Б Ъ Л Г А Р С К А  А К А Д Е М И Я  Н А  Н А У К И Т Е
ИНСТИТУТ ПО ИНФОРМАЦИОННИ И
КОМУНИКАЦИОННИ ТЕХНОЛОГИИ

Илиян Грозданов Илиев

# АВТОРЕФЕРАТ

на дисертация за присъждане на образователната и научна степен „доктор“

# ОПТИМИЗАЦИЯ НА ПРЕХОДА ОТ УПРАВЛЕНИЕ НА АСЕТИ КЪМ УПРАВЛЕНИЕ НА УСЛУГИ В СЛОЖНИ ФЕДЕРИРАНИ СИСТЕМИ В ПУБЛИЧНИЯ СЕКТОР

по докторска програма „Компютърни системи, комплекси и мрежи“
професионално направление 5.3. „Комуникационна и компютърна техника“

Научен ръководител: доц. д-р Велизар Шаламанов

София, 2026 г.

## Съдържание

## ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

Дисертационният труд е посветен на оптимизирането на прехода от управление на асети към управление на услуги в сложни федерирани системи в публичния сектор. Изследването разглежда цифровата трансформация не като внедряване на отделни технологии, а като цялостно архитектурно и организационно пренареждане на начина, по който се планират, предоставят и управляват цифровите услуги.

Актуалността на темата се определя от нарастващата зависимост на публичния сектор от разпределени цифрови услуги, които трябва да функционират надеждно при хетерогенна инфраструктура, ограничени бюджети, високи изисквания към сигурността и нужда от оперативна съвместимост между автономни участници. В този контекст service-centric моделът се разглежда като необходима следваща стъпка след традиционния ресурсно-ориентиран подход.

| | |
|---|---|
| **Автор** | Илиян Грозданов Илиев |
| **Научен ръководител** | доц. д-р Велизар Шаламанов |
| **Докторска програма** | „Компютърни системи, комплекси и мрежи“ |
| **Професионално направление** | 5.3. „Комуникационна и компютърна техника“ |
| **Обем на дисертацията** | 153 стр., 49 фигури, 6 таблици, 127 литературни източника |

### Актуалност на изследването

Системите за управление на ефективността в мрежите на публичния сектор са изправени пред специфични предизвикателства, произтичащи от разпределеното управление, хетерогенността на участниците и динамично променящите се обществени и политически приоритети. Широкото внедряване и комбиниране на цифрови технологии във всички сфери

на обществения и икономическия живот води до цялостно дигитално преобразование, което налага преход от управление на асети към управление на услуги.

Този преход има и по-дълбока историческа логика. В по-ранните етапи на развитие на комуникационните системи беше достатъчно до крайния потребител да бъде осигурена преносна среда, чрез която той да достига до централен изчислителен ресурс. При такъв модел обработката, съхранението и управлението на данните са концентрирани в центъра, а мрежата изпълнява ролята на канал за вход и изход. С нарастването на обема на данните, изискванията към качеството на услугите, необходимостта от сигурност и чувствителността към латентност този модел започва да показва ограничения, които не могат да бъдат преодолени само чрез още по-голяма централизация.

Съвременната дигитална трансформация в публичния сектор не се изчерпва с внедряване на отделни технологии, а представлява преосмисляне на начина, по който се планират, предоставят и управляват цифровите услуги. Този преход е особено сложен във федерирани системи, където множество автономни административни, комуникационни и изчислителни домейни трябва да взаимодействат при различни правила на управление, неоднородна инфраструктура и ограничен контрол върху свързаността, сигурността и капацитета.

В традиционния централизиращ модел акцентът е поставен върху самата инфраструктура и върху поддържането на отделни технически компоненти. В модела, ориентиран към услугите, фокусът се измества към стойността за крайния потребител, качеството на предоставяната услуга и способността на системата да използва наличните асети по гъвкав, координиран и мащабируем начин. В такава среда основният въпрос вече не е само кои технологии се използват, а как те се организират така, че крайният резултат да бъде надеждна, сигурна и икономически оправдана услуга, способна да работи и извън логиката на абсолютната централизация.

В дисертационния труд са разгледани четири представителни класа цифрови услуги: адаптивно мултимедийно разпространение чрез HLS, GPU-базирани изчислителни услуги чрез API и WebSocket, VoIP архитектури с директен медиен обмен и федеративен AIS облак за периферно събиране и обработка на телеметрия в реално време. Тези казуси са различни по приложение, но споделят общи архитектурни проблеми: разделение между управляващ и информационен слой, работа в хетерогенна и често NAT-ограничена среда, защита на идентичности и данни и ефективно използване на ограничени мрежови и изчислителни асети.

В рамките на настоящото изследване оптимизацията се разбира като инженерно и организационно подобряване на прехода към модел, ориентиран към услугите, според няколко основни критерия: намаляване на латентността и подобряване на отзивчивостта на услугите; повишаване на надеждността и устойчивостта при разпределена работа; защита на комуникацията, съдържанието и личните данни; по-ефективно използване на споделените асети; и приложимост в условията на публичния сектор, включително при ограничени бюджети, наследена инфраструктура и разпределена отговорност.

### Обект, предмет, цел и задачи

Обект на дисертационния труд са сложните федерирани системи в публичния сектор, в които множество автономни административни, комуникационни и изчислителни домейни взаимодействат при предоставянето на цифрови услуги.

Предмет на дисертационния труд са подходите, архитектурните модели и технологичните механизми за оптимизиране на прехода от управление на асети към управление на услуги в такива системи, разгледани чрез представителни казуси в областта на мултимедийното разпространение, високопроизводителните изчисления, комуникацията в реално време и федеративната телеметрия.

Основната цел на дисертационния труд е да се разработят подходи за оптимизиране на прехода от управление на асети към управление на услуги в сложни федерирани системи в публичния сектор.

За постигането на тази цел са поставени следните задачи:

1. **Да се анализират** предпоставките за преход от управление на асети към управление на услуги в публичния сектор, включително историческите, технологичните и организационните фактори, които определят необходимостта от такъв преход във федерирани среди, и на тази основа **да се формулират общи принципи и архитектурен модел за управление на услуги в сложни федерирани системи**, приложим към различни класове цифрови услуги в публичния сектор.
2. **Да се анализират криптографските рискове** в компютърните системи за повишаване на сигурността и надеждността на комуникационните услуги.
3. **Да се разработят методи за сигурен достъп до защитено съдържание** и защита на личните данни при предоставяне на цифрови услуги.

4. **Да се разработи архитектура за предоставяне на административни** и изчислителни услуги при поискване за обработка на големи обеми от данни в публичния сектор.
5. **Да се разработи хибридна архитектура** за предоставяне на комуникационна услуга в среда с инфраструктурни ограничения.
6. **Да се предложи архитектурно решение** за телеметрия в реално време в сложни федерирани среди.

### Методи на изследване

За реализиране на поставената цел и задачи са използвани следните методи на изследване:

- системен и сравнителен анализ на съществуващи технологии, архитектури и модели за предоставяне на цифрови услуги;
- исторически и контекстен анализ на развитието на комуникационната и цифровата инфраструктура;
- архитектурно моделиране на услуги и взаимодействия между автономни домейни във федерирана среда;
- анализ на сигурността и надеждността на комуникационни и изчислителни решения;
- проектиране и изследване на практически приложими решения, базирани на реално разработени и внедрени услуги;
- обобщаване на резултатите в общ модел за преход към управление на услуги.

### Обем и структура на дисертационния труд

Дисертационният труд е структуриран в пет глави, увод, заключение, библиография и приложения. В първа глава са разгледани историческите, технологичните и организационните предпоставки за дигитализацията на услугите във федерирани системи в публичния сектор. Във втора глава са анализирани сигурността и надеждността на комуникационните услуги в разпределена среда. Трета глава е посветена на методите за достъп до защитено съдържание и

на защитата на личните данни при видео разпространение. В четвърта глава е изследван преходът към предоставяне на цифрови услуги в публичния сектор чрез административни, изчислителни и федеративни телеметрични услуги. В пета глава са предложени архитектурни решения за оптимизиране на прехода от управление на асети към управление на услуги в реалновремеви комуникационни и телеметрични среди.

Дисертационният труд съдържа 153 страници, 49 фигури, 6 таблици и 127 литературни източника.

## КРАТКО ИЗЛОЖЕНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

### Глава 1. Дигитализация на услугите във федерирани системи в публичния сектор

Първа глава разглежда историческите, технологичните и организационните предпоставки за прехода от управление на асети към управление на услуги. Изследването започва от историческата еволюция на комуникационната среда в България и проследява как натрупаните инфраструктурни дефицити в Североизточна България се превръщат в показателен пример за регионален цифров разлом. Поставен е акцент върху разликата между видимите проявления на дигитализацията – е-услуги, регистри, платформи – и по-дълбоката инфраструктурна и организационна основа, без която тези услуги не могат да функционират надеждно.

Проследен е преходът от аналоговата телефонна мрежа, dial-up достъпа и ранните форми на интернет свързаност към DSL, LAN достъп, коаксиални мрежи и по-късното развитие на FTTH/PON. Анализът показва, че в редица отдалечени райони модернизацията дълго време е била икономически неизгодна за операторите, поради което изоставането се натрупва едновременно като нисък капацитет, висока латентност и ограничена организационна способност за предоставяне на съвременни цифрови услуги. В този контекст са разгледани както техническите характеристики на средата, така и социално-икономическите последици – миграция, отслабване на местния капацитет и забавяне на дигиталната трансформация.

Показано е, че глобални фактори като пандемията от COVID-19 и войната в Украйна ускоряват преоценката на широколентовата свързаност като условие не само за удобство, а за

устойчива гражданско-военна и административна инфраструктура. В тази рамка са анализирани и новите подводни и сухоземни оптични проекти в Черноморския регион, както и значението им за преодоляване на натрупаното изоставане. Изводът е, че физическата инфраструктура остава незаменима основа, но реалната обществена стойност възниква едва когато върху нея бъдат организирани координирани цифрови услуги.

На тази основа в главата се извежда преходът от управление на комуникационни асети към управление на услуги. В традиционния модел фокусът е върху отделните технически ресурси – линии, сървъри, маршрутизатори, приемници. В ориентиран към услугите модел, фокусът се измества към начина, по който тези асети се комбинират и управляват така, че да осигуряват надеждна, сигурна и мащабируема услуга. Това налага ясно разделение между контролен слой (control-plane) и слой за данни (data-plane), както и нова гледна точка към латентността, сигурността и ефективността.

