проценка на ризици од странските инвеститори

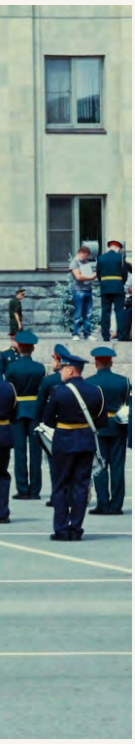
Активности на Руската Федерација

Активностите на Руската Федерација претставуваат значаен безбедносен ризик поради нивниот начин на хибридно и прикриено делување во Европа и Западен Балкан. Со ваквиот начин на нивно делување се прави обид кон создавање внатрешен раздор, одржување на „смрзнати конфликти“ и уривање на довербата во институциите, ерозија на европските вредности на РС Македонија, кои се стратешки и правно втемелени во акти на државата уште од 1991 година.

Начини на дејствување на Руската Федерација

- Пропагандно-дезиформациски кампањи преку интернет-портали, социјални мрежи, посредници и координирани профили
- Злоупотреба на историски, идентитетски, етнички, верски и политички прашања за создавање недоверба и поделби
- Сајбер-шпионажа, попречување на информациски системи и неовластено прибирање или објавување чувствителни информации
- Користење прокси-актери, односно домашни и регионални посредници, маргинални групи и влијателни поединци за остварување на нивни цели и интереси
- Употреба на економски, енергетски и финансиски инструменти за создавање зависност или притисок
- Создавање впечаток дека демократските институции се неефикасни, корумпирани или без доверба и легитимитет

Проценка за 2027 година



Се проценува дека ризикот од директно руско влијание врз официјалните политички процеси во Република Северна Македонија ќе остане низок со оглед на постоечкиот национален консензус за дефинирање на стратешките перспективи на државата. Сепак индиректно, руското малициозно влијание и прокси-делување, се очекува да продолжи со ист интензитет преку медиуми, социјални мрежи, регионални посредници и домашни поединци или групи. Особено внимание заслужуваат координираните кампањи во кои дезинформациите се комбинираат со сајбер-активности, прикриено финансирање и користење локални посредници.

Со оглед дека Руската Федерација ја прогласи Република Северна Македонија за непријателска држава по нејзиното приклучување кон меѓународните санкции поради воената агресија врз Украина, проценка е дека до целосното интегрирање на земјата во ЕУ, ќе продолжи суптилно да ги стимулира билатералните спорови заради забавување на европските перспективи. Безбедносен интерес на Агенцијата претставуваат активности што се насочувани или поддржувани од државни структури и што вклучуваат прикриено влијание, манипулација, корупција, сајбер-дејствување или други постапки со кои можат да бидат загрозени националните интереси, без да навлегува во руската културата, законската, дипломатската, трговската и друга соработка меѓу двете земји.

Активности на Народна Република Кина

Активностите на Народна Република Кина опфаќаат легитимна билатерална соработка во повеќе сфери. Присуството на кинески компании, инвестиции или институции, само по себе не претставува безбедносен ризик, освен ако одредена економска или технолошка соработка создава прекумерна зависност, овозможува пристап до сензитивни податоци и системи или може да влијае врз донесувањето важни државни одлуки.

Фокус на интерес

Употреба на телекомуникациска, дигитална и надзорна технологија преку која се обработуваат големи количини податоци

Академска и истражувачка соработка во области што можат да имаат и цивилна и безбедносна примена

Инвестиции, кредити и договори поврзани со критичната инфраструктура и стратешки сектори

