https://doi.org/10.70265/TIDX2073

КОНЦЕПЦИЯ „НУЛЕВО ДОВЕРИЕ“ В СИГУРНОСТТА

Теодора Личева

THE ZERO-TRUST CONCEPT IN SECURITY

Teodora Licheva

Резюме: *В настоящия доклад анализирам възможностите, предизвикателствата и стратегическите рамки за внедряване на модела с нулево доверие в службите за сигурност в глобален аспект, с фокус върху водещи практики от САЩ, Великобритания и Австралия, за прогнозиране и внедряване на тези модели към специфичния контекст на България. Особен акцент поставям на управленските процеси, организационната култура и технологичните предпоставки, които съпътстват тази фундаментална промяна в киберотбраната.*

Ключови думи: *нови технологии, национална сигурност, киберсигурност*

Summary: *In this report, I analyze the opportunities, challenges, and strategic frameworks for implementing the zero-trust model in security services globally, focusing on leading practices from the US, UK, and Australia, to predict and implement these models in the specific context of Bulgaria. I place particular emphasis on the management processes, organizational culture, and technological prerequisites that accompany this fundamental change in cyber defense.*

Keywords: *new technologies, national security, cybersecurity*

УВОД

В съвременната динамична среда, характеризираща се с размити периметри, хибридни работни модели и все по-усъвършенствани заплахи, традиционните подходи за отбрана, базирани на доверие в рамките на мрежата, се оказват неадекватни и недостатъчни за гарантиране на националната сигурност и отбрана. Разузнавателните служби в световен мащаб, които работят с най-чувствителната информация и са обект на постоянни атаки от държавния и частния сектор, са изправени пред неотложната необходимост от трансформация на своите защитни процеси и схеми. В този контекст, моделът за сигурност с нулево доверие (Zero Trust Architecture – ZTA) се налага като водеща стратегическа философия. Той елиминира

имплицитното доверие и налага стриктна проверка на идентичността и контекста при всяка заявка за достъп, независимо от местоположението на потребителя или устройството (Rose et al., 2020).

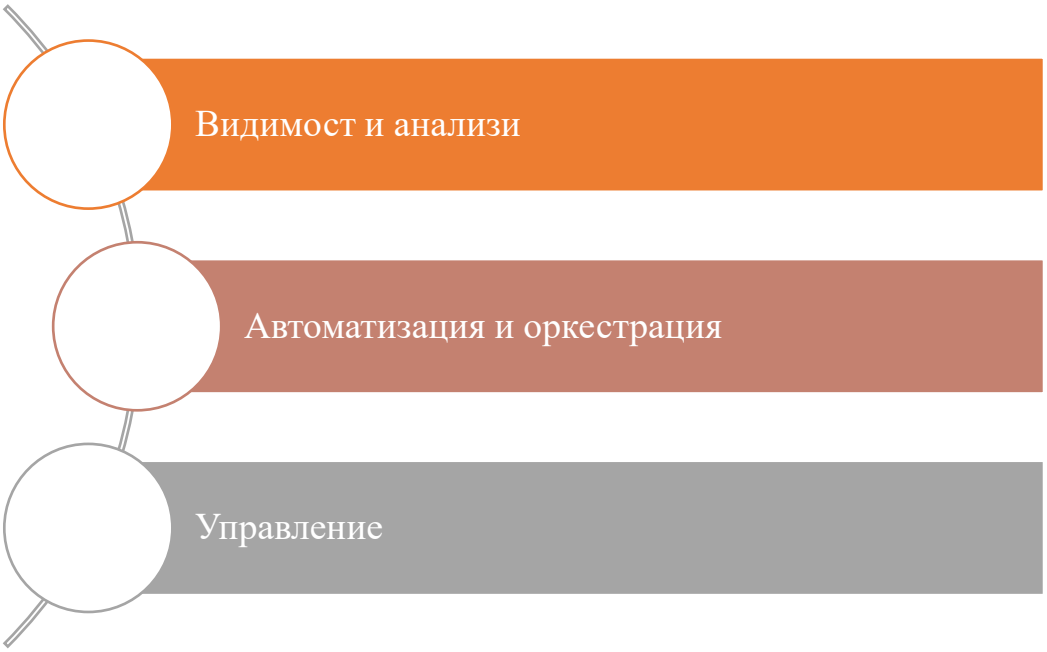
Основният принцип на архитектурата с нулево доверие е „никога не се доверявай, винаги проверявай“. С него се предоставят минимални привилегии и приемане на пробив по подразбиране (Balarabe, 2024).

В основата на доклада са заложени следните основополагащи стандарти и рамки:

- **NIST Special Publication 800-207 „Zero Trust Architecture“:** Служи като фундаментална теоретична основа, дефинираща седемте основни принципа, логическите компоненти (Policy Engine, Policy Administrator, Policy Enforcement Point) и абстрактните модели за внедряване на ZTA.
- **CISA Zero Trust Maturity Model (ZTMM):** Използва се като практически пътеводител за оценка на текущото състояние и планиране на поетапното внедряване. Моделът структурира процеса около пет основни стълба, именно:

Фигура 1. Пет основни стълба на концепцията за нулево доверие

Както и три всеобхватни способности (Rose et al., 2020).



