

Organizational Issues Regarding Hotel Information System Protection Activities

Assist. Prof. PhD Stefka Petrova
University of Economics - Varna, Varna, Bulgaria
s.petrova@ue-varna.bg

Prof. DSc Pavel Petrov
University of Economics - Varna, Varna, Bulgaria
petrov@ue-varna.bg

Abstract

In the current stage of digitalization, the hotel industry is characterized by an intense dependence on information technology. This dependence makes hotel computer networks critical infrastructures requiring a high degree of protection against cyber threats. Hotels represent a particularly vulnerable sector due to the large volume of personal and financial data, numerous external integrations (tour operators, payment systems, online booking platforms), hiring seasonal and rotational staff, and the presence of a variety of devices, often without centralized management. The NIST Cybersecurity Framework 2.0, published in 2024 by the US National Institute of Standards and Technology, offers an integrated cybersecurity management model applicable to all industries, including the hospitality industry. Its strength lies in its adaptability to different organizational sizes and specificities. This publication examines how the measures described can be applied to protect hotel network infrastructure, focusing on organizational issues arising in the implementation process.

Keywords: hotel, cybersecurity, NIST CSF 2.0, Property Management System, Hotel Information System

JEL Code: L86

DOI: 10.56065/IJUSV-ESS/2025.14.2.49

Въведение

В съвременните условия на дигитализация, хотелската индустрия се характеризира с висока зависимост от информационни технологии, като се използват голям брой информационни системи – за резервации (Koh & Hassim 2021), управление на имоти (Property Management Systems PMS), плащания, контрол на достъпа, IoT устройства (Moyeenudin et al. 2021), онлайн платформи за гости и др. Тази зависимост прави хотелските компютърни мрежи критични инфраструктури, изискващи висока степен на защита срещу киберзаплахи. Допълнителни проблеми създават големия обем лични и финансови данни, множество външни интеграции с други информационни системи (туроператори, платежни системи, онлайн резервационни платформи), сезонен и ротационен персонал, разнообразие от устройства.

