

КИБЕРСИГУРНОСТ ПРИ УПРАВЛЕНИЕТО НА ИНТЕЛИГЕНТНИ СГРАДИ

Нончо Димитров

CYBERSECURITY IN THE MANAGEMENT OF SMART BUILDINGS

Noncho Dimitrov

Abstract: Smart buildings are fundamentally reshaping the real estate landscape. By weaving together traditional operational systems—like HVAC and access controls—with modern IT infrastructure, we've unlocked incredible efficiency and comfort. However, this hyper-connectivity is a double-edged sword. As our buildings get "smarter," they become prime targets for cyber threats, often leaving facility managers in a vulnerable position they aren't fully trained to navigate.

This article dives into the messy intersection where operational technology (OT) meets IT. We aren't just looking at the technical glitches; we're cataloging the specific threats aimed at Building Management Systems and addressing the very real "competency gap" currently haunting the industry. By leaning on established benchmarks like the NIS2 Directive, GDPR, and NIST 2.0, we explore what it actually takes to treat a building as a piece of critical infrastructure.

The core takeaway is simple: cybersecurity is no longer just "the IT guy's problem." It has evolved into a high-stakes management discipline. Success here requires a cultural shift—better policies, hands-on staff training, and a risk-governance mindset that is baked into daily operations. We also examine how "Security-by-Design" is shifting from a niche technical requirement to a major competitive advantage in the real estate market.

Ultimately, securing a smart building isn't something you can just "bolt on" as an afterthought. It requires a commitment from the boardroom down to the mechanical room. In today's climate, the owners who view security as a core business value will thrive, while those who ignore the operational and financial risks will find them simply too large to manage.

Key words: smart buildings; cybersecurity; building management systems; facility management; critical infrastructure; risk management.

Увод

През последните две десетилетия секторът на недвижимите имоти премина през една от най-мощните си трансформации – масовата дигитализация на сградния фонд. Жилищата са не само основен елемент от богатството на отделните домакинства, но и ключов двигател на макроикономическата стабилност (Stefanov and Dimitrova, 2025). Въвеждането на системи за сградна автоматизация (BMS), интернет на нещата (IoT) и облачни технологии превърна пасивните конструкции в „умни“ екосистеми. Ползите са неоспорими: оптимизация на енергийните разходи с близо 30% и драстично пониски оперативни разходи. Тази технологична еволюция обаче има и своята „тъмна“ страна – тя отвори врати за уязвимости, за които традиционният фасилити мениджмънт се оказва напълно неподготвен. Особено притеснителен е възходът на т.нар. *siegeware* (цифрова обсада на сгради), при която хакери блокират жизненоважни системи – от пожарогасене до климатизация – и изискват откуп за тяхното „освобож-

даване“. В контекста на болнични заведения и държавни обекти, това вече не е просто ИТ проблем, а сериозна заплаха за обществената сигурност.

Преплитането на оперативните (OT) и информационните технологии (IT) създава парадокс: докато системите стават по-ефективни, мениджърите, обучени предимно в инженерни и строителни дисциплини, се сблъскват с огромен дефицит на знания в сферата на киберзащитата. На този фон регулаторната среда става все по-строга – директиви като NIS2 и стандарти като NIST 2.0 вече третира сградните системи като част от критичната инфраструктура на държавата. Изследването е фокусирано върху управлението на киберсигурността в интелигентните сгради, разглеждани като стратегически активи и елемент на националната сигурност. Предмет на анализ са специфичните заплахи, произтичащи от сливането на ИТ и оперативни мрежи, както и организационните и професионални дефицити, които оставят фасилити мениджърите безсилни пред кибер-физическите рискове.

Целта на работата е да изгради цялостен мо-

дел за управление на киберсигурността в сградния фонд. За постигането ѝ са формулирани следните задачи:

1. Систематизиране на заплахите;
2. Анализ на управленския капацитет;
3. Оценка на регулациите;
4. Разработване на решения.