Можен пристап до деловни, лични, институционални и технички информации

Јавни набавки и долгорочни договори што создаваат зависност од еден снабдувач

Влијание преку економски, дипломатски, медиумски, културни и академски канали

Проценка за 2027 година

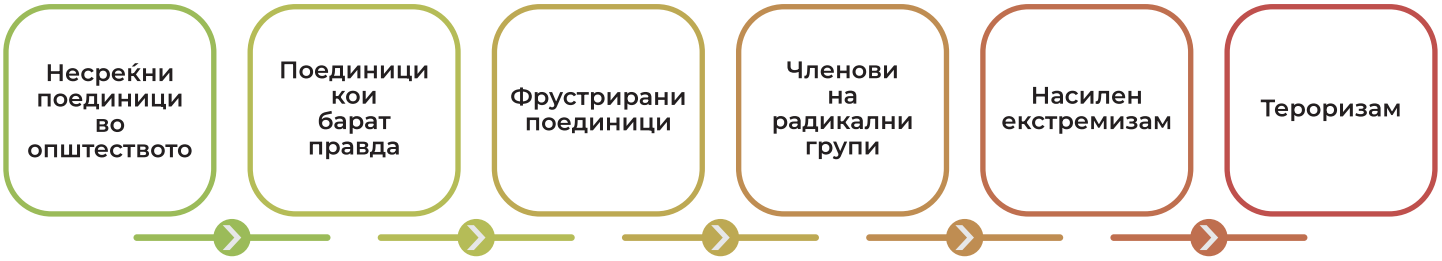
Се проценува дека Народна Република Кина суптилно навлегува во клучните сегменти на општеството преку инвестициски, технолошки и инфраструктурни проекти, како и културни, образовни, академски проекти и програми наменети за медиумите и се обидува да создаде влијателни структури на европскиот континент и меѓу членките на НАТО-алијансата.

Непосредниот безбедносен ризик поврзан со Народна Република Кина се проценува како низок со тенденција на раст во одделни стратешки сектори, особено кога постои долгорочна зависност од странска технологија, финансии или снабдувачи. Генералниот ризик произлегува од можноста за економска, технолошка или информациска зависност, со цел ограничено самостојно одлучување на државата. Овој ризик се зголемува имајќи ја предвид и кинеската регулатива која им наложува на приватните и на државните кинески компании да им овозможат на кинеските безбедносни служби пристап до податоците на корисниците ширум светот.

Насилен екстремизам

Екстремизмот претставува појава на идеологии, ставови и однесувања кои ги надминуваат општествено прифатливите норми, правила и демократски вредности, застапувајќи крајни и непропустливи позиции за постигнување политички, верски, етнички, националистички или други идеолошки цели. Фокусот на безбедносен интерес е насочен кон навремено детектирање на ваквите безбедносни појави кои би можеле од формата на демократско и легално делување и граѓански активизам да преминат во екстрем преку ширење радикални идеи, дискриминација, нетолеранција и отфрлање на другите, со оправдување и примена на насилни дејствија што водат кон радикализам и тероризам.

Скалест модел на психолошки процес што води кон тероризам (Moghaddam Fathali)



Двигатели и ранливости

- Политичка и општествена поларизација, говор на омраза и нормализирање насилна реторика;
- Чувство на неправда, исклученост, понижување или загуба на идентитет;
- Онлајн ехо-комори, алгоритамска радикализација и пропаганда приспособена кон поединецот;
- Влијание на странски конфликти и транснационални идеолошки мрежи;
- Затворска радикализација, контакт со лица со екстремни уверувања и недоволна ресоцијализација и постпенална поддршка;
- Поттикнување локални спорови, меѓуетничка и меѓуверска нетрпеливост и нејзина злоупотреба;
- Психолошки, семејни или социјални проблеми што можат да се комбинираат со насилна идеологија.

Проценка за 2027 година

Во широкиот спектар на безбедносни закани, проценка е дека екстремизмот и особено неговата насилна варијатна и натаму ќе биде еден од клучните ризици поради капацитетот да мобилизира општествени слоеви за остварување идеолошко политички цели, преку предизвикување на демократските вредности и владеењето на правото. Од аспект на екстремизмот и насилните манифестации посебен ризик за земјата претставува промовирање и преземање активности за нарушување на унитарниот карактер на државата и нејзината територијална целовитост.

Насилниот екстремизам се проценува како средно веројатен ризик со високо потенцијално влијание. Особено внимание бараат верски мотивираниот екстремизам, етнонационалистичките и политички мотивираните насилни мрежи, како и мешавината од различни идеологии кај т.н. хибридно радикализирани лица.

Превентивен пристап

Превентивното делување е насочено кон минимизирање на ризикот од насилство, а не кон припадноста на одредена заедница. Координираните активности меѓу безбедносните, образовните, здравствените, социјалните и локалните институции, семејствата, верските заедници и граѓанскиот сектор, се клучни за рано препознавање, онлајн-превенцијата, индивидуализирана проценка, деангажирање, дерадикализација, рехабилитација и реинтеграција.

