VIDEO DATA PROTECTION IN DIGITAL AND INTELLIGENT VIDEO SURVEILLANCE SYSTEMS: TECHNICAL RISKS AND MEASURES*

DEYAN P. IVANOV, DONIKA V. DIMANOVA

ABSTRACT: *Modern digital and intelligent video surveillance systems process significant volumes of video data and increasingly rely on network connectivity, cloud services, and algorithms for automated analysis. These capabilities enhance the effectiveness of surveillance, but at the same time create additional risks to the confidentiality, integrity, and control of personal data. This paper examines the main technical risks arising throughout the lifecycle of video data, including their collection, transmission, storage, processing, and access. Key security measures are analyzed, including encryption, access control, authentication, logging, and monitoring, as well as the specific characteristics of local and cloud storage. Particular attention is also given to intelligent video surveillance systems that use artificial intelligence and automated video analysis, which expand data-processing capabilities but require a higher level of personal data protection. On this basis, technical guidelines are formulated to mitigate risks and enhance the security of video data.*

KEYWORDS: *video data, video surveillance, information security, encryption, access control, cloud storage, artificial intelligence, personal data protection*

DOI: https://doi.org/10.46687/MT26DPI

ЗАЩИТА НА ВИДЕОДАННИТЕ В ЦИФРОВИ И ИНТЕЛИГЕНТНИ СИСТЕМИ ЗА ВИДЕОНАБЛЮДЕНИЕ: ТЕХНИЧЕСКИ РИСКОВЕ И МЕРКИ

ДЕЯН П. ИВАНОВ, ДОНИКА В. ДИМАНОВА

АБСТРАКТ: *Съвременните цифрови и интелигентни системи за видеонаблюдение обработват значителни обеми видеоданни и все по-често използват мрежова свързаност, облачни услуги и алгоритми за автоматизиран анализ. Тези възможности повишават ефективността на наблюдението, но едновременно с това създават допълнителни рискове за конфиденциалността, целостта и контрола върху личните данни. Настоящият доклад разглежда основните технически рискове, възникващи в жизнения цикъл на видеоданните – при тяхното събиране, предаване, съхранение, обработка и достъп. Анализирани са основни мерки за защита, включително криптиране, контрол на достъпа, автентикация, логване и мониторинг, както и особеностите при локално и облачно съхранение. Отделено е внимание и на интелигентните системи за видеонаблюдение, използващи изкуствен интелект и автоматизиран видеоанализ, които разширяват възможностите за обработка, но изискват по-високо ниво на защита на личната информация. На тази основа са формулирани технически насоки за ограничаване на риска и повишаване на сигурността на видеоданните.*

1 Въведение

Развитието на цифровите и IP базираните системи за видеонаблюдение значително променя начина, по който се събират, предават, съхраняват и анализират видеоданни. За разлика от традиционните аналогови решения, съвременните системи използват мрежова инфраструктура, цифрови видеорекордери, облачни платформи и софтуер за автоматизиран

* Докладът е частично финансиран по проект РД-08-94/03.02.2026 г. „Експериментална и изследователска среда за моделиране, анализ и оптимизация на производствени процеси и технологии“

анализ, което създава възможности за по-висока резолюция, дистанционен достъп, мащабируемост и интеграция с други системи за сигурност.

Технологичното развитие обаче увеличава и броя на потенциалните точки на уязвимост. IP камерите функционират като мрежови устройства и могат да бъдат изложени на неоторизиран достъп, неправилна конфигурация, прихващане на видеопотока или компрометиране на съхраняваните записи. Използването на облачна инфраструктура и дистанционен достъп допълнително разширява средата, в която трябва да бъде гарантирана защитата на видеоданните. Сигурността на интелигентните структури в Интернет на нещата е разгледана в [2]. Съвременните киберзаплахи са разгледани в [9], а оценяването на уязвимостите на безжични мрежи в [17].