1. Технологичната екосистема на интелигентните сгради

Системите за управление на сгради (BMS) денонощно събират потоци от данни и координират всичко – от климатизацията (HVAC) и осветлението до асансьорите и пожарната безопасност. Тази сложна мрежа разчита на утвърдени, но често остарели протоколи като BACnet (Building Automation and Control Networking), Modbus (отворен индустриален комуникационен протокол), KNX (европейски стандарт за автоматизация на сгради) или LonTalk (известен преди като LonWorks, разработен за управление на сгради). (Стефанов, 2017, с. 95-96)

От технологична гледна точка, BMS всъщност са подвид на индустриалните системи за управление (ICS). Подобно на електроцентралите или пречиствателните станции, те са проектирани да работят десетилетия (често над 20 години), изискват абсолютна надеждност и трябва да реагират в рамките на милисекунди. Тук обаче се крие и голямото предизвикателство: тези системи са създавани в ера, когато сигурността се е гарантирала чрез физическа изолация, а не чрез криптиране.

Интелигентните сгради стават все по-уязвими към киберзаплахи поради сложната си мрежа от взаимосвързани устройства (Barnabás & Rajnai, 2023). Днес, когато „умните“ сгради се свързват към глобалната мрежа, липсата на вградена защита в BACnet или Modbus ги превръща в „отворена книга“ за нападателите. Командите често се предават в открит текст, което прави манипулацията на хардуера плашещо достъпна за всеки, успял да пробие периметъра на мрежата. Масовото навлизане на Интернет на нещата (IoT), която е революционна мрежова парадигма, при която физическите обекти са вградени със сензори, софтуер и свързаност, което позволява автономно събиране и обмен на данни без човешка намеса (Khan and Yuse, 2019), едновременно най-силният коз и най-слабото място на съвременната архитектура. В една голяма офис сграда могат да функционират

хиляди малки сензори – от термостати до интелигентни контакти. Ползата е измерима: умната оптимизация може да свали енергийните сметки с до 30% и да предвиди повреди на оборудването седмици преди те да се случат.

Парадоксът е, че докато тези устройства носят огромни спестявания, тяхната индивидуална защита често е пренебрегвана. Много сензори работят с фабрични пароли, не поддържат криптиране и рядко получават актуализации. Всеки един от тях е потенциална „входна врата“ към цялата инфраструктура. При хиляди устройства, генериращи милиони точки данни дневно, ръчният надзор е невъзможен. Това прави критично навлизането на алгоритми с изкуствен интелект, които сами да откриват аномалии в този безкраен поток от информация.

Съвременният модел за управление залага на хибриден подход. Критичните решения, изискващи незабавна реакция (например спиране на асансьор или регулиране на налягането), се вземат локално – в т.нар. „периферия“ (Edge). В същото време огромните масиви от данни се изпращат към облачни платформи за мащабен анализ и сравнение между различни обекти.

Този модел е изключително удобен, но и опасен. Облачните платформи са „златни мини“ за хакерите – в тях се съхраняват етажни планове, графици на заетост и спецификации на охранителни системи. Пробив при един доставчик на софтуер (SaaS) може да компрометира стотици сгради едновременно.

Истинското предизвикателство пред фасилити мениджърите днес е да балансират между мощта на облака и сигурността на локалните устройства. Това изисква не само технически решения, но и нова култура на управление, при която сигурността е заложена в самия проект на сградата, а не е просто добавка към месечния абонамент.

2. Киберзаплахи в застроената среда

Кибератаките срещу съвременните сгради не са монолитно явление – те представляват спектър от мотиви и възможности. За да разберем истинския риск, трябва да погледнем отвъд техническия код и да анализираме профила на нападателите – от държавно спонсирани групи до небрежни служители.

Начело на външните заплахи стои т.нар. *siegeware* – специализиран рансъмуер, който не се интересува от кражба на файлове, а от „взе-

мане на заложници“ в лицето на сградните системи. Тук залогът е физически: хакерите блокират асансьорите, деактивират противопожарната охрана или спират климатизацията (HVAC). В критични обекти като болници или центрове за данни оперативният престой е недопустим, което създава огромен психологически натиск върху мениджърите да платят откупа веднага.