Тероризам и онлајн радикализација

Ризикот од терористички акти во земјата во актуелниот момент се оценува како низок и покрај глобалните трендови кои создаваат генерални ризици што произлегуваат од идеолошки мотивирани поединци и групи. Ризиците по националната безбедност и понатаму во најголем дел зависат од транснационални терористички организации, како што се ИСИЛ и Ал-Каеда и нивни подгрупи кои делуваат регионално. Опасноста од онлајн-радикализација и влијанието на меѓународните терористички мрежи во интернет просторот останува висока и покрај моментално ниската тенденција да премине во закана за подготовка и изведување на терористички акти. Од друга страна, присуството на странските терористички борци-повратници во државата и понатаму претставува потенцијален ризик за рецидивизам и идеолошко индоктринирање на млади лица кои евентуално би можеле да извршат изолирани насилни активности со елементи на тероризам.

Приоритети

- Мониторинг и сајбер-безбедност во виртуелниот простор
- Детектирање и попречување активности на „осамени волци“
- Мониторинг над странските терористички борци - повратници
- Континуирана меѓународна соработка и размена на разузнавачки податоци
- Институционална превенција и национална координација

Клучни ризици

Онлајн-радикализација во сајбер-просторот

Достапноста на радикална содржина на интернет овозможува лесно ширење на екстремни и радикални идеологии генерирани од страна на меѓународни терористички организации наменети за ранливите категории граѓани.

Влијание од странски терористички борци - повратници

Повратниците од воените жаришта од Блискиот Исток и понатаму остануваат во фокусот заради нивниот профил и евентуални контакти со нивни истомисленици и соборци, инспирирање и регрутирање млади лица во земјата за извршување на потенцијални терористички дејствија.

Идеолошки мотивирани групи и саморадикализирани поединци (опасност од „осамени волци“)

Глобалните трендови создаваат закани од поединци и мали групи кои дејствуваат самостојно со лесно достапни средства за извршување напади.

Поврзаност со глобални терористички мрежи

Националната безбедност директно се соочува со ризиците што ги генерираат глобалните терористички организации, како што се ИСИЛ и Ал-Каеда, чиишто идеологии и пропагандни мрежи можат да најдат плодна почва за дејствување преку истомисленици/следбеници во земјата.

Проценка за 2027 година

Безбедносните аспекти поврзани со тероризамот во сите форми и димензии и натаму ќе продуцираат безбедносни ризици и закани, а според степенот на закана проценка е дека верско идеолошкиот инспириран и мотивиран тероризам и натаму ќе остане доминантен. И покрај променетите односи на меѓународната терористичка сцена поврзани со флуктуирачки капацитети на доминантните транснационални терористички организации, кои децентрализирано развиваат капацитети за надворешни терористички операции, на краток рок ќе продуцираат ризици од можност за поединечни насилни инциденти.

Организиран криминал и корупција

Организираниот криминал и корупцијата претставуваат ризици за националната безбедност заради потенцијалот преку криминалните мрежи водени од мотивот за стекнување незаконски профит и финансиска моќ, коруптивно да влијаат врз службени лица и врз институциите и медиумите, што резултира со нарушување на економската стабилност, демократските процеси, владеењето на правото и довербата во институционалниот систем во земјава. Посебен ризик претставува употребата на насилството како алатка на организираниот криминал, неговата транснационална димензија, како и можноста истиот да биде ставен во логистичка функција на насилниот екстремизам, тероризмот или разузнавањето.

Најзастапени форми

- Недозволена трговија со дрога и оружје, пропратена со различни форми на насилен криминал
- Криумчарење мигранти и трговија со луѓе
- Перење пари, даночни измами и сомнителни финансиски трансфери
- Злоупотреба на економски процеси
- Коруптивно влијание врз службени лица дел од правосудни, контролни или регулаторни органи
- Еколошки криминал и незаконска експлоатација на природни ресурси
- Криумчарење акцизни стоки
- Сајбер-криминал и измами

Проценка на ризик од организиран криминал за 2027 година

Организираните криминални групи не функционираат изолирано, туку се поврзани во криминални мрежи, кои им овозможуваат висок степен на транснационалност во функционирањето и флексибилност на релоцирање и прикривање на нивните припадници, криминални активности и нелегален профит.

Проценка е дека криминалните мрежи во своите конвенционални криминални активности ќе продолжат да користат физичко и психолошко насилство, коруптивно влијание, но и шифрирани интернет комуникациски алатки за прекугранична координација и регрутација на нови припадници. Онлајн-пазарите и крипто-берзите како нерегулирана зона на финансиска активност ќе ги користат како алатка за прикривање и заштита на своите нелегални профити. Криминалните мрежи ќе продолжат со регрутација на млади лица, како тактика за заштита од идентификување и казнено процесуирање на криминалната мрежа и нејзините високопозиционирани членови.