Особено значение има разглеждането на видеоданните през целия им жизнен цикъл. Сигурността трябва да бъде осигурена още при събирането на информацията, да се поддържа по време на нейното предаване и съхранение и да включва подходящ контрол при последващ достъп, обработка, анализ и изтриване. В този контекст защитата на видеоданните не може да се ограничи до използването на единична техническа мярка, а изисква съчетаване на криптографски механизми, контрол на достъпа, автентикация, проследимост и мониторинг [1, 3].

Криптирането е основна мярка за защита както на данните в транзит, така и на съхраняваните видеозаписи. При мрежово предаване могат да се използват защитени комуникационни протоколи, а при съхранение – криптографски алгоритми, които ограничават възможността за използване на информацията при неоторизиран физически или логически достъп.

Друг съществен компонент е управлението на достъпа. Потребителските профили, диференцираните права, многофакторната автентикация и принципът на най-малките привилегии създават условия различните категории потребители да имат достъп единствено до необходимите им функции и видеоданни. Системното логване на входове, прегледи, експортиране и промени в конфигурацията допълва тази защита чрез осигуряване на проследимост и възможност за последващ анализ на действията [4].

С навлизането на изкуствения интелект и машинното обучение видеонаблюдението все по-често включва автоматично разпознаване на обекти и лица, поведенчески анализ, откриване на аномалии и обработка на информация в реално време. Тези технологии могат да подобрят ефективността на системите, но разширяват и обема и характера на извличаната информация, което увеличава необходимостта от контрол върху начина, по който данните се обработват, комбинират и използват [7].

Целта на настоящия доклад е да се анализират основните технически рискове за видеоданните в цифрови и интелигентни системи за видеонаблюдение и да се систематизират подходящи мерки за тяхното ограничаване.

За постигането на тази цел са използвани методите на анализ, сравнение и систематизация на технически и нормативни източници, като вниманието е насочено към жизнения цикъл на видеоданните и към основните механизми за осигуряване на конфиденциалност, целостност, контрол на достъпа и проследимост.

2 Жизнен цикъл на видеоданните и рискове за сигурността

Защитата на видеоданните следва да се разглежда през целия им жизнен цикъл, тъй като рисковете възникват още при събирането на информацията и продължават при нейното предаване, съхранение, обработка, достъп и изтриване. При цифровите и IP базираните

системи отделните етапи са технологично свързани и компрометирането на един от тях може да повлияе върху сигурността на целия информационен поток.

2.1. Събиране на видеоданни

Началният етап е свързан с определяне на обхвата на наблюдението и конфигуриране на камерите. Параметри като резолюция, честота на кадрите, ъгъл на видимост, чувствителност към движение и наблюдавани зони влияят пряко върху количеството и характера на събираната информация. Неправилната конфигурация може да доведе до заснемане на нерелевантни пространства, прекомерно събиране на данни или неоторизиран достъп до видеопотока.

2.2. Предаване на видеоданни

При IP базираните системи видеоданните се предават през локални или външни мрежи. Това създава рискове от прихващане, подмяна или неоторизиран достъп, особено при дистанционно управление, облачни услуги и комуникация през публични мрежи. Поради това защитата на комуникационния канал представлява ключов елемент от сигурността на видеоданните.

2.3. Съхранение на видеозаписи

Съхранението може да бъде локално, облачно или хибридно. Всеки от тези модели създава различен профил на риск, свързан с физическа загуба или повреда, неоторизиран достъп, зависимост от външен доставчик, ограничен капацитет или прекомерно дълго съхранение на информацията. Изборът на модел следва да бъде съобразен както с техническите характеристики на системата, така и с изискванията за защита на данните.

2.4. Обработка и анализ

Съвременните системи все по-често използват автоматизиран видеоанализ, машинно обучение и изкуствен интелект за разпознаване на лица и обекти, регистрационни номера и поведенчески модели. Тези технологии повишават аналитичните възможности, но разширяват и обема на извличаната информация и могат да създадат риск от прекомерна обработка, профилиране или използване на данните извън първоначално определената цел.