Фигура 2. Трите ключови възможности на концепцията

- **Ръководства на NSA за зрялост на нулевото доверие:** Серията от документи на Агенцията за национална сигурност на САЩ. Агенцията предоставя детайлни препоръки за постигане на напреднала зрялост във всеки от седемте стълба на модела на ZTA на DoD, специално адаптирани за нуждите на системите за национална сигурност (National Security Agency, 2024).
- **Рамки на NCSC (UK) и ACSC (Australia):** Анализират се принципите за дизайн на ZTA на NCSC и концепцията за „модерна защитима архитектура“ (Modern Defensible Architecture) на ACSC, която интегрира принципите на нулево доверие (National Cyber Security Centre [NCSC], 2021).

Синтезираната информацията от тези източници има за цел да предостави структуриран, всеобхватен и практически ориентиран поглед върху трансформиращия потенциал на нулевото доверие за повишаване на киберустойчивостта на службите за сигурност.

2. МОДЕЛ ЗА СИГУРНОСТ С НУЛЕВО ДОВЕРИЕ: ДЕФИНИЦИЯ И ПРИНЦИПИ

Архитектурата с нулево доверие представлява коренна промяна в разбирането на киберсигурността. Тя се отдалечава от остарелия модел на т.нар. „замък и ров“, при който всичко, което се намира в мрежовия периметър, се счита за надеждно и възприема философията „никога не се доверявай, винаги проверявай“ (Zscaler, n.d.). В основата си ZTA

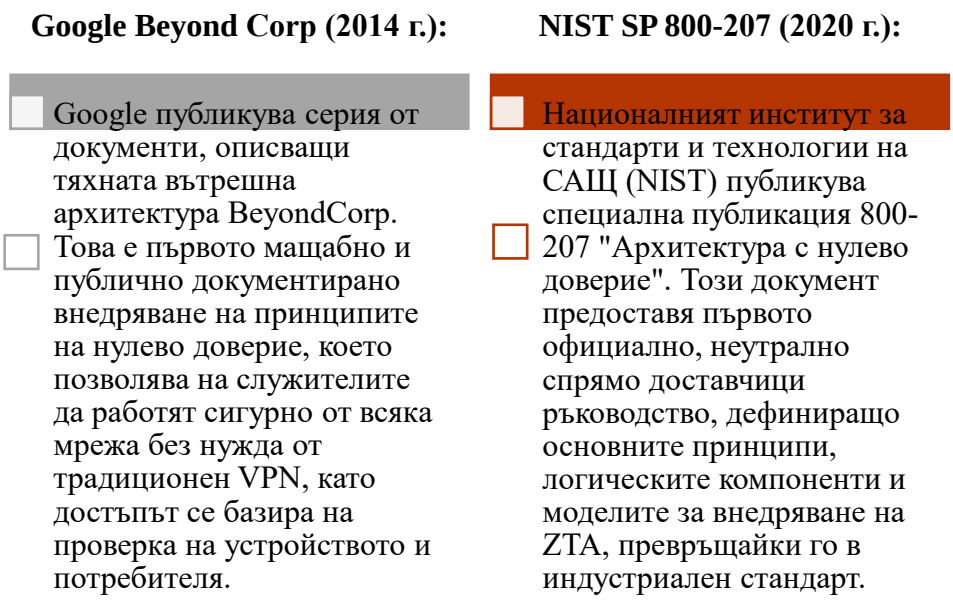
елиминира подразбиращото се доверие и третира всяка заявка за достъп до ресурси като потенциално враждебна, независимо дали произхожда от вътрешна или външна мрежа (Rose et al., 2020). Вместо да се разчита на местоположението, моделът налага динамична и стриктна проверка на идентичността, контекста и оценката на риска при всяка една отделна сесия (CyberArk, n.d.).

Трябва да се има предвид, че това не е конкретен продукт или технология, а стратегически подход към проектирането и внедряването на сигурността, който се фокусира върху защитата на самите ресурси (данни, приложения, услуги), а не върху мрежовите сегменти (Gartner, n.d.).

Еволюция на концепцията

Въпреки че терминът започва да придобива популярност през последното десетилетие, корените на нулевото доверие могат да бъдат проследени до по-ранни концепции, които оспорват адекватността на периметърната сигурност.

- **Де-периметризация (2004-2005 г.):** Международният консорциум Jericho Forum въвежда идеята за „де-периметризация“. Той признава, че нарастващата мобилност, облачните услуги и взаимосвързаността правят традиционния мрежов периметър все по-ненадежден и призовава за преместване на фокуса на защитата към самите данни чрез криптиране и многослойна защита (Sholtz, 2023).
- **Формализиране на „Нулево доверие“ (2010 г.) :**През 2010 г. анализаторът Джон Киндерваг от Forrester Research официално въвежда термина „Нулево доверие“ (Zero Trust) (Illumio, 2021). Основният му аргумент е, че най-голямата уязвимост в сигурността е доверие по подразбиране, което позволява на атакуващите, веднъж проникнали в мрежата, да се оперират в системата безпрепятствено. Именно това свободно боравене с информацията принуждава Киндерваг да предложи модел, базиран на микросегментация и непрекъсната проверка (Illumio, 2021).



Фигура 3. Стандартизиране и приложение на концепцията „Нулево доверие“ (2014-2020 г.) (Sholtz, 2023)

Основни принципи на нулевото доверие

За успешното внедряване на ZTA е необходимо взаимодействие на основополагащите принципи. Те ръководят архитектурните решения и оперативните процеси.