Веројатноста за појава на овој ризик се проценува како висока, а степенот на влијание на организираниот криминал врз општествените процеси и финансиската стабилност се проценува со средно ниво.

Миграциски и прекугранични ризици

Географската положба ја прави државата транзитен дел од т.н. Балканска миграциска рута. Политичката и безбедносната нестабилност на Блискиот Исток и Северна Африка може да предизвикаат зголемени бранови на мигранти.

Криминалните мрежи, со цел зголемување на својот профит имаат тенденција да ги злоупотребат мигрантските движења да создадат илегални канали за криумчарење мигранти, кои истовремено можат да бидат користени за транфер на високоризични лица – терористи, како и нелегална трговија со оружје и дрога. Истите имаат зголемен тренд на користење на интернет платформи за регрутирање, огласување и трансфер на пари.

Приоритети

- Следење на сомнителни финансиски текови и активности поврзани со перење пари
- Идентификување на прикриен финансиски потенцијал на организираните криминалните групи заради намалување на нивната економска моќ
- Континуирани безбедносни проверки и проценки на ризик
- Превентивна заштита на институциите од коруптивно влијание
- Заеднички операции и навремена размена на информации со националните, регионалните и европските партнери
- Идентификација на нови високоризични организирани криминални групи, нивни припадници и криминални активности

Сајбер-безбедност

Сајбер-просторот претставува едно од клучните подрачја во кое граѓаните, институциите и компаниите се соочуваат со современите безбедносни закани. Сè поголемата дигитализација на услугите, деловните процеси и комуникацијата носи значителни придобивки, но истовремено го зголемува и ризикот од злоупотреба, со што се налага потребата од системски пристап кон сајбер-безбедноста.
Последиците од сајбер-инцидентите можат да бидат различни, во зависност од природата и целта на нападот. Можат да опфатат финансиски загуби, кражба, уништување податоци, прекин на електронски услуги и нарушување на довербата на граѓаните и корисниците. Особено сериозни се нападите врз критичната инфраструктура бидејќи нивните последици можат да ги надминат границите на дигиталниот простор и да предизвикаат нарушувања во функционирањето на основните услуги и процеси во физичкиот свет.

Проценка за 2027 година

Веројатноста за сајбер-напади останува висока, а влијанието односно штетата која би ја предизвикале се проценува како висока. Проценка е дека сајбер-криминалните групи заради финансиски мотиви ќе бидат најчести извршители на напади, додека недржавните прокси-актери, во функција на државите ќе продолжат да прибираат информации и да развиваат пристап што може да се активира во услови на криза. Дополнителен ризик претставуваат комбинираните операции, во кои сајбер-нападот се поврзува со ширење дезинформации и манипулативни содржини. Целта на ваквите активности не е само нарушување на информациските системи, туку и создавање страв, паника, недоверба и политички или општествен притисок.

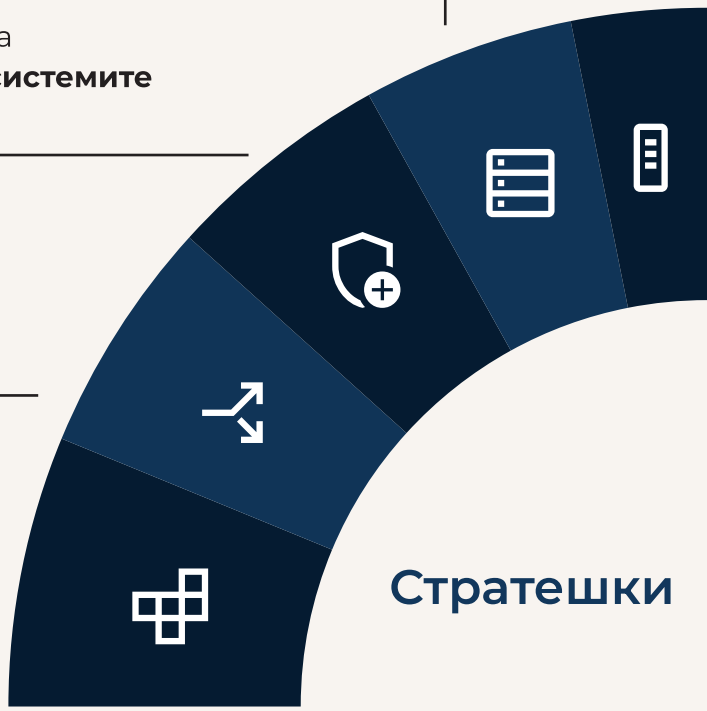
Редовно креирање и тестирање на резервни копии, како и воспоставување планови за континуитет на работењето и опоравување од инциденти