2.5. Достъп до видеоданните

Достъпът до видеопотока, архивите и системната конфигурация представлява критична точка от жизнения цикъл. Недостатъчно разграничените потребителски права, общите профили и слабите механизми за удостоверяване могат да доведат до неоторизирано преглеждане, копиране, промяна или изтриване на записи.

2.6. Мониторинг и изтриване

Последният етап включва проследяване на действията в системата и контролирано приключване на жизнения цикъл на данните. Липсата на достатъчна проследимост затруднява установяването на неправомерни действия, а ненужно продължителното съхранение увеличава обема на информацията, която може да бъде засегната при пробив в сигурността.

В обобщение, жизненият цикъл на видеоданните включва взаимосвързани етапи с различни характеристики и рискове. Ефективната защита изисква тези рискове да бъдат оценявани комплексно, а конкретните технически мерки за тяхното ограничаване да бъдат прилагани последователно при предаването, съхранението, достъпа и обработката на информацията.

3 Криптиране и сигурно съхранение

Криптирането е основен технически механизъм за защита на видеоданните както при тяхното предаване, така и при съхранение. При цифровите и IP базираните системи видеопотокът често преминава през локални мрежи, интернет връзки или облачни услуги, което създава риск от прихващане, неоторизиран достъп или компрометиране на съдържанието. Поради това защитата на видеоданните следва да включва едновременно криптиране на комуникационния канал и на съхраняваните записи [1, 3].

3.1. Криптиране на данни при предаване

При предаване на видеоданни през мрежа е необходимо използването на защитени комуникационни протоколи, които ограничават възможността за прихващане на информацията. Като подходящи решения могат да се използват HTTPS/TLS за защита на преноса и AES за защита на съхраняваните видеоданни. В някои комерсиални решения се прилагат HTTPS/TLS за защита на предаването и AES за криптиране на съхраняваните видеоданни [6].

Използването на криптиран транспорт е особено важно при дистанционен достъп и при системи, които изпращат видеопоток към външни или облачни инфраструктури. В такива случаи липсата на защита на комуникационния канал може да създаде предпоставки за прихващане на видеоданни или компрометиране на сесиите. Забавянето при криптиране и декриптиране на глас през VPN мрежа е разгледано в [8] като отделен пример за влиянието на защитата върху комуникацията.

Защитата при пренос следва да бъде разглеждана и във връзка с удостоверяването на участващите устройства и потребители. Криптираната връзка ограничава риска от неоторизирано наблюдение на трафика, но не може да замести необходимостта от надежден контрол на достъпа и правилна конфигурация на крайните устройства.

3.2. Криптиране на съхраняваните видеоданни

Криптирането на съхраняваните видеозаписи е необходимо за ограничаване на риска при физически или логически достъп до устройствата за съхранение. Това е особено важно при DVR/NVR системи, NAS устройства и облачни платформи, където значителни обеми видеоданни могат да бъдат концентрирани в едно хранилище.

Сред приложимите алгоритми за защита на съхраняваните видеоданни са AES-128 и AES-256, като TLS може да се използва за защита на преноса. Този подход позволява защитата да бъде разпределена между различните етапи на жизнения цикъл на информацията.

При локално съхранение криптирането намалява риска от неоторизирано използване на записите при кражба или физически достъп до носителя.

3.3. Локално, облачно и хибридно съхранение

Локалното съхранение чрез DVR/NVR, твърди дискове или NAS осигурява висока степен на контрол върху данните и позволява работа независимо от постоянна интернет връзка. Неговите основни рискове са свързани с физическа повреда, кражба, ограничен капацитет и необходимост от собствена поддръжка.