В първа глава са дефинирани и четирите представителни класа услуги, които се използват като аналитични казуси в дисертацията: HLS адаптивно мултимедийно разпространение; CUDA анализи през API/WebSocket като „GPU като услуга“; VoIP direct P2P като комуникация в реално време; и федеративен AIS облак за събиране и обработка на телеметрия. Сравнителният анализ между тях показва, че макар да са различни по приложение, всички изискват архитектурно разделение на функциите, механизми за сигурност, устойчивост при ограничения на свързаността и възможност наличните ресурси да бъдат предоставяни като услуга, а не като локално притежаван асет.

Особено внимание е отделено на федерираните системи като естествен отговор на ограниченията на абсолютната централизация. Главата обобщава основните им свойства – автономност на участниците, оперативна съвместимост, сигурен обмен на информация и по-ефективно използване на ресурсите. Като практически значим пример е разгледана AIS средата, в която множество брегови станции, платформи и оператори взаимодействат без да съществува единен централен собственик на всички активи. Показано е, че именно тук възниква необходимостта от междинен федеративен слой за нормализация, дедупликация и координирано предоставяне на данните.

В края на главата са формулирани критериите за оптимизация на прехода към управление на услуги: латентност и отзивчивост, надеждност и устойчивост, сигурност, ефективност при използване на асетите и организационна приложимост. Тези критерии служат като обща рамка за следващите глави, в които се изследват отделните технологични

реализации. Изводът е, че не отделната технология, а архитектурният модел определя дали дадена цифрова среда ще остане набор от ресурси или ще се превърне в система за предоставяне на услуги.

За целите на настоящия дисертационен труд оптимизацията на прехода от управление на асети към управление на услуги се разглежда като многокритериална задача, включваща взаимосвързани инженерни и организационни подобрения.

Първият критерий е латентност и отзивчивост на услугата, което е особено съществено при комуникация в реално време, видео стрийминг и интерактивни изчислителни заявки.

Вторият критерий е надеждност и устойчивост, разбирани като способност на системата да поддържа услугата при инфраструктурни ограничения, откази на отделни възли и променливи мрежови условия.

Третият критерий е сигурност, включваща защита на комуникацията, съдържанието, идентичностите и личните данни, както и ограничаване на последствията при компрометиране на отделни компоненти.

Четвъртият критерий е ефективност при използване на асетите, тоест възможност наличните мрежови, изчислителни и организационни асети да бъдат комбинирани и предоставяни така, че да се постигне по-висока стойност на услугата при ограничени ресурси.

Петият критерий е организационна приложимост, която е особено важна в публичния сектор, където решенията трябва да работят в условия на наследена инфраструктура, ограничени бюджети, разпределена отговорност и необходимост от оперативна съвместимост между автономни участници.

Въз основа на тези критерии в следващите глави се оценяват предложените архитектурни решения и се проследява как те допринасят за оптимизиране на прехода от управление на асети към управление на услуги в различни класове цифрови услуги.

В първа глава беше проследено историческото развитие на комуникационната инфраструктура и бяха изведени причините, поради които в съвременната дигитална среда се налага преход от управление на асети към управление на услуги. Показано бе, че историческите инфраструктурни разломи, ограничената регионална свързаност, нарастващите изисквания към латентност, капацитет и сигурност, както и необходимостта от оперативна съвместимост между автономни участници правят класическия централизиращ модел все по-малко достатъчен.

Анализът на разгледаните класове услуги показа, че независимо от различията помежду им, те споделят общи архитектурни проблеми: необходимост от ясно разграничение между управляващи и информационни функции, защита на идентичности и данни, ефективно използване на комуникационните и изчислителните асети и възможност за предоставяне на функции като услуги, а не само като локално притежавани ресурси.

На тази основа федерираните системи се явяват естествена архитектурна посока за развитие, тъй като позволяват съчетаване на автономност, координация и споделяне на услуги между различни домейни. Именно в този контекст следващите глави разглеждат последователно криптографската основа на доверието, сигурното предоставяне на защитено съдържание, изчислителните услуги при поискване и архитектурните решения за комуникация и федеративна телеметрия в реално време.

## Глава 2. Методи за осигуряване на надеждност при управление на комуникационни услуги

Втора глава е посветена на надеждността и киберустойчивостта на комуникационните услуги в условията на неравномерна дигитализация. Изведена е тезата, че при ускорено навлизане на цифрови технологии в публичния сектор наред с инфраструктурния се формира и киберсигурностен разлом. Затова надеждността на цифровите услуги трябва да се разглежда не само като въпрос на свързаност и капацитет, а и като въпрос на правилно подбрана криптографска основа.

Основният аналитичен фокус е върху слабостите на RSA, когато генераторите на случайни числа работят при ниска ентропия. Разгледани са примери и изследвания, които показват, че неправилното генериране на случайност може да доведе до предвидими криптографски параметри, общи делители между различни RSA ключове и практически компрометиране на системи, използващи иначе „силен“ алгоритъм. Показано е, че проблемът не е само в математическия модел на RSA, а в реалната изчислителна среда, в която той се прилага.

Глава втора разглежда подробно значението на източниците на ентропия, ролята на PRNG и TRNG и ограниченията на Linux-базираните системи при ранно зареждане, когато системната случайност все още не е достатъчно натрупана. Анализирани са възможностите за

използване на хардуерни механизми за ентропия, включително Intel Secure Key, като практически приложима мярка за повишаване на надеждността на криптографските процеси.

На тази основа е аргументиран преходът от RSA към ECC като по-подходяща криптографска основа за разгледаните в този дисертационен труд услуги, функциониращи в разпределени и ресурсно ограничени среди. Показано е, че ECC осигурява съпоставимо ниво на сигурност при значително по-къси ключове, по-малко натоварване на изчислителните ресурси и по-добра приложимост при edge устройства и вградени платформи. Разгледани са ECDSA и ECDH върху NIST криви като практически приложима рамка за удостоверяване и договаряне на ключове в бъдещите архитектури, разработени в дисертацията.

В главата е очертана и перспективата за развитие към post-quantum устойчивост. Макар тя да не е предмет на самостоятелна разработка в дисертацията, анализът показва, че изборът на криптографска схема следва да бъде мислен не еднократно, а като етап от по-дълъг цикъл на адаптация към нови рискове. Така втора глава изгражда криптографската и удостоверителната основа на целия дисертационен труд и подготвя следващите глави, в които сигурността вече се разглежда като част от модела на самата услуга.

Там, където развитието е било непоследователно, фрагментирано или дълго време подчинено на частични и закъснели решения, се натрупват не само ограничения в свързаността и капацитета, но и уязвимости в сигурността. В този смисъл ескалацията на киберпрестъпленията, посегателствата върху лични данни, финансовите злоупотреби, загубата на информация и изнудването, свързано с нея, не са просто страничен ефект от по-широкото използване на технологии, а индикатор, че дигиталната трансформация често протича при неравномерно изградена киберустойчивост. Това показва, че наред с инфраструктурния разлом съществува и взаимосвързан разлом в киберсигурността, който изисква не изолирани мерки, а последователен архитектурен подход към надеждността и защитата на комуникационните услуги. (Jang-Jaccard and Nepal, 2014), (Kostadinov and Atanasova, 2019), (Dineva and Atanasova, 2019).

Спазването на изискванията за киберсигурност е предпоставка за сигурността и безопасността на ИТ инфраструктурите, цифровите ресурси и защитата на личните данни. В това отношение темите за криптографията и достатъчно надеждното генериране на случайни числа, които са в основата на всяка система за криптиране, са от особен интерес (Shalamanov, 2020).

За нуждите на съвременната криптография се използват два вида генератори на случайни числа - истински генератор на случайни числа (TRNG) и генератор на псевдослучайни числа (PRNG) (DiCarlo, 2012).

Генератор на истински случайни числа (TRNG): прилага се, когато RNG трябва да генерира стойности в даден момент, които трябва да са уникални и да не се повтарят в последващи RNG извиквания (Carr, 2003), (L'Ecuyer, 2007). Числата, получени с този тип RNG, се прилагат за операции, които изискват уникални/неповтарящи се числови стойности, генерирани във времето. (Jin, 2004), (Camara, 2019) Пример за такава ситуация е генерирането на криптографски ключ за кодиране/декодиране на данни, инициализиращи вектори, начални числови стойности (seed) за контролирани RNG и др. (Ergün, 2015), (Ryabko et al., 2016)

Генератор на псевдослучайни числа (PRNG): Като основа за този генератор се използва начално случайно число от микро или макро света (seed), а за следващите числа се използва математическа формула. От началната стойност, чрез прилагане на определен алгоритъм, произлизат всички генерирани впоследствие случайни числа. Последващите стойности, по реда им, са възпроизводими. Единствената неочаквана и тайна стойност, която трябва да бъде възможно най-непредсказуема, е началното число, което е „коренът" в основата на тази поредица и инициира генерирането на цялата числова поредица. От тази технология са заимствани удостоверяването с еднократна парола (OTP), генерирането на криптографски ключове, получени от главния коренов ключ (прилага се при съставянето на портфейли в BlockChain - технология на разпределения регистър), удостоверяването чрез HMAC и други.

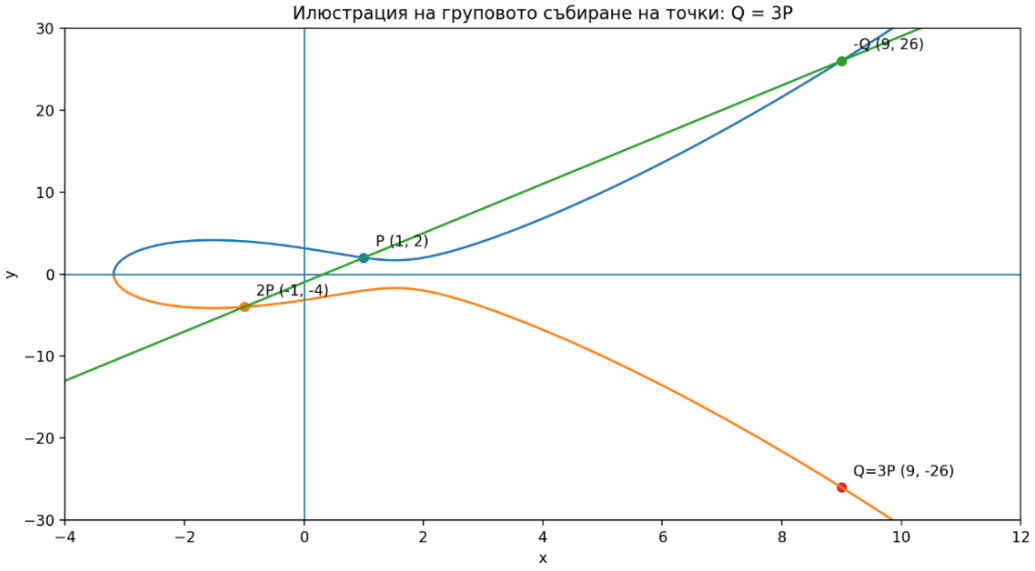
Проблеми с генератора на случайни числа (RNG) са в основата на недостатъка в цифровия сертификат на тайвански гражданин. Бернщайн, Чанг, Ченг, Чоу, Хенингер, Ланге и ван Сомерен представиха доклад по време на Asiacrypt 2013 (Bernstein et al., 2013), в който показаха, че официалните смарт карти за идентификация на граждани, издадени от тайванското правителство, са дефектни. Резултатите им се основават на изследването на (Heninger et al., 2012) върху ключове за сигурност с ниска ентропия. Къде те изследват ключовете за сигурност с ниска ентропия и дали подобни недостатъци могат да бъдат открити в тайванската база данни „Citizen Digital Certificate"? Изследователите са водили проучването с 2 милиона 1024-битови RSA ключа от тайванската база данни „Citizen Digital Certificate" и са установили, че 184 от тези ключове са тривиални за изчисляване в рамките на няколко часа. Те отдават тези слаби RSA ключове на фатален недостатък в хардуерния генератор на

случайни числа (RNG). Случайността, използвана за генериране на RSA ключове, е съдържала недостатъчна ентропия и е създала предвидими модели за RSA прости числа.

