Citation: Styborska K., (2024) 'Analysis of the Impact of technological risks on multi-family residential development', *Space & Form | Przestrzeń i Forma* 60. http://doi.org/10.21005/pif.2024.60.C-04

DOI: 10.21005/pif.2024.60.C-04

ANALYSIS OF THE IMPACT OF TECHNOLOGICAL RISKS ON MULTI-FAMILY RESIDENTIAL DEVELOPMENT

ANALIZA WPŁYWU ZAGROŻEŃ TECHNOLOGICZNYCH NA ZABUDOWĘ WIELORODZINNĄ

Katarzyna Styborska
mgr inż. arch.
Author's Orcid number: 0009-0007-2530-2581

West Pomeranian University of Technology in Szczecin, Poland
Faculty of Architecture

ABSTRACT

The article examines the impact of technological threats on the design, construction, and use of multifamily residential buildings, which, according to the *Global Risk Report 2023*, are critical to the current and future functioning of society. In an era of rapid technological advancement, cybersecurity has become a significant factor influencing both the design and usage of residential units. The study employs a range of methodologies, including literature review and risk analysis, to provide a comprehensive perspective on the issue. The results yield recommendations related to the planning, design, and operation of buildings that can enhance the resilience of housing infrastructure against technological threats, thereby improving the quality of life for residents.

Key words: risk analysis, technological risks, multi-family housing, internet access analysis.

STRESZCZENIE

Artykuł bada wpływ zagrożeń technologicznych na proces projektowania, budowy oraz użytkowania obiektów zabudowy wielorodzinnej, które zgodnie z Raportem Global Risk 2023 są kluczowe dla obecnego i przyszłego obrazu funkcjonowania świata. W dobie dynamicznego rozwoju cyberbezpieczeństwo staje się czynnikiem wpływającym na proces projektowy i użytkowanie jednostek mieszkalnych. W badaniach zastosowano zróżnicowane metody, w tym analizę literatury oraz analizę ryzyka, co pozwoliło na uzyskanie kompleksowego obrazu zagadnienia. Wyniki tworzą zalecenia związane z planowaniem, projektowaniem i użytkowaniem budynku, które mogą zwiększyć odporność zabudowy na zagrożenia technologiczne, poprawiając jednocześnie jakość życia mieszkańców.

Słowa kluczowe: analiza ryzyka, zagrożenia technologiczne, budownictwo wielorodzinne, analiza dostępu do internetu.

1. INTRODUCTION

On November 17, 2019, in the city of Wuhan, Hubei Province, in central China, an epidemic began, which on March 11, 2020, the World Health Organization (WHO) recognized as the COVID-19 pandemic - an event whose consequences no one could have predicted. Restrictions introduced by individual countries, including restrictions on leaving homes or the closure of services and workplaces, meant that the end of the lockdown and the return to everyday life differed in many aspects from the times before the threat of the virus. Countries are entering new conflicts, and global warming is already a fact and all living creatures will have to adapt to functioning in a climate at least 1.5 degrees Celsius higher (Bayley, 2022). In addition to the growing geopolitical, economic and climatic challenges, the development of new technologies is causing the world both excitement and anxiety, and the importance of this issue is emphasized by the theme of the World Economic Forum in Davos in 2023.

Digital tools are playing an increasingly significant role in the functioning of cities and will be crucial in developing future solutions. Smart urban centers and buildings have become commonplace, and the integration of digital tools as essential components of urban and architectural projects is becoming more widespread. Notable examples include digital twins, which enable the creation of virtual representations of physical objects and urban spaces. These twins integrate data from the Internet of Things (IoT), artificial intelligence, and cloud platforms, allowing for detailed analysis, condition simulations, and dynamic, real-time management of urban infrastructure. This facilitates traffic modeling, noise monitoring, and pollution level assessment (Hämäläinen, 2020). Another important tool is Building Information Modeling (BIM), which, by creating three-dimensional models of structures, minimizes coordination errors between various disciplines during construction and serves as a valuable information source for post-construction building management, including infrastructure monitoring and energy efficiency support (Beet, Borman, Koch, König, 2018).

Investigating the relationship between digital technologies and architecture, one of the critical questions should be issues related to security. For instance, digital twins rely on extensive datasets collected from IoT devices and sensors, which may exclude individuals without access to technology. This data exclusion can lead to unequal representations of certain social groups, potentially resulting in discrimination or flawed planning decisions (The MIT Norman B. Leventhal Center for Advanced Urbanism, 2022). In the case of architectural structures, Building Information Modeling (BIM) can present risks regarding the privacy of users' data, including sensitive information about their presence and behaviors (Bakar, Ghapar, Jørgensen, Sameon, Yussof, 2024).