Облачните платформи за видеонаблюдение предоставят възможности за централизирано управление, дистанционен достъп и мащабируемо съхранение, като конкретните механизми за защита зависят от архитектурата и услугите на съответния доставчик [5].

Хибридният модел комбинира локално и облачно съхранение и може да предостави по-гъвкав баланс между контрол, достъпност и резервираност. Независимо от избрания

модел, ефективната защита изисква ясно определени правила за достъп, криптиране, резервиране и срокове за съхранение.

3.4. Срокове за съхранение и сигурно изтриване

Сигурното съхранение не се ограничава до защита на данните по време на тяхното използване. Необходимо е да бъде определен и ясен жизнен цикъл на записите, включително моментът на тяхното изтриване.

Продължителното съхранение на видеоматериали без конкретна необходимост увеличава както техническия риск, така и обема на информацията, която може да бъде засегната при евентуален пробив. Поради това системите следва да поддържат автоматизирани механизми за изтриване след изтичане на предварително определен срок, както и възможност за документиране на тези действия [1, 3].

Когато определени записи трябва да бъдат запазени за по-дълъг период поради конкретен инцидент или друга обоснована необходимост, те следва да бъдат отделени от текущия архив и защитени чрез същите или по-високи механизми за криптиране и контрол на достъпа.

В обобщение, сигурното съхранение на видеоданни изисква съчетаване на криптиране при пренос и съхранение, подходящ избор между локален, облачен или хибриден модел, ясно определени срокове за съхранение и контролирано изтриване. Тези мерки ограничават риска от неоторизиран достъп и подпомагат защитата на данните през целия им жизнен цикъл.

4 Контрол на достъпа и отчетност

Контролът на достъпа е основен елемент от защитата на видеоданните, тъй като ограничава възможността за преглед, обработка, експортиране или промяна на записи само до упълномощени лица. При цифровите и IP базираните системи тази защита следва да обхваща както потребителите, така и устройствата, чрез които се осъществява достъп до системата.

4.1. Автентикация и оторизация

Автентикацията е първият етап от контрола на достъпа и има за цел да установи самоличността на потребителя или устройството. Използването само на потребителско име и парола създава ограничена степен на защита, особено при слаби или повторно използвани пароли. Поради това при системи с повишен риск е препоръчително използването на многофакторна автентикация (MFA), при която достъпът се потвърждава чрез повече от един независим фактор.

След успешна автентикация се прилага авторизация, чрез която се определят конкретните действия, които даден потребител може да извършва. Един от широко използваните подходи е ролевото управление на достъпа (Role-Based Access Control – RBAC), при което правата се предоставят в зависимост от служебната роля. Така например операторът може да има право само да наблюдава видеопотока и архивните записи, докато административните функции за конфигуриране, изтриване или промяна на системните настройки остават ограничени до определени потребители.

Подобен подход съответства на принципа на най-малките привилегии, според който всеки потребител следва да разполага само с правата, необходими за изпълнение на конкретните му функции. При по-сложни системи може да се използва и Attribute-Based Access Control (ABAC), при който правата зависят допълнително от характеристики като време, местоположение или тип устройство.

4.2. Разграничаване на потребителските права

Диференцирането на потребителските права е особено важно при видеонаблюдение, тъй като различните действия върху записите имат различна степен на чувствителност. Прегледът на живо, достъпът до архив, експортирането на видеоматериал, промяната на конфигурацията и изтриването на записи не следва автоматично да бъдат достъпни за всички потребители.

За ограничаване на риска е необходимо да бъдат създадени ясно разграничени роли и права, които се администрират централизирано. При интеграция с корпоративни среди могат да бъдат използвани директории като LDAP или Active Directory, което позволява съгласуване на достъпа до видеосистемата с общите политики за сигурност на организацията.

Периодичният преглед на потребителските профили също има важно значение. Неактивни или вече ненужни акаунти следва да бъдат деактивирани, а предоставените права да се актуализират при промяна на длъжността или отговорностите на потребителя.