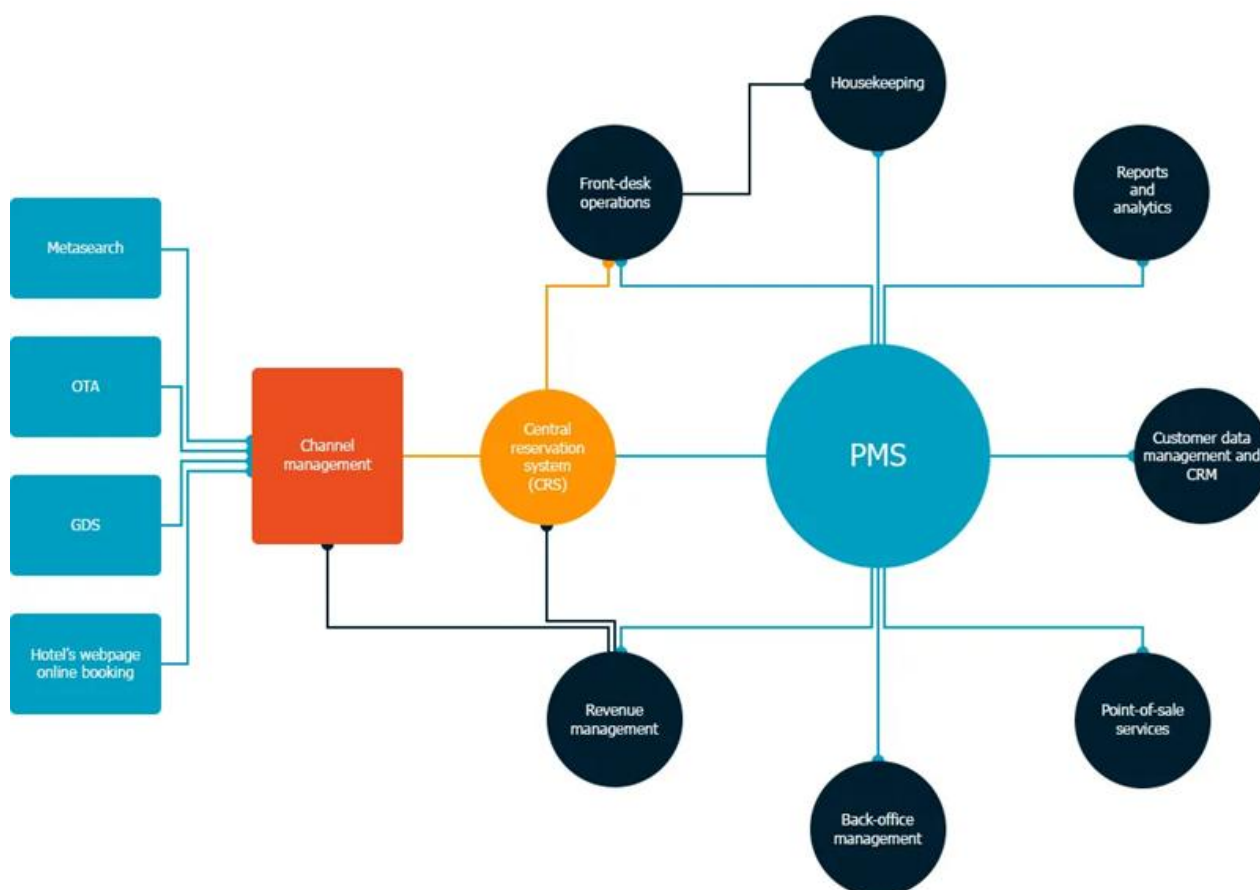
Основните организационни проблеми, които възпрепятстват прилагането на ефективна киберсигурност, включват: недостатъчна координация между ИТ отдел и управленския персонал; ограничени ресурси и ниска осведоменост за риск сред служителите; липса на формализирана политика за сигурност и оценка на риска (Petrov et al. 2021); отсъствие на процедури за реагиране при инциденти; недостатъчна интеграция между технологични и организационни мерки (Thealla et al. 2024). Поради това е необходимо предварително да се организират и проведат дейности, с които да се противодейства на потенциалните заплахи. Самостоятелният подход, базиран само на знанията на локалния мениджмънт не е подходящ, тъй като е възможно да се пропуснат съществени моменти по отношение на организацията, а е по-подходящо да се прилагат мерки, описани, широко обсъждани и поддържани от обществени институции, като например NIS2 директивата на ЕС, документи на САЩ и др. (Parmar & Miles 2024).

Документът NIST CyberSecurity Framework 2.0 (CSF 2.0), публикуван през 2024 г. от Националния институт по стандарти и технологии (NIST) на САЩ, предлага интегриран модел за управление на киберсигурността, приложим във всички индустрии, тъй като може да се адаптира към различни, по размер и специфики на дейността, организации, включително и хотели. Настоящата публикация разглежда как мерките от CSF 2.0 могат да се приложат за защита на хотелска мрежова инфраструктура, като се акцентира върху организационните проблеми, възникващи в процеса на реализация.

1. Базови информационни системи, използвани в хотелите

Типичната ИТ инфраструктура на един хотел е комплексна и включва няколко основни подсистеми, всяка със специфични функции и представлява потенциална точка на уязвимост в киберсигурността на хотела:

- Системата за управление на собствеността (Property Management System, PMS) управлява резервации, настаняване/напускане, разпределение на стаите, тарифиране, профили на гостите (лични данни, предпочитания), фактуриране и отчетност. PMS често се интегрира с други системи и платежни шлюзове. Основните заплахи включват кражба на лични данни и данни от дебитни/кредитни карти, SQL инжекции, атаки чрез уязвими API връзки между системите, атаки с откраднати акаунти с цел блокиране на операциите. На фиг. 1 е показана общата структура и възможностите за интеграция с други системи на системите от тип PMS.



Фигура 1. Структура на система за управление на собствеността (PMS) и възможности за интеграция с други системи

Източник: AltexSoft Inc, 2018, <https://altexsoft.medium.com/hotel-property-management-systems-products-and-features>

- Системата за управление на взаимоотношенията с клиентите (Customer Relationship Management, CRM) събира т.нар. "чувствителна" информация: профили, предпочитания, история на престои и комуникации. За нея са типични атаки тип „phishing“, неоторизиран достъп чрез компрометирани пароли и изтичане на данни вследствие на лошо конфигурирани облачни услуги.