Мрежна сегментација и заштита на критичните системи, со цел ограничување на ширењето на нападите

Примена на сајбер-безбедност, со вградување на **безбедносни механизми во фаза на развој на системите**

Мрежа на тимови за одговор на сајбер-инциденти, со капацитет за навремено откривање, анализа и справување со инцидентите

Национална стратегија за сајбер-безбедност и **ефикасна координација меѓу надлежните институции**



Стратешки

Облици на сајбер-ризици и сајбер-закани

- Фишинг, кражба на лозинки и онлајн-измами – напади кои најчесто се базираат на измама на корисниците со цел откривање сензитивни податоци, како лозинки или банкарски информации, преку лажни пораки, веб-страници или е-пошта;
- Рансомвер и изнуда на податоци – злонамерен софтвер кој ги заклучува или шифрира податоците и бара откуп за нивно враќање, често придружен со закана дека украдените информации ќе бидат јавно објавени;
- Дистрибуирани напади за преоптоварување (DDoS) – напади со кои се оптоваруваат сервери или мрежи со голем број барања, со цел да се онеспособат или да станат недостапни за корисниците;
- Сајбер-шпионажа и тивко долгорочно присуство во мрежи;
- Напади преку синџирот на снабдување – компромитирање на системи преку доверливи трети страни, како добавувачи на софтвер или услуги, со цел индиректен пристап до целната организација;
- Компромитирање на облак услуги и уреди – злоупотреба на слабо заштитени облак (cloud) платформи, мобилни уреди или далечински пристап, особено кога недостасуваат соодветни безбедносни контроли;
- Напади врз индустриски и критични системи – таргетирање на енергетика, водоснабдување, транспорт и производство, каде што нарушувањето може да има реални последици во физичкиот свет;
- Злоупотреба на вештачка интелигенција – користење вештачка интелигенција (AI) за создавање поубедливи измами, автоматско откривање ранливости и генерирање лажни содржини (deepfakes) кои тешко се препознаваат.

правци

Развој и задржување на **квалификуван сајбер-безбедносен кадар** преку образование, обуки и континуирано професионално усовршување

Подигнување на нивото на сајбер-хигиена **кај граѓаните преку системско образование и јавни кампањи**

Зајакнување на безбедноста на синџирот на снабдување преку проценка и контрола на ризиците поврзани со надворешни добавувачи и трети страни

Посебна заштита на децата и младите на интернет преку развивање на дигиталната и сајбер-безбедносната писменост

Критична инфраструктура, економска, енергетска и истражувачка безбедност

Критична инфраструктура и основни услуги

Критичната инфраструктура ги опфаќа системите и услугите без кои не може нормално да функционираат населението, економијата и државата. Тука спаѓаат енергетиката, електронските комуникации, дигиталните и финансиските услуги, водоснабдувањето, здравството, транспортот, снабдувањето со храна, државната управа и итните служби. Прекините можат да бидат предизвикани од сајбер-напади, саботажа, терористички активности, организиран криминал, странско влијание, технички дефекти, човечки грешки, недостиг на ресурси, нарушување на ланците на снабдување, природни непогоди или комбинација од повеќе фактори. Посебен ризик претставуваат поврзаните, односно каскадните последици. На пример, прекин во снабдувањето со електрична енергија може истовремено да влијае врз комуникациите, водоснабдувањето, банкарските услуги, здравството, транспортот и работата на државните институции.

Економска и енергетска безбедност

Економската безбедност може да биде загрозена од корупција, перење пари, незаконски финансиски текови, злоупотреба на јавните набавки и прекумерна зависност од ограничен број странски партнери, снабдувачи или технологии. Дополнителен ризик претставува можноста преку финансиски или деловни односи да се врши влијание врз стратешки компании и важни државни одлуки. Енергетската зависност, нестабилните цени и можните прекини во снабдувањето можат да предизвикаат економски загуби, раст на трошоците за граѓаните и стопанството, социјално незадоволство и политички притисоци. Овие последици можат да бидат особено изразени во услови на поголема регионална или глобална криза.