В статия, публикувана през 2012 г. (Heninger et al., 2012), е показана слабост в TLS (Transport Layer Security) и SSH (Secure Shell) сървъри, включваща слаби ключове за сигурност. Те разкриват, че неправилно функциониращите генератори на случайни числа (RNG) водят до ниска ентропия на случайността за RSA и DSA сървърните ключове, което е причина за компрометирана криптография. Изследователите посочват, че тази уязвимост се дължи на наличието на дупка в ентропията в RNG (/dev/random и /dev/urandom). По време на зареждане /dev/random използва данни, останали от предишното зареждане, за пула на ентропията. Но когато системата е била изключена за дълго време и паметта се върне в основното си състояние, тези данни са предвидими.

RSA алгоритъмът се счита за по-бавен. Обикновено RSA ключовете са с дължина 2048 и 4096 бита. От гледна точка на сигурността на RSA, 2048-битовите RSA ключове не се считат за напълно сигурни. Ето защо повечето организации в момента преминават към 4096-битови ключове. Много организации обаче избягват RSA криптирането поради бавното генериране/алгоритъм на ключовете и поради максималната консумация на машинни ресурси.

Публично са известни P и Q. Тайната (частният ключ) е скаларът d в равенството Q = d·P. Да се изчисли Q от (P, d) е лесно, но да се възстанови d от (P, Q) е трудно при коректно избрани параметри и достатъчно голям порядък на групата, известно в математиката като проблем за дискретния логаритъм върху елиптични криви. ECDLP е фундаментална твърда математическа задача, на която се крепи сигурността на съвременната криптография с елиптични криви (ECC). За “обратния път” в ECC (да се намери $d$ от Q = d·P) стандартният аргумент за трудност е, че в общия модел всяка атака срещу дискретния логаритъм изисква поне Ω() групови операции, където $p$ е най-големият прост делител на реда на групата — т.е. на практика расте като квадратен корен от размера на групата и става непосилно при правилно избрани параметри (Shoup, 1997).




Фиг. 2.2. Илюстрация на груповото събиране на точки: Q = 3P.

За автономни системи от федеративния AIS облак, които често работят върху вградени устройства (Raspberry Pi, edge приемници/форуърдъри), е важно асиметричните операции да са бързи и да не „надуват“ трафика. Алгоритмите базирани на криптографията на елиптичните криви – ECDSA за подписи и ECDH за договаряне на ключ, дават еквивалентна криптографска устойчивост при значително по-къси ключове и подписи спрямо RSA, което е практично за защита от край до край при транспорт между възлите в облака.

NIST Digital Signature Standard (FIPS 186-5) дефинира ECDSA и утвърдените „NIST криви“ P-256, P-384 и P-521, които са широко поддържани в стандартни криптографски библиотеки и хардуерни модули.

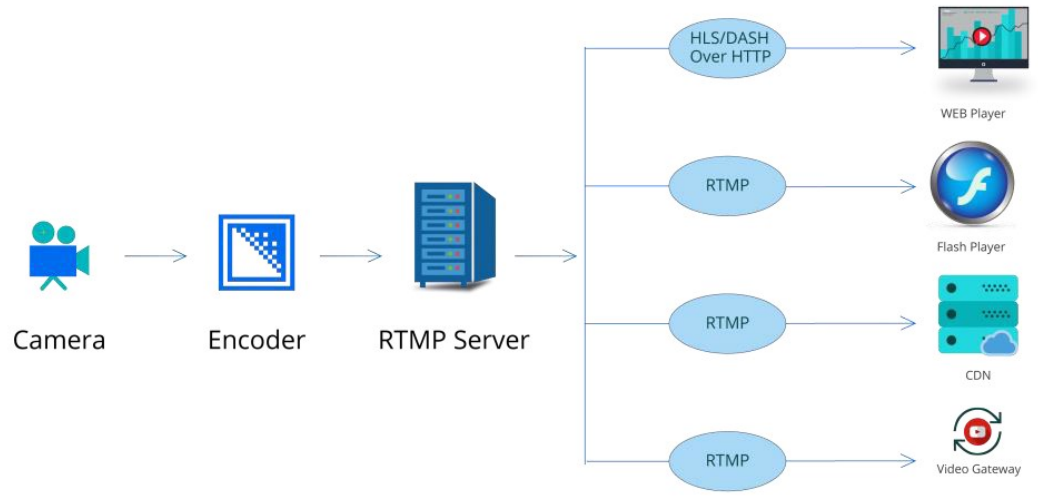
Съгласно препоръките за еквивалентна сила на сигурност (напр. SP 800-57 Part 1), P-256 е типичен избор за около 128-битова устойчивост: публичните ключове и подписите са компактни (десетки байтове), докато RSA за сходно ниво изисква ключове от порядъка на 3072 бита, което увеличава латентността, размера на сертификатите и натоварването при подписване/верификация.

Подобни принципи – подписване на AIS съдържание за автентификация и цялост при запазване на обратна съвместимост – са демонстрирани и в Protected AIS (pAIS), където се използвасхема за съвместимост с криптография, за да се адресират известни AIS уязвимости и да се запази интероперабилност с немодифицирани AIS устройства (Gary Kessler, 2020).

## Глава 3. Методи за достъп до защитено съдържание

Трета глава разглежда методите за достъп до защитено съдържание и възможностите за ограничаване на изтичането на лични данни при предоставяне на мултимедийни услуги. Изходната постановка е, че в съвременния уеб стрийминг защитата на комуникацията и защитата на идентичността на потребителя трябва да бъдат разглеждани като различни, макар и взаимосвързани функции. На тази основа в главата е предложен архитектурен подход, при който разпространението на съдържанието се отделя от процеса на удостоверяване на крайния потребител.

Разгледана е типичната схема на видео разпространение през RTMP нагоре по веригата и HLS към крайния потребител (Фиг. 3.3). Услугата за уеб стрийминг е по същество комбинация от протоколи за upstream (предаване нагоре по веригата) към стрийминг сървъра и downstream (надолу по веригата) към крайните потребители, като най-често използваният набор е RTMP + HLS. Такова разделение на протоколите се е наложило през годините поради спецификата на свързаността на потребителите. Според HLS, видео потокът се разделя на парчета, като периодично се изтегля и чете текстов плейлист в стандартизиран M3U формат, който описва парчетата, достъпни за изтегляне. За да се постигне надеждност на услугата, разпределение на натоварването и ниска латентност към крайния потребител, стрийминг платформата се изгражда на CDN схема с множество възли, които са географски разпределени.




Фигура 3.3. Диаграма, представяща процеса на RTMP стрийминг (източник synopi.com).

Показано е защо HLS е практически подходящ за широкото потребителско разпространение – поддръжка в браузъри и HTML5 плейъри, работа върху HTTP(S), по-добра устойчивост при домашни и мобилни мрежи и възможност за прилагане на стандартни механизми за удостоверяване и авторизация. В същото време е обосновано, че защитата на RTMP комуникацията между студиото и сървъра е по-надеждна чрез предварително изграден криптографски тунел, отколкото чрез разчитане единствено на RTMPS върху крайни устройства с ограничени възможности за сигурност.

Съществен принос на главата е идеята за разделяне между съдържанието и удостоверяването. Разработен е тестов модел, в който видео дистрибуторът не обработва чувствителни лични данни, а потребителската автентификация и издаването на токени се възлагат на отделна доверена услуга. В резултат дори при компрометиране на стрийминг инфраструктурата рискът от изтичане на лични и платежни данни е значително ограничен. Така сигурността не се постига само чрез криптиране, а чрез функционално разделяне на отговорностите.

Главата разглежда и възможността за регионално и локално преразпределение на защитено видео съдържание в среда на малки и регионални интернет доставчици. Изведена е тезата, че при наличие на локална PON инфраструктура и ограничена външна интернет свързаност операторът може да приема един входящ висококачествен поток и да го преразпространява в собствената си мрежа, като така намалява външния трафик и подобрява качеството на услугата за абонатите. Тази логика е поставена в регламентирана среда на контрол на достъпа и защита на ключовия материал, за разлика от историческите практики на нерегламентиран LAN file sharing.

Изводът от трета глава е, че сигурното предоставяне на съдържание не се свежда до базово криптиране на видеофрагменти, а изисква цялостен сервизен модел, в който транспортът, удостоверяването, издаването на ключов материал и локалното разпространение са организирани съгласувано. Така се повишава киберустойчивостта на услугата, намалява се зависимостта от ограниченията на външната интернет свързаност и се подготвя преходът към по-сложни административни и изчислителни услуги в следващата глава.

Тук идва моментът на втория аспект на изследването, който се отнася до видео дистрибутора и разглежда защитата на видео съдържанието спрямо крайните потребители. Тъй като специфичното видео съдържание е предназначено за строго определена група

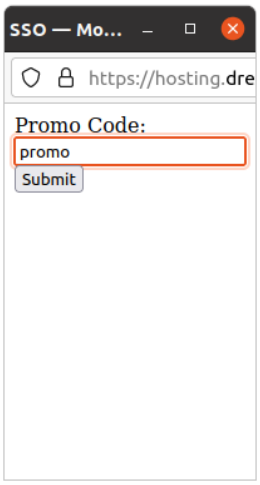
потребители, следва, че HTTPS сървърът първо трябва да бъде конфигуриран съгласно най-добрите практики за сигурност (https://www.ssl.com/guide/ssl-best-practices/). След това трябва да се внедрят механизми за удостоверяване на потребителите.