- Системите за управление на каналите (Channel Management System, CMS) синхронизира наличността на стаите и цените в реално време между PMS и множество онлайн туристически агенции, платформи, глобални дистрибуционни системи (като Booking, Expedia и т.н.) и уебсайта на хотела. Основни рискове са Man-in-the-Middle (MitM) атаки при нешифровани връзки, манипулиране на данни чрез компрометирани API токени, атаки за манипулиране на цените или резервациите.

- Системите за продажба на място (Point of Sale, POS) управляват трансакциите при настаняване, в ресторанти, барове, СПА центрове и други обекти в хотела. Обработват плащания, издават сметки и проследяват инвентара. POS терминалите често работят в обща мрежа с PMS, което създава риск от зловреден софтуер за източване на данни от карти (skimming malware) и атаки тип ransomware, които могат да блокират продажбената инфраструктура.

- Мрежовата инфраструктура за гости и персонал предоставя Wi-Fi, кабелен интернет, IP телефония, и системи за забавление в стаите (например IPTV). Обикновено се разделя на сегментирани мрежи (гости, персонал, IoT системи), които са разположени зад мрежови файървол (Malkawi et al., 2021). Възможни са Man-in-the-Middle (MitM) атаки (в Wi-Fi мрежата за гости), фишинг/социално инженерство (към персонала), неоторизиран достъп през несегментирана мрежа.

- Системите за автоматизация на сгради/управление на енергията контролират и автоматизират климатизацията, осветлението, пожароизвестяването и сигурността. Често са базирани на IoT и при компрометиране на IoT мрежата (напр. чрез уязвим IoT сензор) може да се извършат DoS/DDoS атаки срещу контролери. Възможно е да се извърши саботажни дейности, например чрез промяна на настройките за пожароизвестяване или достъп.

- Системите за сигурност и контрол на достъпа контролират електронния достъп до стаите чрез електронни карти за стаи или мобилен достъп, видеонаблюдение и IoT устройства. Основните рискове са компрометиране на IoT устройства, нешифровани комуникационни протоколи и физически достъп чрез клониране на карти.

За да се ограничат тези рискове, хотелите трябва да прилагат цялостна стратегия за киберустойчивост, включваща редовни одити, многослойна защита, обучение на персонала и строга политика за управление на достъпа. Необходимо е да се премине от реактивни към проактивни организационни мерки, които да са насочени към устойчивостта на системите и защитата на данните на гостите като основен бизнес актив и да се гарантира доверие, непрекъсваемост и защита на данните както на гостите, така и на самия бизнес.

2. Приложение на мерките от NIST Cybersecurity Framework 2.0 при защита на хотелска компютърна мрежа

CSF 2.0 структурира управлението на киберсигурността в шест основни функции, представени в табл.1.

Всяка функция е свързана с категории и под категории, описващи конкретни дейности и резултати, като се описва взаимодействието между техническите и организационните аспекти на сигурността. Важен стратегически момент е създаването на т.нар. "Организационен профил", който описва текущото и/или целевото (желаното) състояние на организацията в областта на киберсигурността. Организационните профили се използват за изясняване, адаптиране, оценка и приоритизиране на резултатите от киберсигурността въз основа на целите на мисията на организацията, очакванията на заинтересованите страни, средата за

заплахи и изискванията. Профилът може да се използва и за оценка на напредъка към целевите резултати. На фиг.2 са представени етапите на работа по създаване на профил на организацията с цел постоянно подобряване на дейностите по киберсигурност.