1. Изрична проверка

„Никога не се доверявай, винаги проверявай“ – това е основният принцип в идеята за нулево доверие. Всяка заявка за достъп трябва да бъде автентифицирана и оторизирана динамично, като се използват всички налични информационни точки, включително:

- **Идентичност на потребителя:** Кой е потребителят и какъв е неговият достъп;
- **Състояние на устройството:** Ниво на сигурност, наличие на пачове, конфигурация и цялост на устройството;
- **Местоположение:** Географско положение и мрежови произход на заявката;
- **Поведение и контекст:** Анализ на типичното поведение и откриване на аномалии;
- **Класификация на данните:** Чувствителност на ресурса, до който се осъществява достъп (Balarabe, 2024).

2. Прилагане на минимални привилегии

Този принцип цели да ограничи потенциалните щети при компрометиране на акаунт или устройство. Потребителите и системите получават достъп само до ресурсите, които са абсолютно необходими за изпълнение на техните функции, и то само за определено време (Rose et al., 2020). Микросегментацията е ключова технология за прилагането на този принцип, защото тя създава гранулирани периметри около отделни или малки групи ресурси, предотвратявайки страничното движение в мрежата (Cloudflare, n.d.).

3. Приемане на пробив по подразбиране

Архитектурата за нулево доверие се проектира с презумпцията, че пробив в сигурността е не просто възможен, а неизбежен. По този начин мисловният модел измества фокуса от превенция към бързо откриване, изолиране и реакция (Balarabe, 2024). Това означава, че всички мрежови потоци трябва да бъдат криптирани, а сигурността не трябва да разчита на предполагаемата „безопасност“ на вътрешната мрежа.

4. Непрекъснат мониторинг и анализ

ZTA изисква непрекъснато събиране и анализ на данни и телеметрия от възможно най-много източници – логове, мрежов трафик, информация за заплахи, състояние на крайните точки и др. (CyberArk, n.d.). Тези данни се използват за непрекъсната оценка на риска, откриване на аномалии в реално време и автоматизиране на ответни действия, като например прекратяване на сесия или повторна автентификация при необходимост (CrowdStrike, n.d.).

2. ИЗПОЛЗВАНЕ НА МОДЕЛА ZERO TRUST В СИГУРНОСТТА

Внедряването на архитектура с нулево доверие в държавните агенции и службите за сигурност по света се ръководи от осъзнаването, че традиционните мрежови защити са неспособни да се справят със съвременните киберзаплахи, особено тези в държавния сектор. Водещи държави са възприели ZTA не просто като техническо решение, а като стратегическо предписание за защита на националната сигурност и критичната инфраструктура.

Примерът от САЩ: Федерален двигател на трансформацията

Правителството на САЩ е най-активният двигател за приемането на ZTA, като процесът е ускорен от президентски указ № 14028 от 2021 г. (Loshin, 2024). Две са ключовите агенции, които ръководят тази трансформация, всяка със специфичен фокус и насоченост.

Агенция за киберсигурност и инфраструктурна сигурност (CISA)

CISA действа като основен координатор и методолог за федералните държавни агенции. Нейният ключов инструмент е Моделът за зрялост на нулевото доверие (Zero Trust Maturity Model - ZTMM), който служи като пътна карта за поетапно внедряване (Cybersecurity and Infrastructure Security Agency [CISA], 2023).

Структура на модела: ZTMM е организиран около пет основни стълба, които представляват ключови области за защита:

1. **Идентичност:** Проверка на потребители и системи.
2. **Устройства:** Оценка на състоянието и сигурността на всяко устройство, което има достъп до ресурси и данните в системата.
3. **Мрежи:** Сегментиране на мрежата и защита на трафика.
4. **Приложения и работни натоварвания:** Защита на приложенията и техните комуникации.
5. **Данни:** Класификация, криптиране и контрол на достъпа до данните (Zero Networks, 2024).

Всеобхватни способности: Моделът включва и три хоризонтални способности, които подпомагат всички стълбове: Видимост и анализи, автоматизация и управление.

Еволюционен подход: CISA насърчава агенциите да не се опитват да внедрят всичко наведнъж, а да следват еволюционен път през нивата на зрялост – от „Традиционно“ към „Първоначално“, „Напреднало“ и „Оптимално“ (Khera, 2023).

Агенция за национална сигурност (NSA)

Докато CISA се фокусира върху цивилните агенции, NSA предоставя по-специализирани и технически задълбочени ръководства, насочени към Министерството на отбраната (DoD), разузнавателната общност и отбранителната индустриална база (National Security Agency [NSA], 2023).

Агенцията публикува серия от Информационни бюлетини за киберсигурност (CSIs), които детайлно описват как да се постигне зрялост във всеки от седемте стълба на ZTA модела на DoD. Тези документи предоставят конкретни препоръки за:

- Укрепване на управлението на идентичността, идентификационните данни и достъпа (NSA, 2023);
- Гарантиране сигурност на устройствата чрез инвентаризация, автентикация и непрекъсната инспекция и мониторинг (NSA, 2023);
- Изолиране на критични ресурси чрез макро- и микросегментация на мрежата (NSA, 2023);

- Защита на данните в покой и в движение чрез криптиране, етикетиране и управление (NSA, 2024);
- Използване на автоматизация и координация за по-бърза реакция при инциденти (NSA, 2024b).

Великобритания: Принципен подход към дизайна (NCSC)

Националният център за киберсигурност на Великобритания (NCSC) възприема по-абстрактен и базиран на принципи подход. Вместо да предписва конкретен модел на зрялост, той публикува осем принципа за дизайн на архитектура с нулево доверие, които да ръководят организациите при създаването на собствени решения (NCSC, 2021).