Паралелно с финансово мотивираните групи наблюдаваме и намесата на държавни участници. Техните цели са стратегически – шпионаж или дълготраен саботаж. Сградите на правителствени агенции или отбранителни контрагенти често стават обекти на „тихо“ проникване, при което нападателите остават в мрежата месеци наред, събирайки данни за движението на персонала или конфигурацията на сигурността.

Най-големият риск често идва „отвътре“. От решаващо значение е, че съществуващите изследвания подчертават значителни пропуски, включително ограничени емпирични оценки и недостатъчно отчитане на човешкия фактор (Ciholas et al., 2019). Парадоксално, пробивите започват с обикновен фишинг имейл, на който служител е кликал несъзнателно. Небрежността – като използването на незащитен Wi-Fi от служебен лаптоп или споделянето на пароли с външни техници – е „отворена врата“, която не изисква сложни хакерски умения. Проблем са и бивши служители или изпълнители, чиито администраторски права не са били своевременно отнети.

В арсенала на нападателите фишингът и социалното инженерство остават най-мощните оръжия. Те често се представят за доверени партньори – например доставчика на асансьорна поддръжка, който изисква „спешен отдалечен достъп“ за отстраняване на повреда. Поради своя оперативен фокус, фасилити мениджърите често дават приоритет на бързата реакция пред протоколите за дигитална сигурност.

Веднъж попаднали в мрежата, нападателите използват зловреден софтуер за странично придвижване (lateral movement). Особено коварни са атаките от типа „Човек по средата“ (Man-in-the-Middle – MitM). При тях хакерът се вмъква в комуникационния път между температурен сензор и контролера на климатизацията. Понеже старите протоколи като BACnet пренасят данните без криптиране, нападателят може лесно да подмени информацията – например да накара системата да „мисли“, че в сградата е прекалено студено, провокирайки агресивно и потенциално разру-

шително поведение на хардуера.

3. Нови предизвикателства пред управлението на съоръженията

Дигитализацията на сградите наложи радикална промяна в профила на фасилити мениджъра. Днес вече не е достатъчно да разбираш от ОВК системи и енергийна ефективност; изисква се хибридна експертиза, която съчетава инженерството с киберсигурността. Рисковете за киберсигурността вече обхващат не само цифровите системи, но и физическата инфраструктура, като например управление на асансьори, ОВК системи и управление на достъпа (Stamatescu et al., 2020).

Традиционното образование в сектора все още набляга на механиката и управлението на бюджети, като почти изцяло пренебрегва ИТ аспектите. Резултатът е опасен вакуум: опитни мениджъри често не правят разлика между мрежова сегментация и защита на данните. От друга страна, чистите ИТ специалисти рядко разбират спецификите на сградната автоматизация.

Един от най-големите парадокси в строителния сектор е разминаването в жизнените цикли. Според тази логика, закупуването на жилище е сравнително бавен процес. Обикновено отнема много време: от създаването на определени условия, през приемането на решение и накрая, до неговото прилагане (Стефанов и Димитрова, 2020, с. 62). Докато една сграда и нейната инсталация се проектират за период от 20-25 години, софтуерните технологии остаряват за 3 до 5. Така се озоваваме в ситуация, в която през 2026 г. управляваме критични системи със софтуер от 2005 г.

Собствениците често са притиснати до стената: те не могат просто да изключат тези системи, защото те поддържат живота в сградата, но и не могат лесно да ги подменят поради огромните разходи. В тези случаи решението е „виртуално инсталиране на корекции“ чрез защитни стени и стриктна мрежова изолация, което намалява, но не премахва риска.

Съвременната сграда е зависима от армия от външни доставчици – от техници на асансьори до облачни оператори. Всяка една от тези връзки е потенциален вектор на атака. Често срещан сценарий е външен изпълнител да получи отдалечен достъп за поддръжка, който обаче остава активен и незащитен дълго след приключване на работата.