Таблица 1. Основни функции, заложи в CSF 2.0

| № | Функция | Основна цел |
|---|------------------------------|---|
| 1 | Govern (управление) | Определя стратегическите политики, роли и отговорности за сигурността; нова функция в версия 2.0. |
| 2 | Identify (идентифициране) | Идентификация на активи, рискове и зависимости. |
| 3 | Protect (защита) | Прилагане на мерки за защита на активите и достъпа. |
| 4 | Detect (откриване) | Наблюдение и откриване на аномалии и инциденти. |
| 5 | Respond (реагиране) | Процедури и действия при киберинциденти. |
| 6 | Recover (възстановяване) | Възстановяване на услуги и подобряване на устойчивостта след инцидент. |



Фигура 2. Връзка между основните функции, заложи в CSF 2.0 и етапи на работа по създаване на профил на организацията

Източник: NIST Cybersecurity Framework 2.0: Quick-Start Guide for Creating and Using Organizational Profiles, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1301.pdf>

В най-общ план, в една хотелска мрежа приложението на CSF 2.0 може да се реализира чрез отчитане на спецификите на дейността. Така например, **функция “Govern”**, която включва управление на киберсигурността, има за цел създаване на организационна структура и култура за управление на киберриска. Приложението в хотелска среда изисква разработване на политика за информационна сигурност (Information Security Policy), включваща всички отдели – рецепция, резервации, финанси, техническа поддръжка и администрация.

Необходимо е определяне на роли и отговорности за всеки служител, свързани с достъп до системи и данни. Тази дейност може да се изпълнява от специално назначен мениджър по киберсигурност или чрез изнасяне на тази функция към външен доставчик (outsourcing). Основен проблем е, липсата на експертен капацитет, тъй като повечето хотели не разполагат с вътрешен ИТ специалист с компетенции по сигурността. Понякога има несъгласуваност в действията между различни отдели (напр. маркетинг и поддръжка) като често действат независимо, без обща стратегия. Възможно е да има недостатъчно финансиране, тъй като сигурността често се възприема като разход, а не като инвестиция. За решаването на тези проблеми при големи хотели може да се създаде комитет по киберсигурност на организационно ниво, който да координира политики, рискови оценки и комуникация с външни доставчици.

Относно **функция “Identify”**, включваща идентифициране на активи и рискове, е необходимо да се определят какви системи, данни и процеси трябва да бъдат защитени. Приложението в хотелска мрежа включва дейности по създаване на инвентаризация на ИТ активите – PMS, POS системи, Wi-Fi инфраструктура, IoT устройства (ключалки, термостати, камери). Картографиране на потоци от данни между PMS, резервационни сайтове и платежни шлюзове. Идентифициране на зависимости от трети страни – външни доставчици, софтуер, облачни услуги. Провеждане на оценка на риска с отчитане на вероятността и въздействието на DoS/DDoS атаки, пробиви на данни или вътрешни злоупотреби. Основни възможни организационни проблеми са липса на актуална документация за активите и честата смяна на персонала, което води до загуба на задълбочено познаване на системите. Внимание трябва да се отделя и при сключване на договори с доставчици относно отговорността при инциденти. Решаването на споменатите проблеми може да се извърши чрез създаване на централизиран регистър на активите и периодично обновяване при промяна в инфраструктурата или договорните отношения.

Функцията “Protect” се отнася за защита на системите и данните чрез прилагане на технически и организационни контроли за предотвратяване на инциденти. Обхваща редица дейности като контрол на достъпа (Access Control) чрез ограничаване на достъпа до административни интерфейси само от доверени IP адреси и използване на уникални потребителски профили и силна автентикация (MFA) за PMS и вътрешните системи. Мрежовата защита може да се реализира чрез сегментиране на хотелската мрежа на отделни VLAN-и (гост мрежа, служебна мрежа, управление на IoT), конфигуриране на защитни стени с правила за блокиране на подозрителен трафик и инсталиране на IDS/IPS системи (напр. Suricata, Snort). Необходимо е и обучение на персонала чрез редовни семинари за разпознаване на фишинг и социално инженерство, както и практически тренировки за реагиране при инциденти. Тези дейности са важни, тъй като несъответствието между човешки потенциал и технически мерки компрометира защитата (например, добра инфраструктура, но слаба дисциплина на служителите и споделяне на пароли). Честата ротация на персонала често води до неактуални потребителски акаунти. Възможно е служителите на рецепция и поддръжка да нямат базови знания за сигурност и затова въвеждането на обучителна програма по киберхигиена, задължителна при назначаване, и автоматизирано управление на достъпа чрез систем и от тип Identity and Access Management (IAM) са от значителна полза.