Принципите са:

1. **Познаване на архитектурата**, включително потребители, устройства, услуги и данни.
2. **Познаване на потребителските и системните идентичности** и тяхната мощност.
3. **Непрекъснат мониторинг и одит** на сигурността на потребителите и устройствата.
4. **Автентикация и оторизация** при всяка заявка за достъп, независимо от предоставения по длъжност такъв.
5. **Политики за достъп, базирани на риска**, които са динамични, адаптивни и отговарящи на съвременните за киберзаплахи.
6. **Защита на данните** – както в покой, така и в движение.
7. **Подобряване на видимостта** и аналитичните способности.
8. **Проектиране на мрежата** с предварителна нагласа, че е враждебна (Canadian Centre for Cyber Security [CCCS], 2022).

Националният център по киберсигурност активно насърчава пилотни програми в държавния сектор за тестване на тези принципи в реална среда, като целта е да се натрупа практически опит, който да информира по-широкото внедряване и приложение (NCSC, 2025).

Австралия: Интеграция в „Модерна защитима архитектура”

Австралийският център за киберсигурност интегрира нулевото доверие в по-широка концепция, която се нарича „Модерна защитима архитектура” (Modern Defensible Architecture – MDA) (Australian Cyber Security Centre [ACSC], n.d.). Тази архитектура е стратегическа рамка, която използва принципите на ZTA – „никога не се доверявай, винаги проверявай” и „приемане на пробив” – като основа за изграждане на устойчиви на кибератаки системи (ACSC, n.d.).

Основополагащите принципи, които са в основата на защитимата архитектура, са:

1. централизирано управление на идентичностите;
2. автентификация с висока степен на сигурност;
3. контекстуална оторизация;
4. надеждна проверка на активите;
5. сигурни крайни точки и намаляване на повърхността за атака.

С този подход се доказва как нулевото доверие може да бъде не само самостоятелна стратегия, а и вграден компонент в холистичен модел за киберустойчивост, който се насърчава на национално ниво (ACSC, 2024).

Архитектурата с нулево доверие в българското разузнаване

Към настоящия момент липсва публично известна информация за конкретни национални стратегии, практики, приети рамки или дори пилотни проекти за внедряване на архитектура с нулево доверие в българските служби за сигурност. Анализът в този раздел е перспективен и има за цел да очертае потенциалните ползи, специфичните предизвикателства и вероятен модел за прилагане, като изведе най-добрите световни практики към българския контекст.

Потенциални ползи и стратегическа необходимост

Приемането на архитектурата за нулево доверие от българските специални служби ще донесе значителни предимства, които надхвърлят чисто технологичните аспекти и засягат националната сигурност и отбрана, както и международните партньорства.

- **Повишена устойчивост срещу заплахи:** Чрез прилагане на принципа на минималните привилегии и микросегментация, тази архитектура значително ограничава възможностите за странично движение на атакуващи, които са успели да преодолеят първоначалната защита (Red River, 2022). Това е критичен процес за противодействие на усъвършенствани постоянни заплахи.
- **Защита на класифицирана информация и чувствителни активи:** Моделът измества фокуса от защитата на периметъра към защитата на самите данни (Rose et al., 2020). Чрез класификация, криптиране и динамичен контрол на достъпа, базиран на принципа за нулево доверие, се осигурява и защита на най-чувствителната информация.
- **Сигурна междуведомствена и партньорска комуникация:** Архитектурата за нулево доверие позволява създаването на сигурни канали за обмен на информация с други национални институции и партньорски служби от НАТО и ЕС. Достъпът се предоставя на база

„необходимост да се знае” след стриктна проверка на идентичността и ролевия достъп, а не на база доверие в мрежата на партньора.

- **Съответствие с бъдещи стандарти на НАТО и ЕС:** С оглед на федералните мандати в САЩ и инициативите във Великобритания и Австралия, нулевото доверие се очертава като стандарт за сигурност в западните демокрации (ACSC, 2024). Приемането му ще улесни оперативната съвместимост и ще демонстрира ангажираност към най-високите стандарти за киберотбрана.

Специфични предизвикателства пред България

Внедряването на архитектурата за нулево доверие в службите за сигурност на България би се сблъскало с редица предизвикателства, които изискват стратегическо планиране и политическа воля.

Таблица 1. Предизвикателства пред България при внедряване на архитектурата за нулево доверие

Категория	Специфични предизвикателства
Нормативни и управленски	Липса на единна национална стратегия за архитектура за нулево доверие; необходимост от актуализация на подзаконовата уредба за защита на класифицираната информация; потенциални трудности в междуведомствената координация
Технологични	Значителен дял на наследени системи, които не са проектирани за нововъведения; бюджетни ограничения за мащабни инвестиции в нови технологии; недостиг на висококвалифицирани експерти по киберсигурност с опит в тази архитектура.
Организационни и културни	Съпротива срещу промяната от утвърдения досега използван базов модел; необходимост от фундаментална промяна в мисленето към „приемане на пробив”; нужда от мащабни програми за обучение и повишаване на осведомеността.

Хипотетична карта за внедряване на архитектурата за нулево доверие

Налагането трябва да бъде поетапен, итеративен процес, а не еднократен проект. Като отправна точка може да се използва Моделът

за зрялост на CISA (ZTMM), който да се приспособи към българската действителност (CISA, 2023).