Проблемът се задълбочава от факта, че мал-

ките подизпълнители често нямат никаква киберкултура. Техен служител, работещ от незащитена домашна мрежа, може неволно да предостави „ключовете от сградата“ на киберпрестъпници. Управлението на този риск изисква не само технически контрол, но и сериозни договорни клаузи, право на одит и многофакторно удостоверяване за всеки външен достъп.

Най-трудната задача пред фасилити мениджъра е да защити бюджета за киберсигурност пред борда на директорите. В сектора на имотите фасилити мениджмънтът традиционно се разглежда като перо за съкращаване на разходи. Сигурността е „невидима“ полза – тя не носи наемни приходи, а само предотвратява евентуални загуби.

Математиката обаче е категорична. Един пробив в болнична сграда или център за данни може да струва милиони под формата на откуп, криминалистични разследвания и съдебни искове. Чрез прилагането на модели за възвръщаемост на инвестициите (ROI), базирани на намаляването на риска, мениджърите могат да докажат, че превантивните разходи всъщност спестяват огромни суми в дългосрочен план. В свят на нарастващи хибридни заплахи, киберустойчивостта вече не е лукс, а задължително условие за оцеляване на пазара.

4. Стратегическо управление на риска и измерения на националната сигурност

В съвременната геополитическа реалност границата между частната собственост и националната стабилност става все по-тънка. Обекти като болници, държавни ведомства, центрове за данни и енергийни възли вече не се разглеждат просто като недвижими имоти, а като критична инфраструктура.

Тази класификация променя всичко. Един киберпробив в интелигентните системи на една електроразпределителна компания може да доведе до каскаден ефект: спиране на охлаждането в центрове за данни, срив на банковите разплащания и парализа на публичните услуги. Когато говорим за болници или правителствени сгради, залогът е още по-висок – от пряка заплаха за човешкия живот до компрометиране на класифицирана информация и системи за командване. Управлението на бизнес процесите се включва в управлението на операциите само йерархично. Операционната стратегия е част (елемент) от общата стратегия на организацията (Забунов и

Забунова, 2015).

Регулаторната среда вече реагира на тези рискове. Европейската директива NIS2 (в сила от октомври 2024 г.) налага строги изисквания за киберсигурност, които обхващат не само самите организации, но и физическите сгради, които ги помещават. За фасилити мениджърите това означава нова отговорност: те вече трябва да предвиждат не само финансово мотивирани хакери, но и спонсирани от държави участници със стратегически цели за саботажи и шпионаж.

За да превърнат една уязвима сграда в защитена крепост, организациите се опират на два златни стандарта.

Рамката NIST CSF 2.0 е изключително практична за сградната среда. Тя не е просто технически списък, а управленски цикъл. Всичко започва с Управлението (Govern) – изричен ангажимент от страна на лидерството. Следват стъпките по Идентифициране на всяко IoT устройство в мрежата и неговата Защита чрез многофакторна автентикация и сегментиране. Ключовият момент тук е Откриването (Detect) – използването на системи, които в реално време разпознават аномалии в поведението на асансьорите или климатизацията, сигнализирайки за потенциална атака още в зародиш.

От друга страна, ISO/IEC 27001 предлага по-строга, административна структура. Този стандарт изисква изграждането на цялостна Система за управление на информационната сигурност (ISMS). За един фасилити мениджър това означава стриктен контрол върху физическия достъп до сървърните помещения, криптиране на комуникациите между сензорите и ясни процедури за проверка на всеки външен посетител или техник. Често най-добрият подход е хибриден: използване на гъвкавостта на NIST за концептуална рамка и детайлните контроли на ISO за оперативно изпълнение. Международните стандарти, които ISO развива, са полезни за организации от индустриалния и бизнес от всякакъв тип, за правителствени и други регулаторни органи, търговски представители, професионалисти, доставчици и клиенти на продукти и услуги в публичния и обществен сектор и най-вече за хората въобще в ролята им на консуматори и крайни потребители (Бонева, 2013).