С цел навременно идентифициране на аномалии, атаки и инциденти е **функция “Detect”**, за реализацията на която се използват системи за централизирано събиране на логове (SIEM), като например Wazuh, Splunk или Elastic Stack. Те се настройват за мрежов мониторинг за откриване на DoS атаки, подозрителен трафик или необичайни заявки към PMS, както и се задава определен праг за алармиране при прекомерен трафик или необичайно натоварване. Много често липсва достатъчен персонал за мониторинг от тип 24/7, липсват ясни процедури за ескалация при аларми, както и използването на различни системи от различни доставчици, при което логовете са с различен формат и несинхронизирани по време.

При невъзможност за поддръжка на собствена автоматизирана SIEM платформа с AI анализ за ранно откриване на инциденти може да се сключи договор с външен доставчик от тип Security Operations Center (SOC).

Реагирането при инциденти, предвидено във **функция “Respond”**, цели ограничаване на ефекта от извършена кибератака. В организационен план е необходимо разработване на Incident Response Plan (IRP), включващ: класификация на инциденти (напр. DoS, пробив, неоторизиран достъп), процедури за изолация на засегнати системи, комуникация с външни партньори и органи, провеждане на тестове за готовност (simulation drills) (Cisco, 2025; CISA, 2025).

Често съществуват редица организационни проблеми, като например липса на яснота кой има право да реагира, липсва вътрешна комуникационна структура при инцидент, отсъствие на външна комуникационна стратегия, при което има риск от увреждане на репутацията при изтичане на данни. Необходимо е създаване на комуникационен механизъм, чрез който да се координират действия между ИТ, мениджмънт и други звена.

Последната **функция “Recover”**, обхваща дейности по възстановяване на нормалните операции след инцидент и извличане на положителен опит. Възстановяването значително се улеснява ако има изградена система от резервни сървъри и системи за бекъп (на място и/или чрез облачна услуга) и редовно се провеждат тестове за възстановяване на данни (disaster recovery tests). Необходимо е да се извършва анализ на инцидентите и актуализация на политиките за сигурност. Много често бекъп процедури съществуват само на хартия и никога не са проверени на практика. Няма ясни критерии за „пълно възстановяване“. Отсъства координация между ИТ и оперативния мениджмънт след инцидента. От полза е създаването на план за непрекъснатост на бизнеса (Business Continuity Plan, BCP), синхронизиран с IRP, който периодично да се тества в реални условия.

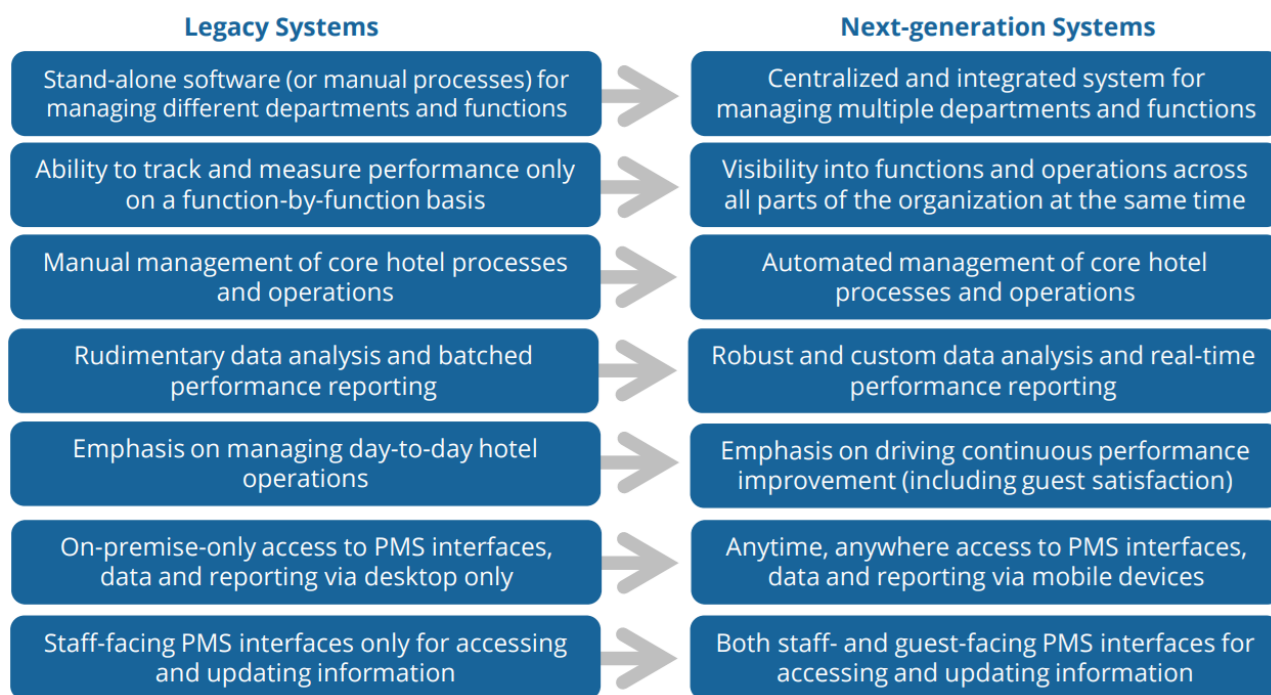
3. Тенденции в развитието на хотелските компютърни системи и тяхната защита