4.3. Логване и проследимост

Контролът на достъпа трябва да бъде допълнен от механизми за регистриране и проследяване на действията в системата. Логовете позволяват да се установи кой потребител е получил достъп, кога е осъществено това, какви действия са предприети и дали са извършени промени в конфигурацията или видеозаписите.

Сред съществените събития, които следва да бъдат регистрирани, са успешни и неуспешни опити за вход, промени на настройки, преглед и експортиране на записи, изтриване на данни и други действия с повишена чувствителност. Подобна проследимост подпомага както своевременното откриване на подозрителна активност, така и последващия анализ при възникване на инцидент [4].

Централизираното събиране и анализ на логове може допълнително да подобри защитата чрез автоматично откриване на нетипично поведение, множество неуспешни опити за достъп или необичайно изтегляне на записи. Това позволява системата да изпълнява не само доказателствена, но и превантивна функция. Наблюдението на комуникационни мрежи с Wireshark е разгледано в [11], а компютърната сигурност и управлението на трафика в [13].

4.4. Отчетност и възможност за одит

Отчетността предполага организацията да може да докаже не само наличието на технически мерки, но и тяхното реално прилагане. В този смисъл логовете, регистрите за достъп, вътрешните правила и разпределението на потребителските права представляват важна част от доказуемата проследимост на операциите.

Периодичните проверки на потребителските права и на регистрираните действия позволяват да бъдат идентифицирани несъответствия, прекомерно предоставени права или неправомерни действия. Този подход подпомага вътрешния одит и създава условия за своевременно коригиране на установени слабости. За обработка и анализ на таблични отчети е относимо разгледаното приложение на динамични масиви в MS Excel [16].

Отчетността е особено важна при системи, в които се обработват чувствителни видеоданни или се използват функции за биометрично разпознаване и автоматизиран анализ. В такива случаи възможността да се проследи всяко действие върху данните е съществен елемент от защитата и от управлението на риска [1, 3].

В обобщение, ефективният контрол на достъпа изисква съчетаване на надеждна автентикация, ясно разграничени права, принцип на най-малките привилегии, системно логване и периодичен одит. Тези механизми не само ограничават риска от неоторизиран достъп, но и осигуряват необходимата проследимост и отчетност при управлението на видеоданните.

5 Интелигентен видеоанализ и възникващи рискове за неприкосновеността на личния живот

Интегрирането на изкуствен интелект и машинно обучение в системите за видеонаблюдение значително разширява възможностите за автоматизирана обработка на видеоданни. Съвременните решения могат да извършват разпознаване и класифициране на обекти, лицево разпознаване, идентифициране на регистрационни номера, проследяване на движение и анализ на поведенчески модели. По този начин видеонаблюдението постепенно преминава от пасивно записване към автоматизирано извличане и интерпретация на информация. Развитието на изкуствения интелект и приложенията му в съвременния свят са разгледани в [10].

5.1. Автоматизиран видеоанализ

Интелигентният видеоанализ позволява обработването на значителни обеми видеоданни в реално време и автоматичното откриване на събития, които биха изисквали продължително наблюдение от оператор. Сред основните приложения са детекция на движение, проследяване на обекти, разпознаване на лица и превозни средства, поведенчески анализ и идентифициране на нетипични ситуации.

Използването на подобни технологии създава възможности за по-бърза реакция при инциденти и за автоматизирано филтриране на значими събития. В същото време обаче количеството информация, която може да бъде извлечена от един видеозапис, се увеличава. Данните вече не се ограничават само до визуално изображение, а могат да бъдат преобразувани в структурирана информация за идентичност, движение, поведение или присъствие в определено пространство.

5.2. Разпознаване на лица и биометрична обработка

Особено чувствителна област е използването на лицево разпознаване за уникална идентификация на физически лица, тъй като в този случай се обработват биометрични данни и възниква повишен риск за правата и свободите на наблюдаваните лица [1, 3].