Киберустойчивостта не означава само да не бъдеш хакнат – тя означава да знаеш какво да правиш, когато това се случи. Тук идва ролята на планирането за непрекъснатост на бизнеса.

5. Бъдещето на киберсигурното управление на имоти

В свят, в който една сграда генерира милиони точки данни дневно, традиционният надзор, базиран на твърди правила, вече е безсилен. Бъдещето принадлежи на изкуствения интелект (ИИ) и машинното обучение, които променят парадигмата: те не търсят „познати“ вируси, а се научават да разпознават какво е „нормално“ за конкретната сграда.

Изследвания от 2025 г. показват впечатляващи резултати – невронни мрежи постигат над 99% точност при идентифициране на аномалии. За един фасилити мениджър това означава система, която реагира мигновено, ако сензор за температура започне да подава физически невъзможни стойности или ако климатизацията внезапно започне да прехвърля големи обеми данни към външен IP адрес в три през нощта.

Ключовото предимство тук е т.нар. „обясним ИИ“. Вече не става дума за алгоритъм, който просто казва „има проблем“, а за система, която аргументира решението си. Това позволява на мениджърите да се доверят на автоматизираните реакции, намалявайки фалшивите тревоги и фокусирайки ресурсите върху реални заплахи, които човешкото око би пропуснало в безкрайния поток от данни.

Докато ИИ е „мозъкът“, който открива заплахи, блокчейн технологията се очертава като „неизличимата памет“ на сградата. Нейната сила се крие в децентрализираните регистри, които правят невъзможно подправянето на системни записи.

Ако хакер проникне в традиционна мрежа, първата му работа е да изтрие следите си в системните лог-файлове. При блокчейн архитектурата това е практически невъзможно – всеки запис за достъп или промяна в конфигурацията е криптографски подпечатан и разпределен в мрежата.

Особено интересни са т.нар. „умни договори“ (smart contracts). Те могат автоматично да налагат правила: например външен техник получава достъп до сървърното помещение само в интервала 9:00 – 17:00 ч. и само ако притежава валиден дигитален сертификат. Макар че предизвикателства като високата латентност и изчислителна цена все още ограничават масовото навлизане, нови протоколи (като IOTA) вече доказват, че технологията е готова за реално приложение в интелигентните градове.

На прага сме на фундаментална промяна в бизнес модела – преходът към „Сграда като услуга“ (Building-as-a-Service). Вместо собствениците сами да изграждат и поддържат ИТ инфраструктура, те все по-често се абонират за облачни платформи, които поемат пълното управление.

Този модел превръща сигурността от „разход“ в „конкурентно предимство“. Доставчиците на BaaS, управляващи хиляди обекти, имат икономическия стимул и мащаба да инвестират в киберзащита от най-висок клас – нещо, което един отделен собственик на офис сграда рядко може да си позволи. Тук говорим за принципа „Сигурност по проект“ (Security-by-Design), където защитата е заложена в самия код на платформата.

Разбира се, моделът BaaS носи и своите рискове – най-вече силната зависимост от един доставчик и превръщането му в централизирана цел за атака. Въпреки това, за големите портфолия от недвижими имоти ползите от централизираното управление, автоматичните пачове и споделената експертиза натежават. В бъдеще сертификати като ISO 27001 ще бъдат толкова важни за пазарната стойност на имота, колкото са енергийните сертификати днес.

Заклучение

Интелигентните сгради представляват революция в управлението на недвижимите имоти, но носят и безпрецедентни киберсигурностни рискове, които изискват холистичен управленски подход. Дигитализацията на сградния фонд генерира огромни оперативни ползи – енергийна оптимизация до 30%, предвидимо поддържане и драстично намалени разходи – но същевременно превръща традиционната критична инфраструктура в уязвима цел за кибератаки с потенциално катастрофални последици за обществената сигурност и националната стабилност.