Както беше изяснено по-напред в изложението, хотелските компютърни системи са комплексна ИТ инфраструктура, която в най-общ план включва административна подсистема: PMS, CRM, HR и финансови системи; оперативна подсистема: POS терминали, системи за достъп до стаи, камери, климатизация и IoT устройства; подсистема за развлечение на гостите: Wi-Fi за посетители, кабелна и IP телевизия (често без адекватно разделяне от вътрешната мрежа); облачна част: платформи за онлайн резервации и плащания.

Всяка подсистема се развива в течение на времето в резултат на последните достижения на техническия прогрес в съответната област. Основните тенденции в развитието на хотелските компютърни системи са насочени към автоматизация, персонализация на преживяването на гостите и пълна интеграция на всички хотелски операции. Чрез системи от тип „големи данни“, базирани на изкуствен интелект, е възможно да се анализират огромно количество данни (Butorova et al., 2022; Kostadinova et al. 2023), например чрез Apache Kudu (Mileva et al. 2021), относно предпочитания на госта, история на престоя, поведение и като резултат да се предлагат динамични и индивидуални препоръки за услуги, стаи, ресторанти или дейности. С цел оптимално управление на приходите (Revenue Management) с помощта на специални алгоритми може да се извършва динамично ценообразуване в реално време, предназначено за различни онлайн платформи, при което цените на стаите се оптимизират на база моментната заетост, търсенето, цените на конкуренцията и други фактори, като по този начин да се максимизират приходите.

Друго направление в повишаване на нивото на дигитализацията (Petrova & Petrov 2023) е дигиталното обслужване или самообслужване – регистрация, настаняване и напускане чрез лицево разпознаване или сканиране на документи; цифрови ключове за стаите на гостите чрез техните мобилни телефони и по този начин премахването на необходимостта от физически контакт (особено подходящо в периоди на пандемии) и др.

Някои големи ИТ компании са разработили пътната карта, описваща тенденциите при миграция към по-нови хотелски системи, които следва да се имат в предвид при преход към PMS от следващо поколение, като са сравнили функционалността на съществуващите системи с тези от следващо поколение (фиг.3).



Фигура 3. Пътната карта, описваща тенденциите при миграция към по-нови хотелски системи, които следва да се имат в предвид при преход към PMS от следващо поколение

Източник: Oracle Hospitality, *The 2023 Smart Decision Guide to Hotel Property*

Management Systems, <https://www.oracle.com/a/ocom/docs/gated/2023-smart-decision-guide-hotel-property.pdf>

Както при всяка информационна система, миграцията към ново поколение хотелски компютърни системи и особено към облачни решения (Jordanov et al. 2024), може да създаде редица проблеми, т.е. съществуват потенциални заплахи и рискове за нормалното изпълнение на дейностите. Например, възможна е загубата на исторически данни за гостите (профили, предпочитания, лоялност), финансови записи или данни за резервациите при прехвърлянето от старата към новата система. Рискът се увеличава, ако има несъвместимост на форматите на данните между стария и новия софтуер или грешки в процеса на преобразуване на данните (експорт/импорт).