За нуждите на изследването е разработен симулатор на такива процеси в бекенда, функциониращ между „голата“ HLS услуга на nginx и крайния потребител, който се грижи за предоставянето на токен на потребителя в бисквитка след валидно удостоверяване и съответно валидира токените от клиентските заявки. Ако токенът не е подаден или е невалиден (изтекъл), бекендът връща 401 Неоторизирано (Mueller, 2015).

Възможностите за получаване на токен са многобройни и разнообразни. Те зависят най-вече от управленските решения на организацията или групата организации.

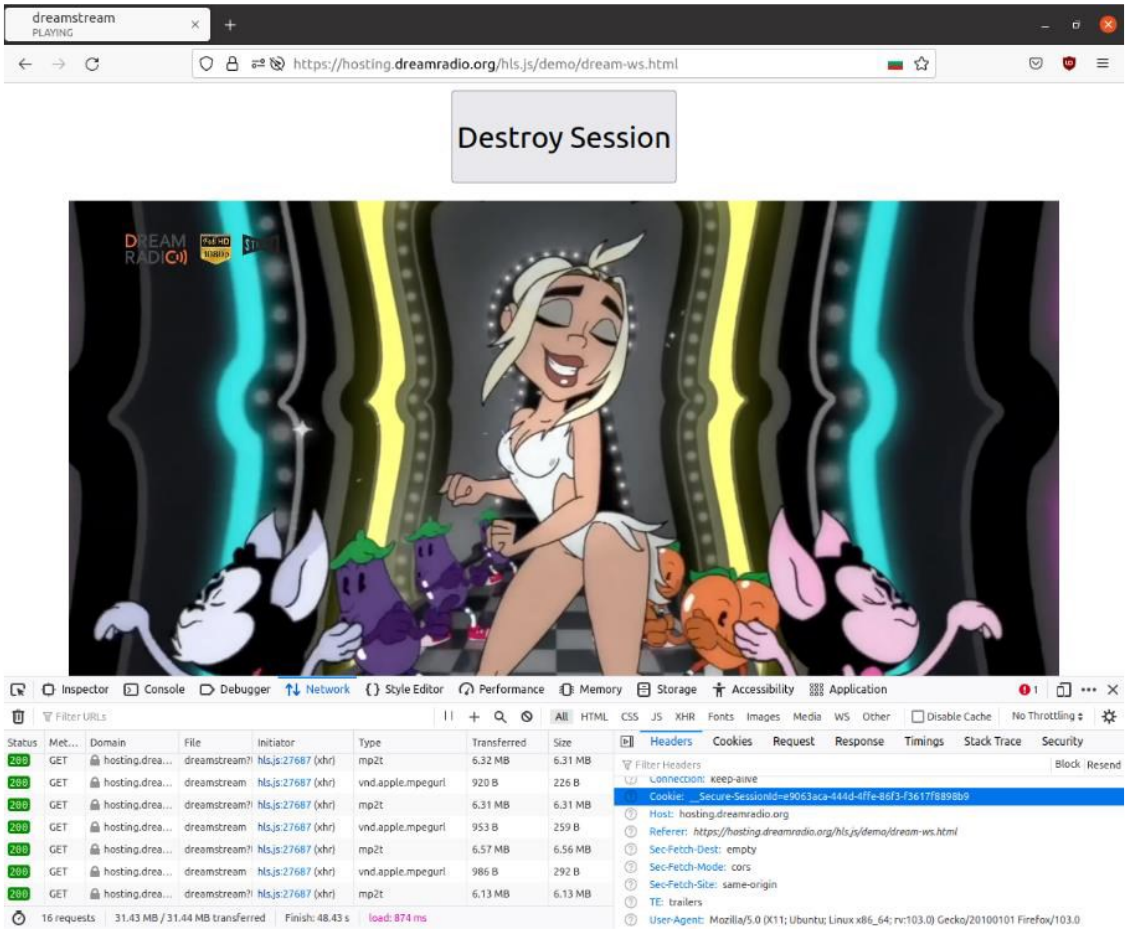
В тази дисертация е разработена семпла услуга за SSO вход за демонстрация.

След извикване на услугата SSO (Фиг. 3.6) и успешно преминаване на процеса на удостоверяване, се стартира потребителска сесия на приложението с произволно генериран криптографски защитен идентификатор и бисквитката на сесията се връща в отговора към клиента.




Фиг. 3.6. Формуляр за получаване на токен за оторизация.

Клиентът е длъжен да предостави токена, за да поддържа сесията активна (Фиг. 3.7). Времевият прозорец, през който токенът е валиден, както и времето за преиздаване, подлежат на дефиниране на управленско ниво, а не на техническо.




Фиг. 3.7. Оторизиране към стрийминг сесия с бисквитки

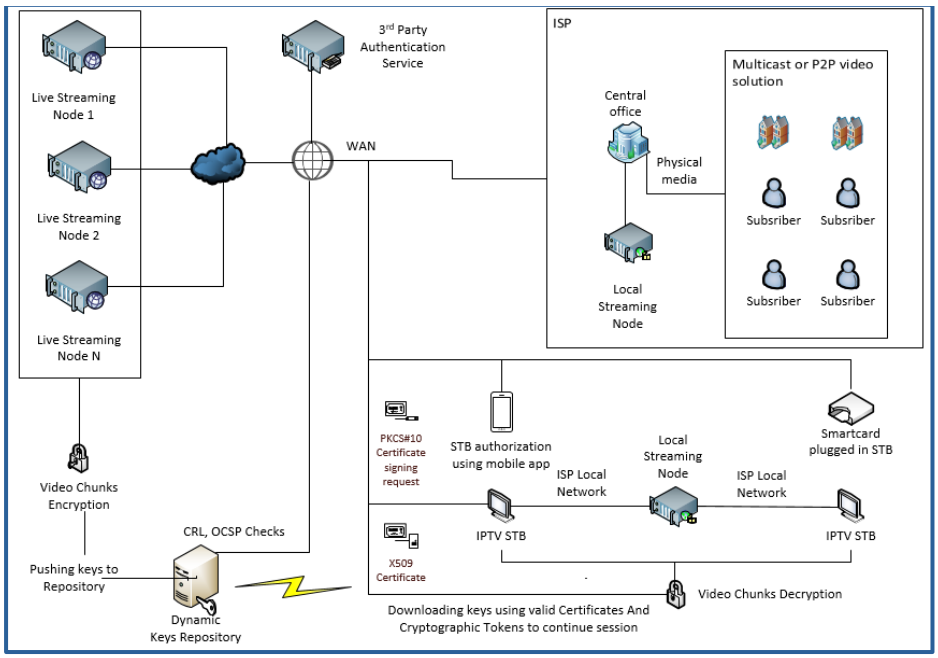
Внедряването на тази SSO услуга има за цел да демонстрира, че самото разпространение на видеото и удостоверяването на потребителите могат да бъдат разделени между различните организации. Това означава, че излъчващата организация и доставчикът на доверие могат да бъдат напълно разделени.

Разработен е и разширен модел за условен достъп (Фиг. 3.13), при който ключовете за декриптиране на HLS потоците се предоставят само след успешно удостоверяване и иницииране на потребителска сесия. По този начин се съчетава логиката на защитеното мултимедийно разпространение с минимизиране на обработката на лични данни от страна на самия дистрибутор. Показано е, че този подход е практически приложим както към по-големи, така и към по-малки стрийминг проекти.

По този начин, изтеглянето на всеки ключ ще бъде защитено от потребителска сесия на приложението срещу неоторизирано изтегляне.

Първоначално потребителят се идентифицира пред доставчик на удостоверителни услуги, който е интегриран със системата, и създава профил за него. Обикновено идентификацията се извършва дистанционно и профилът е достъпен чрез мобилно приложение.

Стрийминг услугата криптира AES ключа всеки път с публичните ключове на всеки x509 сертификат, абониран за стрийма на живо, и изпраща криптираните AES ключове към хранилището.




Фиг. 3.13. Обща схема за дистрибутиране на стрийминг на живо в локална интернет среда

По този начин в дисертацията са разгледани възможностите за защита на комуникацията между стрийминг студиото и RTMP сървъра, от една страна, и HLS комуникацията между видео дистрибутора и крайния потребител, като е предложена идея за внедряване на портал за удостоверяване на потребителите, предоставен от доставчик на услуги за удостоверяване, който освобождава видео дистрибутора от обработка на лични данни и платежни средства. За целите на изследването предложеният подход беше реализиран на тестов сървър, откъдето бяха представени резултатите от изследването. Предимството на предложения подход за защита на стрийминг съдържанието е, че може да се приложи към всякакъв вид високобюджетен или нискобюджетен проект. Също така не се изисква

дистрибуторите на съдържание да се грижат за администрирането на личните данни на потребителите. Това води до още по-висока киберустойчивост на предложеното решение, защото дори при всяко нарушение на сигурността на сървър, няма лични данни, които могат да бъдат откраднати.

## Глава 4. Управление на услуги в сложни федерирани системи в публичния сектор

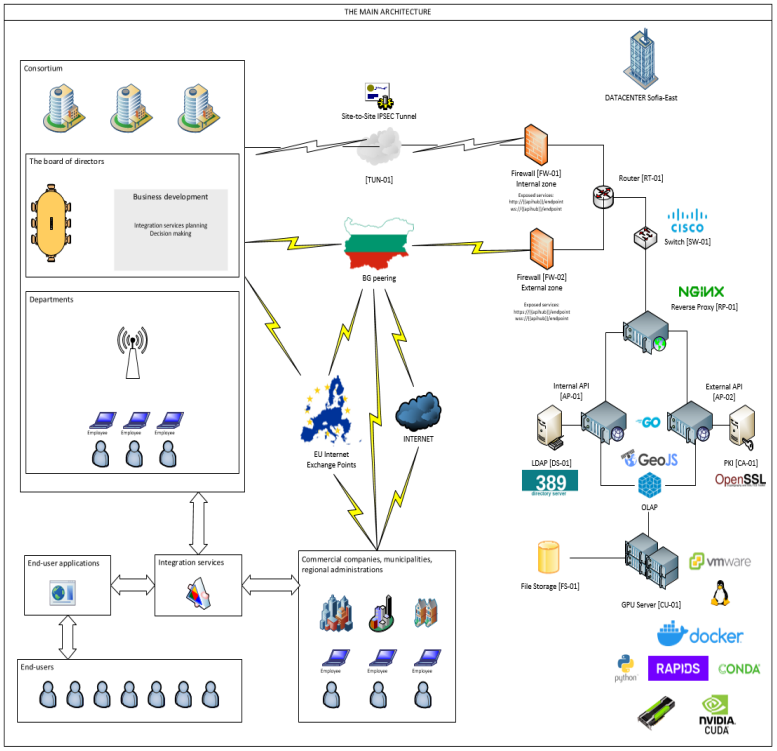
Четвърта глава разглежда управлението на услуги в сложни федерирани системи в публичния сектор чрез три взаимосвързани направления: административни услуги, изчислителни услуги при поискване и федеративна услуга за събиране и предварителна обработка на потокова телеметрия. Общата идея е, че преходът към ориентиран към услугите модел може да се реализира както чрез централизирани изчислителни услуги, така и чрез разпределени федеративни механизми, в зависимост от характера на задачата.