Ключовият проблем произтича от технологичния парадокс: системите за управление на сгради разчитат на остарели протоколи (BACnet, Modbus), проектирани преди десетилетия за физически изолирани среди, без вградена киберзащита. Свързването им с интернет и масовото навлизане на IoT устройства с фабрични пароли и липса на криптиране създават милиони потенциални "входни врати" към критичната инфраструктура. Паралелно с това, фасилити мениджърите – традиционно обучени в

инженерни дисциплини – изпитват сериозен дефицит на компетенции в сферата на киберсигурността, докато регулаторната среда (NIS2, NIST 2.0) вече третира сградите като елемент на националната сигурност.

Заплахите еволюират от финансово мотивиран *siege warfare* – който блокира жизненоважни системи като асансьори и климатизация – до държавно спонсориран шпионаж и саботаж. Най-честите пробиви обаче идват от "вътрешни" уязвимости: небрежност на служители, незащитен отдалечен достъп за външни техници и слаб контрол върху веригата от подизпълнители. Управлението на този риск изисква не само технически мерки, но и културна трансформация – от борда на директорите до техническия персонал.

Решението лежи в многопластов подход: внедряване на стандартизирани рамки (NIST CSF 2.0, ISO 27001), интеграция на изкуствен интелект за откриване на аномалии в реално време, използване на блокчейн технологии за неизличими одит-логове и възприемане на принципа "Security-by-Design" още на етап проектиране. Моделът "Сграда като услуга" (Building-as-a-Service) се очертава като икономически ефективно решение, при което специализирани доставчици поемат цялостната отговорност за киберустойчивостта на мащабни портфолия.

Най-важният извод е, че киберсигурността вече не е изолирана техническа функция, а стратегически императив за управлението на съвременните имоти. Собствениците, които третират сигурността като основна бизнес стойност и инвестират в превантивни мерки, ще реализират дългосрочна конкурентна позиция и ще избегнат многомилionenните загуби от инциденти, съдебни иски и репутационни щети. В контекста на нарастващите хибридни заплахи, киберустойчивостта е критично условие за оперативна непрекъснатост, защита на обществената сигурност и пазарна устойчивост на недвижимата собственост.

Литература

Бонева, С. (2013) „Международната организация по стандартизация – двигател за развитието на стандартите от серията ISO 9000, ISO 14000 и ISO 9001:2000 и системите за управление на качеството“, в *Членството на България в Европейския съюз: четири години по-късно*.

София: Университет за национално и световно стопанство (УНСС), с. 156–168. Достъпно на: <https://www.ceeol.com/search/chapter-detail?id=926275>

(Boneva, S. (2013) 'International Organization for Standardization – Driving the Development of the ISO 9000, ISO 14000 and ISO 9001:2000 Standard Series and Quality Management Systems', in *Bulgaria's Membership in the European Union: Four Years Later*. Sofia: University of National and World Economy (UNWE), pp. 156–168. Available at: <https://www.ceeol.com/search/chapter-detail?id=926275>)

Забунов, Г. и Забунова, А. (2015) „Проблеми на прилагане на управлението на бизнес процесите във фасилити мениджмънта“, в *Строително предприемачество и недвижима собственост*. Варна: ИУ - Варна, с. 106–112. Достъпно на: <https://www.ceeol.com/search/chapter-detail?id=556396>

(Zabunov, G. and Zabunova, A. (2015) 'Problems of Implementation of the Business Processes Management in Facility Management', in *Construction Entrepreneurship and Real Property*. Varna: University of Economics - Varna, pp. 106–112. Available at: <https://www.ceeol.com/search/chapter-detail?id=556396>)

Стефанов, Др. (2017) „Интелигентните сгради и системите за сградна автоматизация“, *Недвижими имоти и Бизнес*, Том I (2), с. 93–97.