От техническа гледна точка системите за биометрично разпознаване изискват особено строг контрол върху достъпа до шаблоните и резултатите от анализа, както и върху начина, по който тези данни се съхраняват, комбинират и впоследствие използват. Когато резултатите се използват за автоматизирано вземане на решения, е относимо разгледаното третиране на тези решения според GDPR [15].

5.3. Профилиране и анализ на поведението

Поведенческият анализ позволява системите да идентифицират модели като продължителен престой, движение в определена посока, струпване на хора или отклонения от предварително зададено поведение. Подобни функции могат да подпомогнат сигурността, но създават риск видеоданните да бъдат използвани за по-широко профилиране от първоначално определената цел на наблюдението.

Този риск нараства при комбиниране на видеоданни с други информационни източници или при автоматично създаване на поведенчески характеристики. Затова интелигентният анализ следва да бъде ограничен до ясно дефинирани функции и до

информацията, действително необходима за конкретната цел. Принципите за минимизация и ограничение на целите остават приложими независимо от технологичната сложност на системата [1, 3].

5.4. Облачна и периферна обработка с изкуствен интелект

Интелигентният анализ може да бъде осъществяван както централизирано, така и на периферните устройства. При облачните решения видеоданните или резултатите от анализа се предават към външна инфраструктура, което създава допълнителни изисквания към защитата при трансфер, контрола на достъпа и съхранението.

Edge AI решенията позволяват част от обработката да се извършва непосредствено в камерата или в периферно устройство. Това може да намали необходимостта от постоянно предаване на целия видеопоток към централен сървър и да ускори реакцията на системата. И двата подхода намират приложение в съвременните интелигентни системи за видеонаблюдение.

Независимо от архитектурата, защитата следва да обхваща както първичния видеопоток, така и вторично генерираните данни – метаданни, идентификационни резултати, класификации и алармени събития.

5.5. Възникващи рискове за неприкосновеността на личния живот

Автоматизираният анализ увеличава не само функционалността, но и потенциалния риск за личната неприкосновеност. Системите могат да обработват по-голям обем информация, да извличат допълнителни характеристики и да създават връзки, които не са очевидни от първоначалния видеозапис. Подобна тенденция се наблюдава и при други AI-базирани системи, където разширяването на аналитичните възможности може да създаде нови рискове, свързани с чувствителни данни, прекомерна обработка и недостатъчен контрол върху информацията [7]. Техническите рискове за неприкосновеността при генеративния изкуствен интелект са разгледани отделно в [14].

В този контекст принципите Privacy by Design и Privacy by Default придобиват особено значение. Защитата на личните данни трябва да бъде включена още при проектирането на системата чрез ограничаване на събираните данни, контрол върху аналитичните функции, диференциран достъп до резултатите, подходящо криптиране и проследимост на автоматизираните операции [1, 3].

При внедряване на интелигентни видеосистеми е необходимо да се оценява не само техническата им ефективност, но и характерът на информацията, която могат да извличат. Колкото по-голяма е степента на автоматизация и възможността за идентификация или поведенчески анализ, толкова по-голяма е необходимостта от ясни ограничения, контрол и периодична оценка на риска. Анализът на причините и последствията като метод за управление на риска е разгледан в [12].

В обобщение, интелигентният видеоанализ създава значителни възможности за повишаване на ефективността на видеонаблюдението, но променя и характера на рисковете за личните данни. Ефективната защита изисква техническите механизми за AI анализ да бъдат съчетани с минимизация на данните, строг контрол на достъпа, прозрачност, проследимост и предварително управление на риска.

6 Препоръки

Анализът на техническите рискове показва, че защитата на видеоданните не следва да се основава на единични механизми, а на последователно прилагане на взаимно допълващи се мерки през целия жизнен цикъл на информацията. Ефективната защита изисква още при

проектирането на системата да бъдат определени подходящи механизми за криптиране, контрол на достъпа, проследимост, съхранение и изтриване на данните.