Етап 1. Стратегическа подготовка и оценка – около една година

1. **Дефиниране на „повърхността за защита”:** Определяне на най-критичните данни, активи, приложения и услуги, които трябва да бъдат защитени.

2. **Изработване и приемане на рамка:** Официално възприемане на адаптирана версия на ZTMM като национален стандарт за специалните служби за сигурност на страната.

3. **Оценка на зрелостта:** Извършване на първоначална оценка на текущото състояние спрямо петте стълба на модела - идентичност, устройства, мрежи, приложения и данни), за да се идентифицират най-големите пропуски и аномалии (Zero Networks, 2024).

Етап 2. Стартиране на пилотни проекти – между 2-3 години

Вместо да се извърши мащабно внедряване, трябва да се стартират пилотни проекти в ограничени, но в същото време критични области.

- **Приоритет на стълб „Идентичност”:** Основната и първа стъпка, за да има успех внедряването на архитектура за нулево доверие, е изграждането на централизирана и надеждна система за управление на идентичността (NSA, 2023). Необходимо е да се внедри и устойчива на фишинг многофакторна автентикация за достъп до всички системи.
- **Пилотен проект за сигурен отдалечен достъп:** Замяна на традиционния VPN за избрана група потребители с решение за мрежов достъп с архитектура за нулево доверие, което прилага динамичен контрол на база идентичност и състояние на устройството (Microsoft, n.d.).

Етап 3. Поетапно разширяване – зависи от скоростта и приемането на предните етапи, но вероятно след 3-5+ години.

В основа на натрупаната практика от пилотните проекти, внедряването се разширява към другите стълбове.

- **Микросегментация (Стълб „Мрежи”):** Стартира с определяне на най-критичните активи в собствени микроперимetри.
- **Управление на устройствата (Стълб „Устройства”):** Въвеждане на системи за непрекъснат мониторинг и оценка на състоянието на крайните точки, като достъпът се разрешава само от съвместими и сигурни устройства (NSA, 2023).

Успехът на подобна трансформация зависи не само от технологичния напредък на службите за сигурност, а също и от от ясната визия, политическата подкрепа на най-високо ниво и

готовността за дългосрочна промяна в организационната култура и управленските процеси.

3. УПРАВЛЕНСКИ ПРОЦЕС И СТРУКТУРА НА СИГУРНОСТТА

Внедряването на архитектура с нулево доверие е най-вече управленско предизвикателство, което изисква фундаментална трансформация на организационната структура, процесите за взимане на решения и механизмите за контрол. Успехът не зависи само от технологичните решения, а от способността на ръководството да наложи и управлява дългосрочна промяна, да осигури ресурси и да изгради нова култура на сигурност, базирана на принципа „никога не се доверявай, винаги проверявай" (Balarabe, 2024).

Управленски модели на архитектура за нулево доверие

От анализа на водещите държави се открояват два основни управленски модела за внедряване на архитектурата в сектор за сигурност.

1. Централизиран модел, по примера на САЩ

Процес на взимане на решения: Решението за преминаване към този протокол в САЩ е взето на най-високо политическо ниво чрез Президентски указ 14028 (IBM, n.d.). По този начин се дава задължителен характер на всички федерални агенции да разработят и изпълнят планове за внедряване.

Контрол и отчетност: Службата за управление и бюджет упражнява строг контрол чрез меморандум М-22-09, който определя конкретни срокове и цели до края на фискалната 2024 година (CISA, 2023). Агенциите са задължени да се отчитат редовно, което създава силен механизъм за отчетност.

Структура: Агенциите действат като централни методологични и координиращи звена. Агенцията по киберсигурност и инфраструктурна сигурност предоставя общата рамка за цивилните агенции, докато Националната агенция по сигурност предлага специализирани насоки за разузнавателната общност и отбраната, осигурявайки единство на подхода, но и гъвкавост според спецификата на сектора (National Security Agency, 2024).

2. Децентрализиран модел, воден от насоки (Великобритания и Австралия)

Процес на взимане на решения: Във Великобритания и Австралия подходът е по-скоро консултативен. Не се налагат строги мандати, а се публикуват принципи за дизайн и архитектурни рамки

(NCSC, 2021). Решението за внедряване е от компетенцията на самите ведомства, които са насърчавани да приемат принципите.

Контрол и отчетност: Контролът е по-слабо формализиран. Той се осъществява чрез насърчаване на добри практики, провеждане на пилотни проекти и споделяне на опит (NCSC, 2025). Отчетността е по-скоро вътрешна отговорност за всяка организация и се базира на оценка на риска, а не на изпълнение на централно зададени срокове.

Таблица 2. Сравнителна таблица за петте стълба със съответните технологии, критични контроли и принципи на архитектурата за нулево доверие

Стълб	Примерни практики/ технологии	Критични контроли	Връзка с принципите на Zero Trust
Идентичност	Identity&Access Management (IAM), Многофакторна автентикация (MFA), SSO	Управление на достъпа, строго RBAC, управление на идентичности, MFA enforcement	Verify Explicitly, Least Privilege Access, Continuous Monitoring
Устройства	Endpoint Detection&Response (EDR), Device Inventory, Постоянна оценка на устройството	Контрол на състоянието, инвентаризация, AV/EDR, управление на политики	Verify Explicitly, Assume Breach, Continuous Monitoring
Мрежи	Микросегментация, SDN, криптирана комуникация, Zero Trust Network Access (ZTNA)	Сегментиране на трафика, Network PolicyEnforcement, IDS/IPS, мониторинг на връзки	Least Privilege, Assume Breach, Monitor All Traffic
Приложения и работни натоварвания	API Gateways, Контрол на достъпа до приложения, container security, application whitelisting	Сигурна разработка на софтуер, стенни полици (firewall policies), runtime защита	Verify Explicitly, Least Privilege, Continuous Authorization
Данни	Data Loss Prevention (DLP), шифроване, класификация, политики за достъп до данни	Класификация, криптиране на данни, одит на достъпа, dynamic authorization	Protect Data, Verify Explicitly, Assume Breach

Управление на процеса и организационна промяна

Преходът към архитектурата за нулево доверие изисква създаването на нови роли и отговорности, както и промяна в организационната култура.