Artificial intelligence and automation have been transforming technological progress for many years; however, the release of ChatGPT by OpenAI in 2022 has accelerated this development at an unprecedented pace. In the era of AI growth, designers are expected to focus even more on human-centered approaches, where the quality of their work is determined by nuances, as many answers can now be obtained with a single click (Lundeholm, 2023). Real risks necessitate new approaches to space creation, impacting society, the natural environment, and culture.

This study focuses on multifamily residential buildings, which shape urban spaces significantly and directly affect individuals as social beings. Housing plays a crucial role in human life, providing security, psychological comfort, privacy, independence, a sense of belonging, personal development, and social support.

The objective of this article is to verify the relationship between multifamily residential buildings and potential risks posed by technological advancements in the design, construction, and usage processes, as well as to identify preventive measures that could influence the shaping of building structures and shared spaces. The research methodology employed allows for a comprehensive understanding of the phenomenon under study. This choice was motivated by the desire to grasp both theoretical aspects of threats and their practical implications on the design process and building usage. The starting point for the article was an analysis of the *Global Risk Report* 2023. Based on this, categories of technological threats were identified and analyzed through research literature, revealing a prevalence of publications by governmental organizations focused on social housing and

significant gaps regarding protection against technological threats in commercial buildings of various standards.

2. RESEARCH MATERIALS AND METHODS

The aim of this study is to analyze the impact of technological threats on the design, construction, and usage processes of multifamily residential buildings, while also assessing the relevance of such analyses. The first step in the research methodology involved identifying technological risks associated with multifamily housing, presented in Section 3.1. The author uses categories of technological threats listed in Table 1: *Links between the Effects of Emerging Information Technologies and Multifamily Housing Issues*. These categories, highlighted in the *Global Risk Report 2023*, are considered crucial for the future functioning of society. Based on interviews with experts in multifamily architectural design, the author identifies those most relevant to the study (Table 1).

The literature review (Section 3.2) constitutes the next stage of research, aimed at identifying existing findings on the impact of digital technologies and cyber threats on various phases of the building life cycle. This stage employs a systematic approach, encompassing reviews of scientific publications and industry reports, with a focus on research related to digital exclusion and cybercrime that may influence the design of multifamily structures. This analysis enables the identification of technological threats and their implications, forming the basis for the planned risk analysis.

In Section 3.3, the author applies a quality management-based research method known as Failure Mode and Effects Analysis (FMEA) to analyze risks and their impacts on the design, construction, and operation of architectural structures. FMEA, developed in the United States in the 1950s as a classified method for military, aviation, and aerospace purposes, was declassified and popularized in the U.S. in the 1970s and 1980s, and later in Europe. It is currently used across numerous industries, allowing for continuous process improvement and quality management. Since the 1990s, it has also been used as a risk management tool (Kowalik, 2018). Figure 1 illustrates the FMEA process when applied to buildings. Based on this framework, a tailored analysis is designed to identify risk categories relevant to multifamily housing during the design, construction, and operational phases (Table 2). The proposed method is implemented in a selected multifamily housing complex (Table 3), with findings intended to serve as guidelines for similar projects.

The conducted research will evaluate the need for further analyses related to technological threats throughout the life cycle of multifamily buildings. The author will address whether there are protective measures to safeguard residents of multifamily complexes from technological threats through design interventions and an appropriate building management strategy.

3. RESEARCH

3.1 Adverse outcomes of frontier technologies

The term "Adverse outcomes of frontier technologies" refers to potential negative effects or consequences related to the use of innovative information technologies, including: AI, Internet of Things (IoT), brain-computer interfaces (IMK), biotechnology, quantum computing, metaworld (World Economic Forum, 2023). According to the Global Threats Report 2023 (World Economic Forum, 2023), the following effects of these activities are indicated, which are presented and categorized in the table (Tab. 1). Technological threats for which there are connections with the subject of multi-family construction will be analyzed in the next part of the article.

Tab. 1. Linking the effects of the development of innovative information technologies with the topic of multi-family construction. Source: by autor

Name of the risk (development effects adverse outcomes of frontier technologies)	Risk category	Connections with the subject of multi-family building complexes
Breakdown of critical information infrastructure	technologiczne	-
Dezinformation	socjologiczne	-
Terrorist attacks	geopolityczne	+
Cyfrowe wykluczenie	technologiczne	+
Digital power concentration	technologiczne	-
Widespread cybercrime and cyber insecurity	technologiczne	+

* Risk categories: technological, social, economical, environmental, geopolitical (World Economic Forum, 2023)

3.2 Literature analysis

3.2.1 Digital inequality- literature analysis in the context of connections between the issue and the design of multi-family building complexes

The term "Digital inequality" refers to people or communities with limited access to digital technologies. Exclusion from the benefits of, among others: availability of the Internet and the ability to use these tools leads to an increase in social, economic and educational inequalities (World Economic Forum, 2023).