На първо място, видеоданните следва да бъдат защитени както при предаване, така и при съхранение. Използването на защитени комуникационни протоколи и криптиране на архивите ограничава риска от прихващане и неоторизиран достъп. При облачни и хибридни решения е необходимо допълнително да се оценяват механизмите за защита, предлагани от външния доставчик, както и условията за достъп, резервиране и изтриване на данните [1, 3].

Контролът на достъпа следва да бъде организиран чрез индивидуални потребителски профили, надеждна автентикация и ясно разграничени права. При системи с дистанционен достъп или повишен риск е препоръчително използването на многофакторна автентикация, както и периодичен преглед на активните профили и предоставените разрешения. Правата за преглед, експортиране, конфигуриране и изтриване на записи не следва да бъдат предоставяни по подразбиране на всички потребители.

Системното логване на действията е друга необходима мярка. Регистрирането на достъпи, промени в конфигурацията, експортиране и изтриване на записи създава необходимата проследимост и подпомага анализа при инциденти. Периодичният преглед на логовете може да бъде използван и като превантивен механизъм за установяване на необичайна активност или опити за злоупотреба [4].

При интелигентни системи за видеонаблюдение е необходимо техническите възможности за автоматизиран анализ да бъдат ограничени до ясно определени функции и цели. Особено внимание следва да се отделя на лицевото разпознаване, поведенческия анализ и комбинирането на видеоданни с други информационни източници. В тези случаи прилагането на принципите Privacy by Design и Privacy by Default, както и предварителната оценка на риска, имат ключово значение за ограничаване на прекомерната обработка и на неоторизираното използване на чувствителна информация [1, 3, 14].

Необходимо е също да бъдат определени ясни срокове за съхранение и механизми за автоматизирано изтриване на записите. Натрупването на видеоданни извън необходимия период увеличава потенциалните последствия при компрометиране на системата и затруднява управлението на информацията.

7 Заключение

Развитието на цифровите и интелигентните системи за видеонаблюдение значително разширява възможностите за събиране, обработка и анализ на видеоданни, но едновременно с това увеличава изискванията към тяхната сигурност. Защитата на информацията следва да се разглежда като непрекъснат процес, който обхваща всички етапи от жизнения цикъл на видеоданните – от тяхното събиране и предаване до съхранението, достъпа, анализа и изтриването.

Анализът показва, че основните технически рискове са свързани с неоторизиран достъп, прихващане на мрежовия трафик, компрометиране на съхраняваните записи, недостатъчен контрол върху потребителските права и ограничена проследимост на действията в системата. При интелигентните решения допълнителни рискове възникват от автоматизираното извличане на информация, лицевото разпознаване, поведенческия анализ и възможността за комбиниране на видеоданни с други информационни източници.

Ефективната защита изисква съчетаване на криптиране при предаване и съхранение, надеждна автентикация, диференциран контрол на достъпа, системно логване и периодичен преглед на действията и потребителските права. Необходимо е също да бъдат прилагани ясни правила за сроковете на съхранение и контролирано изтриване на записите, така че да се ограничи ненужното натрупване на чувствителна информация.

Особено значение придобива интегрирането на защитата още на етапа на проектиране на системите. Прилагането на принципите Privacy by Design и Privacy by Default създава възможност рисковете да бъдат ограничени предварително, вместо мерките за защита да бъдат добавяни едва след възникване на проблеми.

В обобщение, сигурността на видеоданните в съвременните системи за видеонаблюдение зависи не от единична технология, а от цялостна архитектура за защита, която съчетава технически контрол, проследимост и управление на риска. Подобен подход позволява да се използват възможностите на цифровите и интелигентните видеосистеми, като едновременно с това се ограничава рискът за конфиденциалността, целостта и неприкосновеността на обработваната информация.