- **Управление и визия:** Успешната трансформация започва с ясна визия и ангажираност от страна на висшето ръководство. Лидерите трябва да са наясно, че тази архитектура е дългосрочна стратегическа инвестиция, а не краткосрочен технологичен проект с бързи резултати.
- **Секторни екипи:** Внедряването засяга всички аспекти на ИТ и сигурността. Необходимо е създаването на многофункционални екипи, включващи експерти по идентичност, мрежи, крайни точки, приложения и данни, за да се осигури холистичен подход (Microsoft, 2024).
- **Промяна в работните процеси:** Най-голямото предизвикателство е преодоляването на страха от нововъведения и работни дейности. Това изисква непрекъснато обучение и комуникация, за да се обясни на служителите защо новите, по-стриктни мерки за сигурност са необходими и как те допринасят за защитата на работата на организацията. Преминаването към мислене „приемане на пробив" е в основата на тази промяна (Balarabe, 2024).

Управленския процес за България: Препоръки

При отсъствие на съществуваща рамка, България е най-добре да възприеме хибриден управленски модел, който съчетава елементи от централизирания и децентрализирания подход.

1. **Създаване на централен координационен орган:** Необходимо е да се определи водеща структура, която да разработи национална рамка и модел на зрялост за архитектурата за нулево доверие, адаптирани от моделите на САЩ. Този орган трябва да има правомощията да предоставя методологични указания и да координира дейностите между различните служби и структурни звена.

2. **Политически действия:** Необходимо е процесът да бъде стартиран с акт на Министерския съвет, което да придаде необходимата тежест и да осигури политическа подкрепа и бюджетно финансиране в дългосрочен план.

3. **Поетапно внедряване:** Вместо строги крайни срокове за пълно внедряване, е по-добре да се възприеме поетапен подход. Всяка служба трябва да бъде задължена да разработи собствен план за внедряване на базата на националната рамка и да се отчита ежегодно пред координационния орган за постигнатия напредък по нивата на зрялост.

4. **Изграждане на експертен капацитет:** Ключов елемент от управленския процес трябва да бъде създаването на програми за обучение и сертифициране на експерти по архитектурата за нулево доверие в рамките на държавната администрация и службите, за да се намали зависимостта от външни консултанти и да се изгради вътрешен капацитет за устойчиво развитие.

Предизвикателства, възможности и казуси

Преходът към архитектура с нулево доверие е сложен и многопластов процес, който надхвърля чисто технологичното внедряване. Той представлява фундаментална промяна в организационната структура, управленските процеси и културата на сигурност. Анализът на световния опит разкрива общи предизвикателства, но и значителни възможности за усъвършенстване на киберустойчивостта, които са пряко приложими и към контекста на българските служби за сигурност.

Основни предизвикателства при прилагането на модела за нулево доверие

Внедряването на архитектурата се сблъсква с препятствия в три основни направления: технологично, организационно и регулаторно.

1. Технологични предизвикателства

Наследени системи: Едно от най-големите препятствия е наличието на остарели системи и приложения, които не са проектирани да поддържат съвременни протоколи за автентикация, API-базиран достъп или динамични политики. Интегрирането им в ZTA среда е сложно, скъпо и понякога невъзможно без цялостна модернизация и надграждане на системата.

Сложност и оперативна съвместимост: Архитектурата за нулево доверие не е един продукт, а екосистема от взаимосвързани решения – за управление на идентичността, сигурност на крайните точки, микросегментация, мониторинг и т.н. (Microsoft, n.d.). Осигуряването на безпроблемна оперативна съвместимост между резултати от различни доставчици и избягването на „заключването” в една технология е сериозно предизвикателство пред инженерния сектор.

Управление на данните: За да се приложат ефективни политики за достъп, е необходимо данните да бъдат открити, класифицирани и етикетирани според тяхната чувствителност. В големи, наследствено натрупани масиви от информация, този процес може да бъде изключително труден и ресурсоемък, но е задължителна стъпка съгласно предложените по-горе модели (Zero Networks, 2024).

2. Организационни предизвикателства

Съпротива срещу промяната: Често най-голямото предизвикателство е човешкият фактор. Служителите и ИТ администраторите са свикнали с периметърния модел и имплицитното доверие във вътрешната мрежа. Преходът към среда, където всяко действие се проверява, може да бъде възприет като неудобство, забавяне на работата или липса на доверие, ако не е обяснен точно и конкретно.

Промяна в мисленето към „Приемане на пробив”: Философията, че пробивът е неизбежен, изисква и фундаментална промяна от превантивен към проактивен подход, фокусиран върху бързо откриване на пробиви и незабавна реакция (Red River, 2022). Това засяга начина, по който се проектират мрежите, как се разследват инциденти и как се разпределят ресурсите за сигурност.