(Stefanov, Dr. (2017) „Inteligentnite sgradi i sisteme za sgradna avtomatizatsiya“, *Nedvizhimi imoti i Biznes*, Том I (2), с. 93–97)

Стефанов, Др. Димитрова, М. (2020) „Развитие на строителната активност в България в периода 2010-2019 година“, *Строително предприемачество и недвижима собственост*, том 35, с. 60–68.

(Stefanov, Dr. Dimitrova, M. (2020) „Razvitie na stroitelната aktivnost v Bŭlgariya v perioda 2010-2019 godina“, *Stroitelno predpriemachestvo i nedvizhima sobstvenost*, том 35, с. 60–68.)

Barnabás, S. and Rajnai, Z. (2023). Cyber Security Analysis of Smart Buildings from a Cyber Security Architecture Point of View. *Interdisciplinary Description of Complex Systems*, 21(2), pp.141–147. doi:<https://doi.org/10.7906/indecs.21.2.2>.

Bryant, S. (2025). Cybersecurity Risks in Smart Buildings | KMC Controls. [online] KMC Controls | Building Geniuses. Available at: <https://www.kmccontrols.com/blog/the-hidden-cyber-risks-of-smart-buildings/>.

Chang, M, Koerber, B & Murat Soganci 2022,

Converge IT and OT to turbocharge business operations' scaling power, McKinsey & Company. [online] Available at: <https://www.mckinsey.com/capabilities/operations/our-insights/converge-it-and-ot-to-turbocharge-business-operations-scaling-power>.

Ciholas, P., Lennie, A., Sadigova, P. and Such, J.M. (2019). The Security of Smart Buildings: a Systematic Literature Review. [online] arXiv.org. doi:<https://doi.org/10.48550/arXiv.1901.05837>.

Cybergensecurity.com. (2025). \r\n \n Cybersecurity in Building Management Systems and Smart Sites\r\n \r\n. [online] Available at: <https://www.cybergensecurity.com/cybersecurity-in-building-management-systems-and-smart-sites>

Darktrace.com. (2024). Darktrace. [online] Available at: <https://www.darktrace.com/cyber-ai-glossary/cybersecurity-for-building-management-systems>.

Help Net Security (2025) Exposed and unaware? Smart buildings need smarter risk controls. [Online] Available at: <https://www.helpnetsecurity.com/2025/07/04/building-management-systems-bm-s-risk/>

Khan, J.Y. and Yuce, M.R. eds., (2019). Internet of Things (IoT). Jenny Stanford Publishing. doi:<https://doi.org/10.1201/9780429399084>.

Shah, S.F.A., Mazhar, T., Khan, M.A., Khan, S.A., Ullah, N., Ahmad, W., Jiang, W. and Hamam, H. (2025). Challenges of IoT sensors in smart buildings ecosystems and integration of blockchain

for enhanced security and efficiency. Sustainable Computing: Informatics and Systems, [online] 49, p.101279. doi:<https://doi.org/10.1016/j.suscom.2025.101279>.

Stamatescu, G., Stamatescu, I., Arghira, N. and Făgărășan, I. (2020). Cybersecurity Perspectives for Smart Building Automation Systems. [online] IEEE Xplore. doi:<https://doi.org/10.1109/ECAI50035.2020.9223152>.

Stefanov, D. and Dimitrova, M. (2024) 'Housing Loan Trends in Bulgaria and Croatia: An Analysis of Some Important Indicators (2011-2022)', *Journal of Electrical Systems (JES)*, 20(11s), pp. 3278–3290. Available at: <https://journal.esrgroups.org/jes/article/view/8069/5478>

Veridify Security and Veridify Security (2023). The Importance of Protecting Smart Building Technology from Cyber Threats. [online] Veridify Security. Available at: <https://www.veridify.com/article/the-importance-of-protecting-smart-building-technology-from-cyber-threats/>

Assoc. Prof. Dr. Noncho Dimitrov, PhD
University of National and World Economy,
Department of National and Regional Security
1700 Sofia, Student District,
No.19 December 8th st., UNWE, cab. 5030
E-mail: noncho_dimitrov@unwe.bg