При неуспешната или нестабилна интеграция с всички останали системи - POS (касови апарати), счетоводен софтуер и др., може да се получи дублиране на резервации, грешки в ценообразуването или невъзможност за фактуриране. При облачни системи (Gulmez et al. 2015), липсата или прекъсването на интернет връзката може да доведе до спиране на достъпа до системата, което прави невъзможни дейностите по настаняване, напускане и управление на текущите резервации.

При преход към нови системи следва да се отчита, че е много вероятно да има периоди, в които нито старата, нито новата система работят пълнофункционално, и за да не се създават оперативен хаос и лошо обслужване на гостите, трябва да се избягват натоварените сезони и пикови моменти. Влияние може да окаже и човешкият фактор, тъй като персоналът, свикнал с години да работи със старата система, може съзнателно или подсъзнателно да се съпротивлява срещу промяната. Възможно е служителите да не използват пълния потенциал на новата

система, а само основните функции поради недостатъчното или некачествено обучение (Maria et al., 2018). Това води до грешки в работата, спад в ефективността и разочарование. В този смисъл следва да се очаква, че докато служителите свикнат с новите интерфейси, работни процеси, начини на отчитане, и прочие, скоростта на обслужване ще намалее, което може да доведе до опашки на рецепцията и забавяне на обслужването на гостите.

Заклучение

В заключение, NIST CSF 2.0 предлага шест ключови функции за управление на киберриска, което за един хотел означава създаване на политиката за сигурност на чувствителните данни, идентифициране на всички активи (PMS, POS, IoT устройства в стаите) и техните уязвимости. Защитата се извършва чрез използване на силни пароли, многофакторно удостоверяване и сегментиране на мрежата (за гости, за персонал). Откриването на аномалии и опити за проникване в мрежата (Simeonidis et al. 2024) са от съществено значение, за да може да се реагира бързо при инциденти, като се изолират засегнатите системи. В случай на сериозни инциденти, следва процес на възстановяване, при което трябва да се осъществи бързо възобновяване на всички хотелски операции (като резервации и настаняване) след кибератака, чрез предварително въведен план за архивиране и възстановяване на данни.

Основните тенденции в развитието на хотелските компютърни системи са пълната автоматизация и персонализация на преживяването на гостите, автоматично прогнозно ценообразуване, мобилното и безконтактно обслужване, преминаване към облачни платформи. Миграцията към нови хотелски системи е свързана с основни рискове като загуба или непълна миграция на исторически данни и оперативен хаос поради нестабилна интеграция с други системи. Ключови заплахи са също съпротивата на персонала, недостатъчното обучение и зависимостта от интернет връзката при облачните решения, което може да доведе до спад в производителността и непредвидени финансови разходи.

References

1. Butorova, A., Baglaeva, E., Subbotina, I., Sergeeva, M., Sergeev, A., Shichkin, A., & ... (2022). Application of the Wavelet Data Transformation for the Time Series Forecasting by the Artificial Neural Network. In *International Conference on New Trends in the Applications of Differential Equations in Sciences*. Cham: Springer International Publishing. pp.365-370. DOI: <https://doi.org/10.1007/978-3-031-21484-4>
2. CISA (2025). Cybersecurity and Infrastructure Security Agency. Incident Response Plan (IRP) Basics, [Online] Available from: https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf [Accessed 28/10/2025]
3. Cisco (2025). What Is an Incident Response Plan for IT?, [Online] Available from: <https://www.cisco.com/site/us/en/learn/topics/security/what-is-an-incident-response-plan.html> [Accessed 28/10/2025]
4. Gulmez, M., Ajanovic, E., & Karayun, I. (2015). Cloud-based vs desktop-based property management systems in hotel. *The USV Annals of Economics and Public Administration*, 15(1 (21)), pp.160-168. DOI: [https://doi.org/10.4316/aepa.2015.15.1\(21\).160-168](https://doi.org/10.4316/aepa.2015.15.1(21).160-168)
5. Jordanov, J., Simeonidis, D., & Petrov, P. (2024). Containerized Microservices for Mobile Applications Deployed on Cloud Systems. *International Journal of Interactive Mobile Technologies*, 18(10), pp.48-58. DOI: <https://doi.org/10.3991/ijim.v18i10.45929>
6. Koh, W. S., & Hassim, Y. M. M. (2021). Hotel reservation management system. *Applied Information Technology and Computer Science*, 2(2), pp.973-992. DOI: <https://doi.org/10.30880/aitcs.2021.02.02.061>
7. Kostadinova, I., Dimitrov, G., Martsenyuk, V., Rancic, D., Dirgova-Luptakova, I., Jovancevic, I., & ... (2023). Research and Analysis of IT Specifications of Good Practices in the Area of Artificial Intelligence. In *2023 16th International Conference on Advanced Technologies*,