Истражувачка и технолошка безбедност

Универзитетите, истражувачките центри и иновативните компании располагаат со знаење, податоци и технологии што можат да имаат комерцијална, безбедносна или двојна примена, односно да се користат и за цивилни и воени цели. Главните ризици се поврзани со неовластен пренос на технологии, прикриено финансирање, кражба на интелектуална сопственост, сајбер-шпионажа и несоодветна заштита на чувствителните истражувачки податоци. Поради тоа, меѓународната научна и технолошка соработка треба да се развива отворено, но со соодветна проценка на можните безбедносни ризици.

Природни и климатски ризици како безбедносни катализатори

Пожарите, поплавите, сушите, екстремните температури, земјотресите и загадувањето можат значително да ја зголемат ранливоста на критичната инфраструктура, да предизвикаат прекин на основните услуги, економски загуби, раселување на населението и дополнителен притисок врз институциите. Кризите предизвикани од природни непогоди можат да создадат и простор за ширење дезинформации, финансиски измами, злоупотреба на помошта и други криминални активности. Поради тоа, природните и климатските појави се разгледуваат како фактори што можат да ги влошат постојните безбедносни ризици.

Проценка за 2027 година

Во 2027 година веројатноста за краткотраен или ограничен прекин на некоја критична услуга се проценува како средна и можните последици се оценуваат како средни. Помалку е веројатен долготраен и истовремен прекин на повеќе системи, но доколку се случи, последиците би можеле сериозно да го нарушат секојдневниот живот, економијата и работата на институциите. Веројатни причини за подолготрајни прекини во критичните услуги би можеле да бидат сајбер-инциденти и саботажа, додека краткотрајните нарушувања во снабдувањето веројатно би биле предизвикани од технички дефекти, човечки грешки и природни непогоди.

Посебно внимание бараат меѓусебната зависност на енергетските, комуникациските, финансиските, здравствените и транспортните системи, како и зависноста од странски технологии, опрема и снабдувачи.

Приоритети

Приоритет во 2027 година ќе биде континуираното превентивно делување и навремено обезбедување информации со цел непречено функционирање на основните услуги вклучително и во услови на криза, преку:

- Идентификување безбедносни ризици и закани.
- Следење појави и активности кои можат да доведат до нарушување на функционирањето на критични системи;
- Проценка на можните последици од безбедносни закани;
- Навремено информирање на надлежните институции за релевантни сознанија;
- Размена и споделување безбедносно значајни информации со надлежни институции согласно закон;
- Следење ризици поврзани со тероризам, шпионажа, организиран криминал, хибридни закани и други активности што можат да имаат импликации врз националната безбедност и критичната инфраструктура;
- Придонес кон превентивното делување и јакнењето на отпорноста на државата

Агенцијата не ја заменува улогата на институциите и операторите кои се непосредно надлежни за функционирањето, одржувањето и физичката или техничката заштита на критичната инфраструктура. Нејзината улога е првенствено превентивна во безбедносно-контраразузнавачкиот домен.

Јавната информираност - придонес кон безбедноста

Националната безбедност е заедничка одговорност. Институциите мора да бидат подготвени и отчетни, компаниите да ги штитат своите системи и податоци, медиумите да ги проверуваат информациите, а граѓаните одговорно и безбедно да ги користат дигиталните технологии, како и да препознаваат и алармираат за сомнителни појави.
Информирано, поврзано и отпорно општество е најсилната одбрана од современите безбедносни закани.

Најдобрата заштита не е реакцијата откако кризата ќе започне, туку навременото проценување на ризикот, намалување на ранливоста, минимизирање на заканите, зајакнување на довербата меѓу институциите и зголемување на подготвеноста за одговор на целото општество.

Агенцијата за национална безбедност во рамките на својата законска надлежност ќе продолжи да ги идентификува и проценува заканите, да обезбедува рано предупредување и да ги информира законски определените корисници. Професионализмот, законитоста, политичката неутралност, заштитата на човековите права и соработката со домашните и меѓународните партнери остануваат основа на нејзината работа.

CIP - Каталогизација во публикација
Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

355.40(497.7)"2027"(047.31)

БЕЗБЕДНОСНА проценка за 2027 година /
[уредник Бојан Христовски]. -
Скопје : Агенција за национална безбедност на Република Северна Македонија, 2026. - 32 стр. : илустр. ; 25 см

ISBN 978-608-67632-0-6

а) Безбедност -- Македонија -- 2027 -- Истражувања

COBISS.MK-ID 69502469

ПОСВЕТЕНИ НА БЕЗБЕДНОСТА
ВЕРНИ НА ДРЖАВАТА

АГЕНЦИЈА ЗА НАЦИОНАЛНА БЕЗБЕДНОСТ