Недостиг на умения: Внедряването и поддръжката на този модел изисква задълбочени познания в множество области – облачни технологии, управление на идентичността, автоматизация, анализ на данни. В българските служби за сигурност има осезаем недостиг на квалифицирани експерти.

3. Нормативна уредба и бюджет

Актуализация на нормативните актове: Съществуващите закони и подзаконови актове за защита на класифицирана информация често са писани с идеята за физически периметър на сигурност. В случай на внедряване на архитектурата за нулево доверие те трябва да бъдат преразгледани и актуализирани, за да отразят динамичния, базиран на идентичност и данни подход на модела.

Бюджетна несигурност: Тази архитектура е дългосрочна инвестиция, а не еднократен разход. Несигурността в бюджетното планиране и необходимостта от доказване на възвръщаемост на инвестициите пред политическото ръководство могат да забавят или спрат процеса. Управленският модел в САЩ, където преходът е наложен с президентски указ и подкрепен с бюджетни насоки от надзор, показва един от начините за преодоляване на това предизвикателство (Wiz, n.d.).

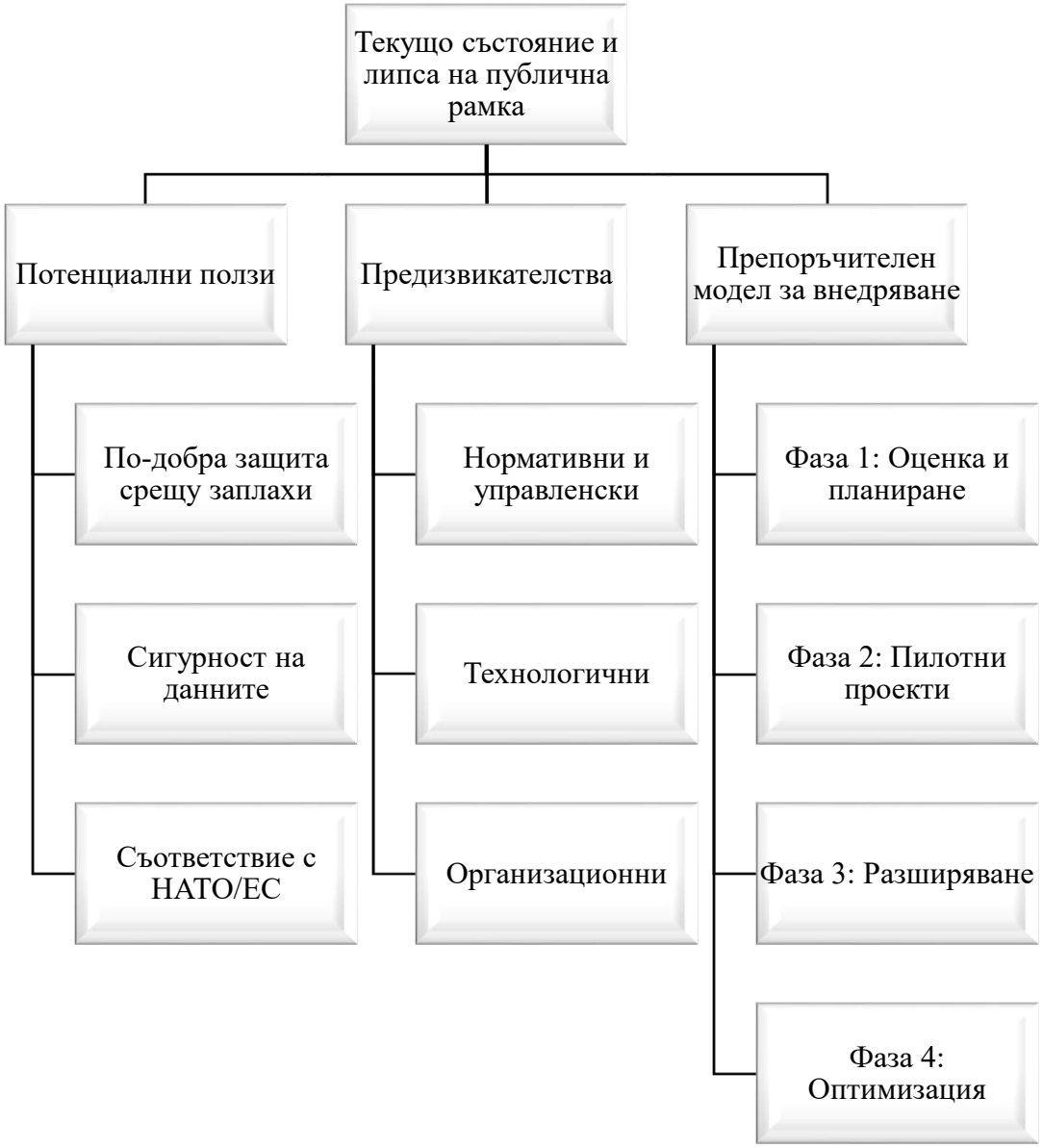
Възможности и стратегически ползи

Въпреки предизвикателствата, преходът към модела за нулево доверие открива значителни възможности за модернизация и повишаване на ефективността на службите за сигурност.

- **Подобрена видимост и ситуационна осведоменост:** Чрез непрекъснато събиране и анализ на телеметрия от всички компоненти

на архитектурата, този модел предоставя безпрецедентна видимост върху това кой, какво, кога, къде и как осъществява достъп до ресурси (CyberArk, n.d.). Това позволява бързо откриване на аномалии и потенциални заплахи.