В първото направление е показано, че сложни аналитични и административни функции могат да се предоставят като услуга, вместо да се дублират локално във всеки офис или администрация. Разработена и имплементирана е архитектура с HTTP API за приемане на файлове и задачи, обратна WebSocket сигнализация за известяване в реално време и самостоятелен демон insightd, който изпълнява GPU-ускорената обработка чрез RAPIDS. Така API/WebSocket слоят функционира като междинен service layer между потребителите на анализа и самата изчислителна услуга.

Анализът на геопространствените данни е ключов фактор за дигиталната трансформация и регионалното развитие в случая на градоустройството, решавайки проблеми с трафика, включително като ясна посока за прехода към умни градове (Erskine et al, 2014). Тя е от съществено значение и за търговските организации чрез вземане на решения в редица случаи като планиране на мрежово покритие, инвестиционни изследвания, оценка на риска и анализ на пазара (Wickramasuriya et al., 2013). Така наречените услуги за онлайн аналитична обработка (OLAP) стават все по-необходими (Rivest et al., 2005), тъй като предоставят различни механизми за анализ на геоданни в отдалечени дигитални среди, позволявайки това да се извършва напълно автоматично. Човешката история многократно е показвала, че всяка промяна или революция е трудна, болезнена и се случва в продължение на дълъг период от време. Тук не се наблюдава изключение. Днес работният процес все още не е автоматизиран,

въпреки всички практически изисквания за развитието на компютърните технологии в момента.

Анализирани са основните практически проблеми на дигиталната трансформация в администрациите: липса на достатъчно ИТ умения, частична и несинхронизирана трансформация, високи разходи за специализиран хардуер и трудности при интеграцията между различни системи. Предложеният модел решава тези проблеми чрез централизиране на тежките изчисления и предоставяне на стабилен интерфейс към вътрешни и външни потребители. Това означава, да се предоставят онлайн услуги за анализ на геопространствени данни (Фиг. 4.1). Същевременно партньорските организации увеличават интереса си към тази област, като създават авангардни продукти. Освен това, повечето от тях не биха искали да създават сложна инфраструктура за тази дейност и биха се отказали от разработването на собствен софтуер, който изисква задълбочени познания за многомерна обработка на данни. Следователно, те биха се съсредоточили върху разработването на високо ниво на софтуер и услуги за своя бизнес и в този случай предоставянето на онлайн аналитична услуга ще бъде чудесна възможност за това.



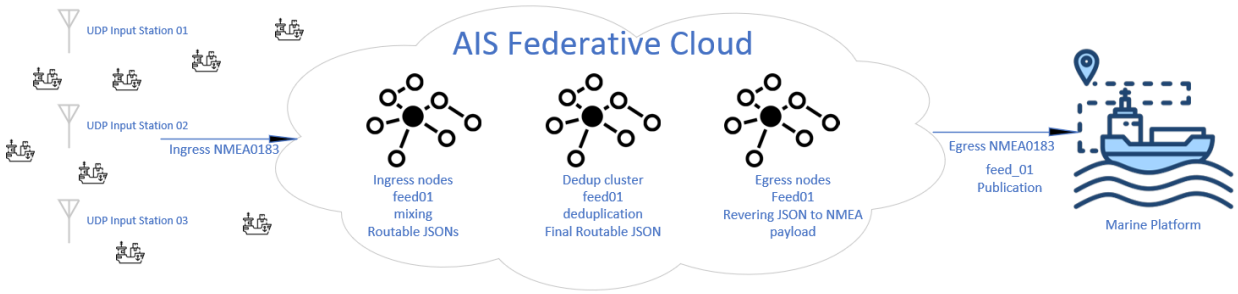

Фиг. 4.1. Представяне на основната архитектура на платформата, разработена в тази дисертация.

Целта на предоставянето на API услугата е, от една страна, да се даде възможност за интеграция с потенциално заинтересовани организации, които да се възползват от централизирана услуга за анализ на данни (de Castro Lima, 2018), а от друга страна, да се улеснят техническите им задачи в сравнение с това сами да предприемат действия за изграждане на собствени услуги за анализ на данни. Като важен момент трябва да се спомене, че само с изграждането на API услуги задачите по интеграция не се изчерпват, тъй като те не представляват еднократно действие във времето, а подлежат на промени и подобрения. В тази връзка е необходимо да се наблегне на CI/CD подходите, които следват установените принципи, а за организации, които не разполагат с висококвалифициран персонал, това може да бъде особено предизвикателство.

Втората линия в главата е свързана с федеративния AIS облак. Тук паралелизмът не се разбира като ускоряване на една централизирана задача, а като едновременно съществуване на множество потокови процеси по приемане, нормализация, дедупликация, маршрутизиране и доставка. Показано е, че AIS средата изисква различен архитектурен подход: данните пристигат непрекъснато, от множество източници, и изискват незабавна предварителна обработка близо до мястото на приемане.

На тази основа е предложен архитектурен модел на федеративен AIS облак (Фиг. 4.7) с ясно разделение между control-plane и data-plane, както и с роли ingress, transit, dedup и egress. Важна характеристика на този модел е, че една и съща автономна система може да изпълнява различни роли за различни логически потоци, а вътрешната ѝ реализация остава автономна, стига да поддържа договорения интерфейс към останалите участници. По този начин услугата се изгражда върху федерация от оператори, а не върху централен собственик на всички приемни точки.

Вътрешната архитектура на всяка AS е напълно автономна (може да е един процес или голям клъстер), а общото поведение се формира от стандартен външен интерфейс: идентичност (с механизми на асиметрична криптография), функционални възможности и правила за сдвояване, отчетност.




Фиг. 4.7. Обща архитектурна схема на AIS федеративен облак, предложена в тази дисертация

Ролите Ingress, Transit/bridge, Dedup/aggregator, Egress не са фиксирани за дадена AS. Една и съща AS може да изпълнява различни роли за различни логически потоци. Федеративният характер идва от това, че системата не налага един „правилен“ софтуер, всеки оператор може да избере технологичен стек, стига да поддържа интерфейса към останалите. От практическа гледна точка предложеният модел следва да отговаря едновременно на изисквания за лесно включване на нови участници, съвместимост със съществуващите морски платформи и устойчиво нарастване на броя възли без концентрация на обработката в един център.

Изводът от четвърта глава е, че управлението на услуги в сложни федерирани системи не предполага единствена архитектурна рецепта. При част от задачите е по-ефективно централизирането на изчислителната тежест и предоставянето ѝ като услуга, а при други е необходима разпределена федеративна организация близо до източника на данни. И в двата случая обаче решаващи са ясното разделение на функциите, възможността за координирано управление и освобождаването на крайните участници от притежаването и поддържането на всички необходими локални асети.

Нормативните спецификации за AIS подчертават реално-времевия характер на системата: AIS е автономен, самоорганизираща (без master), а тактическата информация трябва да се обменя непрекъснато (типично поне на 10 s, при някои маршрути до 2 s). За да се постигне подобна „жива“ картина в крайбрежни райони, решаваща е плътността на наземните приемници: всяка допълнителна антена/приемник точка не само разширява геометричното покритие, но и повишава вероятността за прием на слаби/частично закрити предавания.

Проблемът е, че повече приемници означава повече повторения на едни и същи AIS репорти, които „наводняват“ изхода към платформите. Точно тук федеративният облак има

системна стойност: той позволява плътна крайбрежна мрежа за прием в реално време, а едновременно с това извършва дедупликация и нормализация преди доставката към платформи.

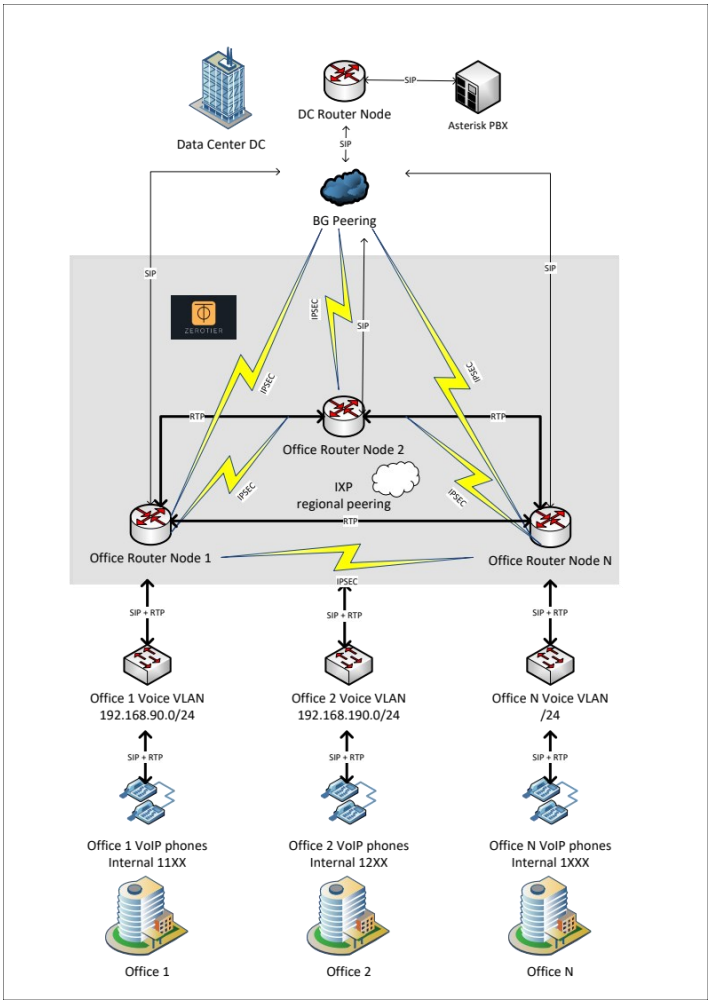
Междудомейн рутирането чрез BGP използва постоянно установени т.нар. peering сесии за обмен на маршрутна информация между автономни системи (RFC 4271). MPLS предлага логическа абстракция на пътя чрез етикети, полезна като метафора за „логически поток“ и класове трафик (RFC 3031). P2P DHT системи като Kademlia (Maymounkov et al., 2002) показват как децентрализирани възли откриват ресурси/пътища без централен контрол. В масовия целеви сценарий участниците в облака са малки оператори. Пътищата могат да се изменят динамично по различни причини от практиката, свързани с преконфигурирания от страната на интернет доставчика, временни прекъсвания и тн. Централната маршрутизация е анти-федерирана и често остарява; затова се предпочита търсене в локалния граф на свързаностите. Типичен алгоритъм е BFS по съседи с време на живот (TTL) спрямо лимит на скокове и с кеш на успешната следваща цел.