ЛИТЕРАТУРА:

[1] Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (GDPR).

[2] Стоянова, В. Интернет на нещата – анализ на сигурността при интелигентни структури. II International Scientific Conference CONFSEC, Borovets, 2018, Year 2, Issue 2 (4). ISSN 2603-2945 (Print), ISSN 2603-2953 (Online).

[3] European Data Protection Board. Guidelines 3/2019 on Processing of Personal Data through Video Devices, Version 2.0, 2020.

[4] Комисия за защита на личните данни. Добри практики от надзорната дейност на КЗЛД.

[5] Върбанова, Г. Значение на електронните доказателства в контекста на киберсигурността и националната сигурност. Варна: ВВМУ „Н. Й. Вапцаров“, 2024. ISBN 978-619-93016-0-9.

[6] AxxonSoft. Video Surveillance as a Service (VSaaS) Platform / Cloud Solutions.

[7] Anviz. Smart AI Surveillance / CCTV Solutions.

[8] Denev, D. Analytical study of the delay introduced as a result of encryption/decryption of voice transmitted over a VPN network. Journal Scientific and Applied Research, Vol. 20, 2021, pp. 80–85, ISSN 1314-6289.

[9] Nikolov, L., Slavyanov, K. On the Contemporary Cybersecurity Threats. Proceedings of the First International Scientific Conference CONFSEC 2017, Borovets, 11–14 December 2017, pp. 142–144, ISSN 2603-2945 (Print), ISSN 2603-2953 (Online).

[10] Dimitrova, E., Denev, D. The Development of Artificial Intelligence and its Applications in the Modern World. Proceedings of the Scientific Conference with International Participation MATTEH 2024, Vol. 2, Communication and Computer Technologies, Shumen, 2024, pp. 153–160, ISSN 1314-3921.

[11] Denev, D. Surveillance with Wireshark and its Use in Communication Networks. Annual of Konstantin Preslavski University of Shumen, Vol. XIII E, 2023, pp. 104–109, ISSN 1314-8818.

[12] Arabadzhieva-Kalcheva N., Tsankov Ts., Todorova M. Cause-Consequence Analysis as a Risk Management Method. Annual of Konstantin Preslavsky University of Shumen, Vol. XIV E, Faculty of Technical Sciences, 2024, ISSN 1314-8818, pp. 184–188. https://doi.org/10.46687/YT24NEL

[13] Iliev, D., Denev, D. Computer Security and Traffic Management in Communication Networks. Proceedings of the Scientific Conference with International Participation MATTEH 2024, Vol. 2, Communication and Computer Technologies, Shumen, 2024, pp. 161–169, ISSN 1314-3921.

[14] Kuzmanova, E., Dimanova, D. Technical Privacy Risks in Generative AI (GenAI) – Lessons from OWASP and Real-World Failures. 10th International Conference on Energy Efficiency and Agricultural Engineering (EE&AE 2025), 5–7 November 2025, Starozagorski Bani, Bulgaria. IEEE. DOI: 10.1109/EEAE65901.2025.11273791.

[15] Simeonova I. How GDPR treats automated decision-making. Journal Scientific and Applied Research, Konstantin Preslavsky University Press, 2025, ISSN 1314-6289 (Print), ISSN 2815-4622 (Online), pp. 164–175. https://doi.org/10.46687/jsar.v29i1.461

[16] Todorova-Lazarova, V. P. Dynamic Arrays in MS Excel for Data Processing and Analysis in Information Systems. International Scientific Conference UNITECH 2025, Gabrovo, 2025, pp. 1–6, ISSN 1313-230X.

[17] Nikolov, L. G. Wireless Network Vulnerabilities Estimation. Security & Future, Vol. 2, No. 2, 2018, pp. 80–82, ISSN 2535-0668 (Print), ISSN 2535-082X (Online).