- Systems and Services in Telecommunications (TELSIKS)*, IEEE, pp.284-290. DOI: <https://doi.org/10.1109/TELSIKS57806.2023.10316145>
8. Malkawi, R., Alsmadi, I., Aleroud, A., & Petrov, P. (2021). A firewall-adversarial testing approach for software defined networks. *Journal of Theoretical and Applied Information Technology*, 99(1), pp.227-241.
 9. Maria, N. N., Thecla, O. K., Chukwu, S., & Ifenyinwa, O. (2018). An analysis on the impact of the usage of Fidelio OPERA property management system in Transcorp Hilton Hotel Abuja. *European Journal of Computer Science and Information Technology*, 6(2), pp.1-19. DOI: <https://doi.org/10.37745/ejcsit.2013>
 10. Mileva, L., Petrov, P., Yankov, P., Vasilev, J., & Petrova, S. (2021). Prototype model for big data predictive analysis in logistics area with Apache Kudu. *Economics and Computer Science*, 7(1), pp.20-41. [Online] Available from: <http://eknigibg.net/Volume7/Issue1/spisanie-br1-2021.pdf> [Accessed 28/10/2025]
 11. Moeenudin, H. M., Williams, J., Srivastava, C., & Manivel, K. (2021). Cloud based property management system in integration with IoT. *Turkish Journal of Computer and Mathematics Education*, 12(9), pp.221-225.
 12. NIST Cybersecurity Framework 2.0: Quick-Start Guide for Creating and Using Organizational Profiles, [Online] Available from: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1301.pdf> [Accessed 28/10/2025]
 13. Oracle Hospitality, The 2023 Smart Decision Guide to Hotel Property Management Systems, [Online] Available from: <https://www.oracle.com/a/ocom/docs/gated/2023-smart-decision-guide-hotel-property.pdf> [Accessed 28/10/2025]
 14. Parmar, M., & Miles, A. (2024). Cyber Security Frameworks (CSFs): An Assessment Between the NIST CSF v2. 0 and EU Standards. In *2024 Security for Space Systems (3S)*, IEEE, pp.1-7. DOI: <https://doi.org/10.23919/3S60530.2024.10592293>
 15. Petrov, P., Stoev, S., Radev, M., Sergeev, A., & Dimitrov, G. (2021). Risk management processes in information systems development. *International Multidisciplinary Scientific GeoConference Surveying Geology and Mining Ecology Management, SGEM*, 21(7), pp.467-473. DOI: <https://doi.org/10.5593/sgem2021/2.1/s07.18>
 16. Petrova, S., & Petrov, P. (2023). Models for Determining the Reached Level of Digitalization. In *International Conference on Informatics in Economy*. Singapore: Springer Nature Singapore, pp.137-147. DOI: https://doi.org/10.1007/978-981-99-6529-8_12
 17. Simeonidis, D., Petrov, P., Penchev, G., Petrova, S., Dimitrov, G., & Petrivskiy, V. (2024). Performance and Accuracy Assessment of Detecting Network Intrusions with eSOM-Based Techniques. In *2024 International Conference Automatics and Informatics (ICAI)*, IEEE, pp.586-591. DOI: <https://doi.org/10.1109/ICAI63388.2024.10851699>
 18. The NIST Cybersecurity Framework (CSF) 2.0 [Online] Available from: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf> [Accessed 28/10/2025]
 19. Thealla, P., Nadda, V., Dadwal, S., Oztosun, L., & Cantafio, G. (Eds.). (2024). *Corporate cybersecurity in the aviation, tourism, and hospitality sector*. IGI Global. DOI: <https://doi.org/10.4018/979-8-3693-2715-9>