Разгледаните в предходните глави въпроси на асиметричната криптография, избора на по-леки и приложими схеми с елиптични криви, управлението на идентичности и защитата на транспортния канал са пряко релевантни и към федеративния AIS облак. Защитата само на транспортно ниво, например чрез тунелиране или криптиран канал между две точки, е необходима, но не е достатъчна в среда с множество автономни участници и с възможно преминаване на потока през повече от един възел. В подобна архитектура е необходимо произходът и целостта на данните да останат проверими и отвъд конкретния транспортен сегмент. Поради това защитата на приложно ниво може да се разглежда като естествено допълнение към транспортната защита: идентичността на участника се удостоверява чрез механизми на асиметрична криптография, а полезните данни и придружаващите ги метаданни могат да бъдат подписвани така, че да останат валидируеми по целия път на услугата. В този контекст по-леките схеми с елиптични криви са особено подходящи, тъй като позволяват практична защита в разпределена среда с ограничени ресурси. По аналогия с разгледания в предходната глава принцип за отделяне между съдържание и удостоверяване, и тук транспортът, идентичността и самите данни следва да се разглеждат като различни, макар и взаимосвързани слоеве на услугата.

## Глава 5. Оптимизация на прехода от управление на асети към управление на услуги

Пета глава е кулминацията на дисертационния труд и представя две практически валидирани направления за оптимизация на прехода от управление на асети към управление на услуги: хибридно VoIP решение за среда с регионални интернет доставчици и архитектура на федеративен AIS облак за предоставяне на навигационна телеметрия като услуга.

В първата част е изследван реален корпоративен сценарий с офиси във Варна и Балчик, при който са налице три основни проблема: недостатъчен капацитет спрямо съвременните нужди, липса на практика за предоставяне на разширени L2/L3 услуги и необичайно висока латентност дори между географски близки точки. Анализът показва, че при класическа централизирана VoIP архитектура медийният трафик би трябвало да преминава през централния PBX, което излишно удължава пътя на аудиото и увеличава риска от загуби и колебания в качеството.




Фиг 5.5. Архитектура на решението

Предложеното решение (Фиг. 5.5) е хибридна архитектура, при която Asterisk PBX в дейта център изпълнява само ролята на централен SIP сигнализационен сървър, а RTP аудио потоците се предават директно peer-to-peer между крайните точки чрез ZeroTier наслагваща свързаност и допълнителна IPsec защита.

Архитектурният смисъл на този избор е двоен: от една страна, централното управление на обажданията и правилата се запазва; от друга, самият полезен трафик следва най-краткия практически възможен маршрут между участниците.

Показано е как тази архитектура адресира и трите основни проблема. Тежкият аудио трафик не се концентрира в централната „звезда“, което разтоварва каналите към дейта центъра. Липсата на публични IP адреси се преодолява чрез динамична виртуална свързаност, която позволява изграждане на P2P канали и в NAT-ограничена среда. Най-съществения практически резултат е намаляването на латентността: вместо приблизително 25 ms при пренос през центъра е постигната латентност около 15 ms при директна медийна връзка между офисите.

Ефективността на решението е валидирана чрез анализ на сигнализационния и медийния трафик с Wireshark. Проследени са регистрацията на терминалите към Asterisk, SIP диалогът при установяване на повикване, договарянето на кодек и последващият директен RTP обмен между локалните мрежи на двата офиса. Тези наблюдения потвърждават, че централата управлява само сигнализацията, а гласовият поток се обменя директно, което е именно практическото проявление на прехода от управление на ресурс в центъра към предоставяне на услуга чрез координирано разпределена архитектура.

Досега разгледаните услуги в този дисертационен труд – видео стрийминга, GPU услугата при поискване, VoIP комуникацията в реално време и федеративният AIS облак представляват различни инженерни режими, но споделят обща архитектурна логика: разделение на функциите, контрол върху латентността, наблюдаемост и устойчивост при отпадане на компоненти. Затова дизайнът на федеративния AIS облак следва да заема доказани практики от стрийминг системите, реалновремевите комуникации и федеративните облачни модели, като ги адаптира към особеностите на навигационната телеметрия и на многодомейнната среда.

Втората част на главата разглежда федеративния AIS облак вече не само като концептуална архитектура, а като средство за оптимизация на предоставянето на телеметрия като услуга. Предложена е компактна формализация на ресурсния ефект при централизиран и федеративен модел.

| Означение | Смисъл |
|---|---|
| N | брой активни приемни възли |
| λu(N) | интензивност на полезния уникален поток от AIS събития |
| ddup(N) | среден коефициент на дублиране преди локална дедупликация |
| dres(N) | остатъчен коефициент на дублиране след локална или регионална дедупликация |
| κ | относително тегло на дедупликацията спрямо чистото приемане и пренос |
| Cnf(N) | нормализиран централен ресурс при нефедеративен модел |
| Cfed(N) | нормализиран централен ресурс при федеративен модел |
| G(N) | архитектурна полза от федеративния подход като отношение между двата ресурса |

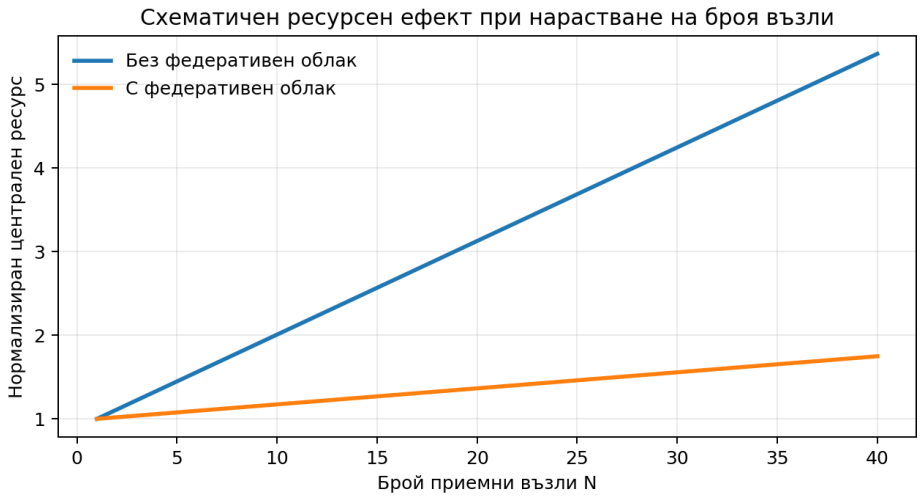
Таблица 5.1. Означения

Ако λu(N) обозначава полезния уникален поток от AIS събития, а ddup(N) – коефициента на дублиране, то при нефедеративен модел централният ресурс трябва да поеме суров поток $\lambda raw(N)=ddup(N)\cdot\lambda u(N)$. Нормализираният централен ресурс може да бъде записан като $Cnf(N)=ddup(N)+\kappa\cdot(ddup(N)-1)$, където вторият член изразява допълнителната тежест по дедупликация. При федеративен модел част от пречистването се извършва по-близо до източника и към по-горно ниво достига поток с остатъчен коефициент dres(N), така че $Cfed(N)=dres(N)+\kappa\cdot(dres(N)-1)$. Отношението $G(N)=Cnf(N)/Cfed(N)$ изразява архитектурната полза от изнасянето на част от обработката към по-ниските нива на федерацията.

Тази формализация не претендира за емпирично калибриран модел, а служи да покаже най-съществената зависимост: при силно припокриване на приемните зони суровият входящ поток към централен възел нараства по-бързо от полезния уникален поток. Следователно

централизираната система плаща цена не само за транспортирането на данните, но и за дедупликацията им. При федеративен модел значителна част от тази тежест се абсорбира по-ниско в архитектурата чрез локална дедупликация, нормализация и предварителна обработка.

Следователно архитектурната полза от федеративния подход нараства с увеличаване на броя на възлите и със степента на локално припокриване. Това показва, че при отсъствие на федеративен облак нарастването на броя приемни точки води до еквивалентно нарастване на необходимия централен ресурс, докато при федеративна организация част от това натоварване се абсорбира на по-ниско ниво чрез локална дедупликация и предварителна обработка. Фиг. 5.12 представя схематична зависимост между броя на приемните възли и необходимия централен ресурс при два режима: без федеративен облак и с федеративен облак. За илюстрация е прието, че коефициентът на дублиране преди локална дедупликация нараства по зависимост $d_{dup}(N)=1+0.07\cdot(N-1)$, а остатъчният коефициент след локална или регионална дедупликация — по зависимост $d_{res}(N)=1+0.012\cdot(N-1)$, при $\kappa=0.6$. Параметрите са илюстративни

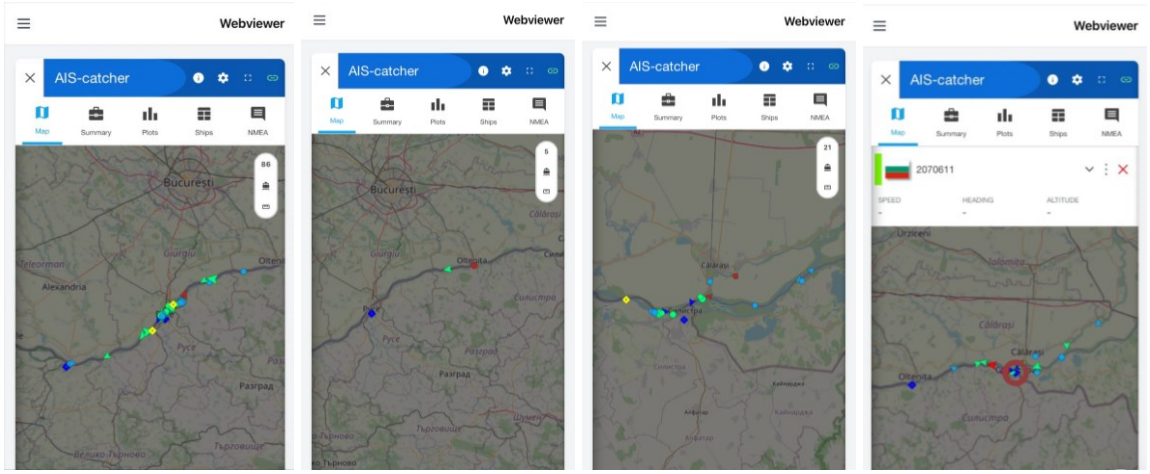



Фиг. 5.12. Схематичен ресурсен ефект при нарастване на броя възли

Практическият ефект е и организационен. Административният потребител не се интересува от това коя конкретна станция е приела дадено AIS съобщение, а от това да получи надеждна картина за конкретен оперативен участък. Поради това в дисертацията се предлага услугата да се дефинира не спрямо физическите активи, а спрямо искания резултат – например базов дедупликиран и географски ограничен поток за определен участък от

фарватера. Така приемането, пречистването, дедупликацията и пространственото ограничаване се превръщат в координирана услуга, а не в несвързани операции върху разпокъсани асети.