- **Автоматизация и координация на сигурността:** Динамичният характер на архитектурата налага използването на автоматизация. Политиките за достъп могат да се прилагат автоматично, чрез програмиране и използване на умни договори, на базата на променящия се риск, а рутинните задачи по сигурността могат да бъдат оркестрирани, освобождавайки ценен човешки ресурс за по-сложни аналитични дейности. Ръководителите на Националната агенция за сигурност на САЩ силно наблягат на автоматизацията като ключов елемент за постигане на зрялост (NSA, 2024b).
- **Опростяване на архитектурата в дългосрочен план:** Макар първоначалното внедряване да е сложно, в дългосрочен план може да се достигне до опростяване на архитектурата. Чрез премахване на сложни мрежови сегменти и разнородни VPN решения в полза на унифициран, базиран на идентичност контрол, който намалява оперативната тежест и се подобрява потребителското изживяване.
- **Стимулиране на дигиталната трансформация:** Архитектурата за нулево доверие е ключов фактор, който позволява сигурното възприемане на облачни услуги, мобилна работа и технологични възможности, без да се прави компромис със сигурността.



Фигура 3. Ползи, предизвикателства и препоръчителен модел за внедряване в службите за сигурност на България

ЗАКЛЮЧЕНИЕ

Изследването за внедряването на архитектурата за нулево доверие в сферата на сигурността е новаторско решение, което вече се използва и дава положителни резултати. Настоящата дигитална среда предлага различни методи за компрометиране на националната сигурност и е задължително разузнавателните служби да използват иновациите, за да гарантират безопасността на обществото.

Архитектурата с нулево доверие се утвърждава като водещ стратегически отговор на съвременните предизвикателства в областта на киберсигурността. Нейното внедряване изисква не само технологична трансформация, но и дълбока промяна в организационната култура, управленските процеси и нормативната

среда. Успехът на тази трансформация е функция от ясна стратегическа визия, политическа подкрепа на институционално ниво и дългосрочен ангажимент към изграждане на устойчив вътрешен капацитет. За България приемането на ZTA не е въпрос на избор, а стратегическа необходимост, която се налага от геополитическите обстоятелства и непрекъснато променящите се киберзаплахи.

ЛИТЕРАТУРА:

Australian Cyber Security Centre. (2024, June 17). *New Zero Trust guidance: Seeking industry feedback*. www.cyber.gov.au

Australian Cyber Security Centre. (n.d.). *Foundations for modern defensible architecture*. www.cyber.gov.au

Australian Cyber Security Centre. (n.d.). *Modern defensible architecture*. www.cyber.gov.au

Balarabe, T. (2024, May 1). *What is Zero Trust Architecture (ZTA)? NIST 800-207 Zero Trust Architecture*. Medium. medium.com

Canadian Centre for Cyber Security. (2022, June). *A zero trust approach to security architecture* (ITSM.10.008). www.cyber.gc.ca

Cloudflare. (n.d.). *What is Zero Trust security?* www.cloudflare.com

CrowdStrike. (n.d.). *What is zero trust security?* www.crowdstrike.com

CyberArk. (n.d.). *What is NIST SP 800-207?* www.cyberark.com

Cybersecurity and Infrastructure Security Agency. (2023, April). *Zero trust maturity model* (Version 2.0). www.cisa.gov

Gartner. (n.d.). Zero trust architecture. www.gartner.com

IBM. (n.d.). *What is Zero Trust?* www.ibm.com

Illumio. (2021, July 14). *John Kindervag shares Zero Trust's origin story*. www.illumio.com

Khera, S. (2023, April 20). *Adopting Zero Trust principles: CISA's Maturity Model*. Zscaler. www.zscaler.com

Loshin, P. (2024, May 14). *History and evolution of zero-trust security*. TechTarget. www.techtarget.com

Microsoft. (2024, October 30). *Zero Trust adoption framework overview*. learn.microsoft.com

Microsoft. (n.d.). *What is Zero Trust architecture?* www.microsoft.com

National Cyber Security Centre. (2021, July 23). *Zero trust architecture design principles*. www.ncsc.gov.uk

National Cyber Security Centre. (2025). Industry assurance: Supporting a thriving cyber security industry. In *NCSC Annual Review 2025*. www.ncsc.gov.uk

National Security Agency. (2023, March 14). *NSA releases recommendations for maturing Identity, Credential, and Access Management* [Press release]. www.nsa.gov

National Security Agency. (2023, October 19). *NSA shares recommendations to advance device security within a Zero Trust framework* [Press release]. www.nsa.gov

National Security Agency. (2024, April 9). *NSA issues guidance for maturing data security* [Press release]. www.nsa.gov

National Security Agency. (2024, July 10). *NSA's final Zero Trust pillar report outlines how to achieve faster threat response* [Press release]. www.nsa.gov

National Security Agency. (2024, March 5). *NSA releases maturity guidance for the Zero Trust Network and Environment pillar* [Press release]. www.nsa.gov

Red River. (2022, April 20). *What are the three principles of Zero Trust?* redriver.com

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020, August). *Zero trust architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Wiz. (n.d.). *Zero Trust architecture: Principles and implementation*. www.wiz.io

Zero Networks. (2024, May 15). *Zero Trust pillars: Fast-tracking cyber resilience*. zeronetworks.com

Zscaler. (n.d.). *What is Zero Trust?* www.zscaler.com