Особено показателен е дунавският пример Русе – Тутракан – Силистра, при който отделните приемни точки наблюдават частично припокриваща се AIS картина. При традиционен модел крайният потребител би получил смесен поток от различни станции и различни речни сегменти. При федеративния модел логическият ред на обработка е нормализация, времево подреждане, дедупликация, географско ограничаване и при нужда контекстно допълване с релевантни непозиционни съобщения. Така към крайния потребител достига не сурова инфраструктурна смес, а селектирана и оперативно значима услуга. Поради това при традиционен модел за подаване на данни според физическите активи крайният получател не получава „чист“ поток за търсения участък, а смес от съобщения, които се отнасят и до съседни речни сегменти (Фиг. 5.13).




Фиг. 5.13. Изследване на AIS приема в района на Русе, Тутракан, Айдемир и Силистра

Миксирането на потоците, дедупликацията и пространственото ограничаване се извършват във федеративната среда, близо до мястото на приемане, без операторът да поддържа тези функции локално. Осигурява се и проследимост на дейностите по приемане, транзит, дедупликация и доставка, без операторът на станцията да е натоварен с управление на тези компоненти.

Практическата релевантност на подобен подход се вижда и в европейските инициативи за интеграция на речни информационни услуги. EuRIS е реализирана като обща и централизирана точка за достъп, която събира данни от националните инфраструктури и предоставя услуги през уеб портал и програмни интерфейси, като суровите AIS данни постъпват към средата през защитена VPN свързаност (Zwicklhuber and Kaufmann, 2023). В този смисъл предложеният тук модел не отрича подобни решения, а ги надгражда, като измества акцента от централизирано събиране на инфраструктурни потоци към федеративно предоставяне на пречистена услуга според конкретен участък и конкретна административна потребност. Сходна посока се наблюдава и при DANRiSS и неговото планирано надграждане DANRISS 2, където се търси интегрирана платформа, избягване на дублирането между администрациите, използване на сензори, анализ на данни и решения с изкуствен интелект за усъвършенстван мониторинг и инспекции (Министерство на транспорта и съобщенията, 2018), (Министерство на регионалното развитие и благоустройството, 2026).

Пета глава показва, че оптимизацията на прехода от управление на асети към управление на услуги не се изчерпва с подмяна на една технология с друга. При VoIP тя се проявява като разделяне между централизирано управление и директен пренос на полезния трафик. При федеративния AIS облак тя се проявява като разделение между управляващ и информационен слой, периферно събиране, нормализация, дедупликация и предоставяне на телеметрия като услуга вместо като статично наследяване на отделни физически станции. В този смисъл главата завършва дисертационния труд с два практически валидирани модела на ориентиран към услугите трансформация при услуги с най-висока чувствителност към латентност, устойчивост и динамика на средата.

## РЕЗЮМЕ НА ПОЛУЧЕНИТЕ РЕЗУЛТАТИ

Получените резултати потвърждават основната теза на дисертационния труд, че оптимизацията на прехода от управление на асети към управление на услуги в сложни федерирани системи не се изчерпва с избор на единична технология, а изисква цялостен архитектурен подход. Такъв подход не омаловажава значението на инфраструктурата, а я поставя в правилния системен контекст.

В областта на сигурността е аргументирана необходимостта от преход към по-съвременни удостоверителни и защитни механизми. Анализът на зависимостта на RSA от качеството на ентропията показва, че надеждността на цифровите услуги зависи не само от самия алгоритъм, а и от реалната изчислителна среда. На тази основа е обоснована ECC като по-подходяща криптографска основа за съвременни разпределени и ресурсно ограничени среди, както и необходимостта от бъдещо развитие към post-quantum устойчивост.

В областта на мултимедийните услуги е показано, че защитата на съдържанието и защитата на личните данни могат да бъдат съчетани по-ефективно чрез разделяне между разпространението на съдържанието и удостоверяването на потребителите. По този начин се ограничава обработката на чувствителни данни от страна на видео дистрибутора и се повишава киберустойчивостта на услугата.

В областта на административните и изчислителните услуги е валидиран практически приложим модел за централизирано предоставяне на API/WebSocket-базирани и GPU-ускорени услуги за обработка на геопространствени данни, реализиран чрез междинен слой за достъп и известяване и чрез самостоятелния демон insightd. Това намалява нуждата от скъп локален хардуер, улеснява интеграцията и позволява по-ефективно използване на изчислителните асети в публичния сектор.

В областта на реалновремевата комуникация и телеметрия са показани два практически значими модела на ориентиран към услугите трансформация: хибридна VoIP архитектура с централизирана сигнализация и директен P2P пренос на медия; и федеративен AIS облак с разделение между управляващи и информационни функции, периферно събиране, нормализация, дедупликация и координирано предоставяне на данните. И в двата случая фокусът се измества от собствеността върху отделни ресурси към предоставянето на надеждна услуга с ясно определен резултат.

Общият извод е, че инфраструктурата е необходима основа, но реалната цифрова стойност възниква тогава, когато върху нея се изграждат координирани услуги. Следователно ориентиран към услугите и федеративният подход представляват не временна технологична мода, а логична следваща стъпка в развитието на цифровите системи в публичния сектор.

## ПРИНОСИ

Основните научни и научно-приложни приноси на дисертационния труд могат да бъдат обобщени, както следва:

1. **Разработен е общ модел за преход** от управление на асети към управление на услуги в сложни федерирани системи в публичния сектор. Моделът обединява цифрови, мрежови и изчислителни ресурси в интегрирани услуги с гарантирано качество. Това оптимизира надеждността и сигурността на процесите, като същевременно подобрява тяхната ефективност и организационна приложимост при управление на данни.
2. **Изборът на ECC (Elliptic Curve Cryptography) е аргументиран** като по-подходяща криптографска основа за разглежданите в дисертацията разпределени услуги с ограничени ресурси. Това е постигнато чрез детайлен анализ на дефицитите на RSA при ниска ентропия и формулиране на практически насоки за повишаване на криптографската устойчивост. При ECC нуждите от ентропия за генериране на сигурен ключ са значително по-ниски спрямо RSA (поради по-малкия размер на ключа за същото ниво на сигурност), което е критично за IoT устройства и „edge“ услуги, където източниците на истинска случайност често са ограничени.
3. **Разработени са методи за сигурно предоставяне** на мултимедийни услуги чрез разделяне на процесите по разпространение на съдържанието от удостоверяването на потребителите. Този подход ограничава обработката на лични данни от дистрибутора, осигурява регламентирана редистрибуция и повишава киберустойчивостта на услугата.
4. **Разработена е архитектура за предоставяне на административни** и изчислителни услуги при поискване (on-demand). Тя включва API-базиран достъп до обработка на геопространствени данни и специализиран демон insightd за централизирано GPU-ускорено изчисляване. Този подход минимизира зависимостта от скъп локален хардуер и значително улеснява интеграцията с външни системи. Използването на GPU-ускорена обработка чрез специализиран демон е ключово предимство в контекста на геопространствените данни (GIS). Комбинацията от API достъп и GPU демон архитектурно разделя интерфейса за управление от тежките изчисления. Поради високите изисквания за паралелизация при масиви от пространствени данни, централизираните структури предлагат значително по-висока ефективност и изчислителна мощ в сравнение с капацитета на стандартните локални работни станции.

5. **Разработена е хибридна VoIP архитектура** за комуникационни услуги в среди с инфраструктурни ограничения. Моделът съчетава централизирана SIP сигнализация с директен пренос на медийния трафик, което минимизира латентността и елиминира негативното влияние на техническите ограничения при регионалните доставчици. Това помага за заобикаляне на проблеми с NAT траверс или ограничаване на честотната лента от страна на доставчиците.
6. **Предложена е архитектура на федеративен AIS облак** за предоставяне на навигационна телеметрия като услуга. Тя се базира на стриктно разделение между управляващите и информационните функции и въвежда специализирани роли за обработка на потоци от данни. Интегрирани са механизми за дедупликация, пречистване и нормализация, които гарантират координираното предоставяне на надеждни телеметрични услуги. Федеративният облак може да обединява данни от различни източници, без да ги централизира принудително. Модулът за нормализация и дедупликация ефективно филтрира „шума“, породен от дублирането на телеметрични пакети в гъсти сензорни мрежи. Това позволява изграждането на единна, консистентна картина на трафика в реално време.

По този начин формулираните приноси очертават цялостен модел за оптимизиране на прехода от управление на асети към управление на услуги в сложни федерирани системи в публичния сектор.

## БЪДЕЩИ ИЗСЛЕДВАНИЯ

Получените резултати в дисертационния труд очертават редица възможности за бъдещо развитие и разширяване на предложените модели и архитектурни решения.

На първо място, логично продължение представлява развитието на федеративния AIS облак чрез усъвършенстване на механизмите за агрегиране, обработка и защитен транспорт на телеметрични потоци. В тази посока могат да бъдат изследвани подходи за следване на маршрутизиращи политики според NMEA v4 Tag Blocks, както и схеми за криптиране на транспорта през несигурни мрежи. Практическа основа за такова развитие е платформата AISMixer, предназначена за смесване на сигнали от един район в общ поток.

На второ място, перспективна посока е разширяването на модела към периферна обработка на данни чрез интегриране на леки алгоритми за локален анализ в общински и регионални възли. Подобен подход би позволил част от обработката да се извършва по-близо до източника на данни, което може да намали латентността, да ограничи натоварването на централната инфраструктура и да създаде предпоставки за по-проактивни цифрови услуги.

Четвърта възможност е свързана с усъвършенстване на механизмите за доверие, проследимост и междуорганизационно взаимодействие в среди с множество автономни участници. В този контекст могат да се изследват средства за регистриране на събития, проследяване на жизнения цикъл на данните и автоматизирано отчитане на качеството на предоставяните услуги, включително при договорени параметри на обслужване.

Перспективна насока за бъдещи изследвания е въвеждането на edge AI във федеративния AIS облак. Това би позволило част от анализа да се извършва още в периферните възли чрез ранно откриване на аномалии, предварителна оценка на риск и отделяне на значими събития. Подобен подход е в синхрон и с актуални инициативи по Дунав, включително DANRISS 2, където вече се търси съчетаване на изкуствен интелект, сензори и интеграция на данни.

Посочените направления не променят основната рамка на дисертационния труд, а представляват нейно естествено разширяване към по-висока степен на автономност, сигурност, мащабируемост и интелигентност на услугите в сложни федерирани системи.

## ПУБЛИКАЦИИ ПО ТЕМАТА НА ДИСЕРТАЦИЯТА


1. **I. Iliev,** I. Blagoev and Y. Terziev, "Hybrid VoIP Solution to Address Regional ISP Challenges," 2025 6th International Conference on Communications, Information, Electronic and Energy Systems (CIEES), Ruse, Bulgaria, 2025, pp. 1-6, doi: 10.1109/CIEES66347.2025.11300241.
2. **Iliev, Il.,** Blagoev I., Centralized Parallel Computing as a Cloud Service for Solving Digital Transformation Problems in Smart Cities. 2023 4th International Conference on Communications, Information, Electronic and Energy Systems (CIEES), IEEE, 2023, DOI:10.1109/CIEES58940.2023.10378756, 1-1-4-4

3. **Iliev, I.**, **Blagoev, I.**, An Approach to Improve Web Video Streaming Security and Prevent Personal Data Leakage. Information & Security: An International Journal, 53, 1, Procon, 2022, ISSN:1314-2119, DOI:10.11610/isij.5306, 78-88
4. Blagoev, I., Balabanov, T., **Iliev,** I. RSA Weaknesses Caused by the Specifics of Random Number Generation. Information & Security: An International Journal, 50, 2, Procon Ltd., 2021, ISSN:0861-5160, DOI:10.11610/isij.5028, 171-179, 2021
5. Blagoev, I., Balabanov, T**., Iliev,** I. The Randomness in Shared Web Hostings. Extended Abstracts of 16th Annual Meeting of the Bulgarian Section of SIAM, Fastumprint, 2021, ISSN:1313-3357, 9-10
6. Iliev, I., Blagoev, I. Security Considerations and Techniques for Video Streaming Distribution in Home ISPs (International Conference on Electronics, Engineering Physics and Earth Science (EEPES 2026) which will be held on 24th-27th June, 2026 in Bandirma, Turkey).

## УЧАСТИЕ В ПРОЕКТИ

Национална научна програма „Сигурност и отбрана“ (ННП СО).

## ЗАБЕЛЯЗАНИ ЦИТИРАНИЯ

Iliev, I., Blagoev, I., An Approach to Improve Web Video Streaming Security and Prevent Personal Data Leakage. Information & Security: An International Journal, 53(1), Procon, 2022, DOI: 10.11610/isij.5306. 78-88

Цитира се в:

1. Daniela Borissova, Milena Bankovska, Katia Rasheva-Yordanova, Zornitsa Dimitrova, Multicriteria Model for Evaluation of Learning Management Systems, WSEAS Transactions on Business and Economics, 2025, DOI: 10.37394/23207.2025.22.101.
2. Yinka Akintunde Fagbile, Nollywood, Film Streaming, and Ethical Practices, Integral Research, Vol. 02, No. 03, 2025.

## БИБЛИОГРАФИЯ


1. Julian Jang-Jaccard and Surya Nepal, “A survey of emerging threats in cybersecurity,” Journal of Computer and System Sciences 80, no. 5 (2014): 973-993.
2. Georgi Kostadinov and Tatiana Atanasova, “Security Policies for Wireless and Network Infrastructure,” Problems of Engineering Cybernetics and Robotics 71 (2019): 14-19.
3. Kristina Dineva and Tatiana Atanasova, “Regression Analysis on Data Received from Modular IoT System,” 33rd Annual European Simulation and Modelling Conference ESM’2019, Palma de Mallorca, Spain, December 2019.
4. Velizar Shalamanov, Vladimir Monov, Ivaylo Blagoev, Silvia Matern, Gergana Vassileva, and Ivan Blagoev, “A Model of ICT Competence Development for Digital Transformation,” Information & Security: An International Journal 46 (2020): 269-284, https://doi.org/10.11610/isij.4619.
5. David F. DiCarlo, “Random Number Generation: Types and Techniques,” Theses (Liberty University, Center for Computer and Information Technology, 2012).
6. James Carr, “Simple Random Number Generation,” Computers & Geosciences 29, no. 10 (2003): 1269-1275, https://doi.org/10.1016/j.cageo.2003.07.002.
7. Pierre L’Ecuyer, “Random Number Generation,” in Handbook of Simulation: Principles, Methodology, Advances, Applications, and Practice, edited by James E. Gentle, Wolfgang Karl Härdle, and Yuichi Mori (Berlin, Heidelberg: Springer, 2007), https://doi.org/10.1007/978-3-642-21551-3_3.
8. Andrew Jin, David Ling, and Alwyn Goh, “Biohashing: Two factor authentication featuring fingerprint data and tokenised random number,” Pattern Recognition 37 (2004): 2245-2255.
9. Carmen Camara, Honorio Martín, Pedro Peris-Lopez, and Muawya Aldalaien, “Design and Analysis of a True Random Number Generator Based on GSR Signals for Body Sensor Networks,” Sensors 19, no. 9 (2019): 2033, https://doi.org/10.3390/s19092033.
10. Salih Ergün, “Security analysis of a chaos-based random number generator for applications in cryptography,” 15th International Symposium on Communications and Information Technologies (ISCIT), Nara, Japan, 2015, 319-322, https://doi.org/10.1109/ISCIT.2015.7458371.
11. Boris Ryabko, Jaakko Astola, and Mikhail Malyutov, Compression-Based Methods of Statistical Analysis and Prediction of Time Series (Cham, Switzerland: Springer International Publishing, 2016).
12. D. J. Bernstein, Y.-A. Chang, C.-M. Cheng, L.-P. Chou, N. Heninger, T. Lange, and N. van Someren, “Factoring RSA Keys from Certified Smart Cards: Coppersmith in the Wild,” in Advances in Cryptology – ASIACRYPT 2013 (Proceedings, Part II), K. Sako and P. Sarkar, eds., Lecture Notes in Computer Science, vol. 8270, Bengaluru, India, Dec. 1–5, 2013, pp. 341–360. Springer, Berlin, Heidelberg, 2013, doi: 10.1007/978-3-642-42045-0_18.

13. Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J. Alex Halderman, “Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices,” 21st USENIX Security Symposium, Bellevue, WA, Aug. 8–10, 2012, pp. 205-220.
14. V. Shoup, “Lower Bounds for Discrete Logarithms and Related Problems,” in Advances in Cryptology — EUROCRYPT ’97, W. Fumy, ed., Lecture Notes in Computer Science, vol. 1233, pp. 256–266, Springer, 1997, doi: 10.1007/3-540-69053-0_18.
15. Kessler, Gary C. “Protected AIS: A Demonstration of Capability Scheme to Provide Authentication and Message Integrity.” TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation (2020).
16. Synopi. “RTMP streaming process diagram.” Достъпно на: https://synopi.com/.
17. SSL.com Support Team. “SSL/TLS Best Practices for 2023.” Достъпно на: https://www.ssl.com/guide/ssl-best-practices/.
18. John Paul Mueller, Security for Web Developers: Using JavaScript, HTML, and CSS, 2015, ISBN-13:978-1491928646.
19. M.A. Erskine, D.G. Gregg, J. Karimi, and J.E. Scott, “Business Decision-Making Using Geospatial Data: A Research Framework and Literature Review,” Axioms 3 (2014): 10-30, https://doi.org/10.3390/axioms3010010.
20. R. Wickramasuriya, J. Ma, M. Berryman, and P. Perez, “Using geospatial business intelligence to support regional infrastructure governance,” Knowledge-Based Systems 53 (2013): 80-89, https://doi.org/10.1016/j.knosys.2013.08.024.
21. S. Rivest, Y. Bédard, M.-J. Proulx, M. Nadeau, F. Hubert, and J. Pastor, “SOLAP technology: Merging business intelligence with geospatial technology for interactive spatio-temporal exploration and analysis of data,” ISPRS Journal of Photogrammetry and Remote Sensing 60, no. 1 (2005): 17-33, https://doi.org/10.1016/j.isprsjprs.2005.10.002.
22. J. de Castro Lima, Computing Data Cubes Over GPU Clusters, Monografia, Federal University of Ouro Preto, Institute of Exact Sciences and Biology, Undergraduate Program in Computer Science, December 2018. Достъпно на: https://www.monografias.ufop.br/bitstream/35400000/1527/6/MONOGRAFIA_ComputingDataCubes.pdf
23. Yakov Rekhter, Susan Hares, and Tony Li, “A Border Gateway Protocol 4 (BGP-4),” RFC 4271, January 2006, doi:10.17487/RFC4271.
24. Arun Viswanathan, Eric C. Rosen, and Ross Callon, “Multiprotocol Label Switching Architecture,” RFC 3031, January 2001, doi:10.17487/RFC3031.

25. Petar Maymounkov and David Mazières, “Kademlia: A Peer-to-Peer Information System Based on the XOR Metric,” in Revised Papers from the First International Workshop on Peer-to-Peer Systems (IPTPS ’01), Springer-Verlag, Berlin, Heidelberg, 2002, pp. 53–65.
26. Zwicklhuber, T., and M. Kaufmann, “EURIS (European River Information Services System) – The Central European RIS Platform: Introducing a Joint RIS System Among 13 European Countries,” in Li, Y., Hu, Y., Rigo, P., Lefler, F. E., and Zhao, G., eds., Proceedings of PIANC Smart Rivers 2022, Lecture Notes in Civil Engineering, vol. 264, Springer, Singapore, 2023, pp. 850–856, doi:10.1007/978-981-19-6138-0_75.
27. Министерство на транспорта и съобщенията. „Bulgaria and Romania with a common regime for ships inspections on the Danube.“ 22.02.2018. Достъпно на: https://www.mtc.government.bg/en/category/1/bulgaria-and-romania-common-regime-ships-inspections-danube
28. Министерство на регионалното развитие и благоустройството. „Модерна система ще следи за замърсяване на Дунав от кораби.“ 23.03.2026. Достъпно на: https://www.mrrb.bg/bg/moderna-sistema-ste-sledi-za-zamursyavane-na-dunav-ot-korabi/.