The problem of digital exclusion in the context of modern multi-family construction appears in scientific literature even before 2021 and the emergence of the COVID 19 pandemic. Already in 2016, the importance of access to the Internet, and in particular access to broadband Internet, is emphasized. The development of this tool since the 1990s has been rapid and its capabilities began to be used very quickly in the fields of education, employment, health, social services and the creation and dissemination of knowledge (Celeste, DiMagio, Hargittai, Shafer, 2003). At the same time, this has led to growing social disparities, because it is the neediest people, young people from families with limited income, who have become defenseless in this area, and the long-term effects of living in technology-enriched education will impact their further development. There are 5 key aspects of digital exclusion (Peppel, Computing, 2016):

– differences in equipment, i.e. technologies enabling access to the Internet,
– autonomy in using the Internet,
– differences in the level of skills in using the Internet and technologies enabling its access,
– differences in the level of social support, including help from family, friends and public institutions,
– the purposes of using digital technologies, including the ways in which people use the Internet to increase their economic productivity and political and social capital.

In the context of multifamily housing, autonomy in Internet access can directly impact the design process, necessitating the creation of infrastructure that allows for individual connections and customized configurations. Regardless of the chosen service provider, designers must incorporate independent connections for each residential unit and support technology that ensures fast and stable Internet access. This includes planning for access points, fiber-optic installations, or 5G systems, which, in turn, influence the spatial arrangement of the building and the layout of electrical and network installations.Home Internet access enables increased control over the environment, more frequent usage, and thus the potential for education, information acquisition, and income generation. For families, establishing a safe digital space and controlling access to appropriate content is also a significant consideration (Inglot-Brzęk, E., 2011).

The trends mentioned above accelerated on an unprecedented scale in a very short time with the outbreak of the Covid 19 pandemic. The need to switch to online services made digital access an indispensable tool for maintaining health, economic well-being, and participation. in social life. This time, the previously mentioned exclusion group was joined by seniors for whom telemedicine has become a common model for managing their health problems (Asher, Arnold, Nassau-Brownstone, 2021).

Members of the Affordable Housing for the Future (SAHF) organization, through their research and experience, see the key connection between digital accessibility, health and wealth status. They propose short-term solutions, including a program for renting mobile devices and hotspots, as well as long-term solutions interfering with the management and structure of complexes of multi-family facilities consisting of economically available apartments aimed at remedying digital exclusion (Asher, Arnold, Nassau-Brownstone, 2021).

3.2.2 Widespread cybercrime and cyber insecurity- literature analysis in the context of connections between the issue and the design of multi-family building complexes

The term " widespread cybercrime and cyber insecurity" encompass various forms of criminal activity conducted through computer networks and associated threats to data security, information systems, and Internet users (World Economic Forum, 2023). In the context of multifamily housing, a notable example of cybercrime is the incident that occurred in 2016 in Lappeenranta, Eastern Finland, where hackers used a Distributed Denial of Service (DDOS) attack to disable the heating system and hot water supply in two smart apartment buildings.

In recent years, the number of cyberattacks has increased, largely influenced by the COVID-19 pandemic (Scott, 2023). This surge has led to heightened attention to digital data protection and network security across various sectors in construction. However, literature reviews indicate that multifamily buildings have either not adopted these strategies or have done so only minimally (Scott, 2023). During the design phase, architects, as project coordinators across multiple disciplines, and engineers have the opportunity to integrate cybersecurity considerations into the execution or technical design phase and provide appropriate usage guidelines for the occupants.

In reviewing scholarly publications, the author did not find articles directly addressing the general lack of cybersecurity in the context of multifamily housing. However, numerous references to the dangers posed by cybercrime to residential properties can be found in public media.

“Cybercrime is a growing problem in an increasingly connected world” (European Parliament 2020). Thanks to the Internet of Things (IoT), which refers to a network of devices connected to the Internet, we can open and close doors or garage gates, check monitoring on our phones, and even heat the oven on the way home, in addition to electronic baby monitors, refrigerators, vacuum cleaners and many other smart devices (Alahi, Ghayvat, Gui, Liu, Mukhopadhyay, 2015). This creates an information network not only of individuals, but also of systems and devices that can operate independently of humans (Kabrońska, Wysocki, 2016). If a household has many connected devices, cybercriminals, by taking over one of them, have access to a rich database related to the functioning of their owner, which may facilitate a potential attack or attempt to extort data (Blaicke, Rot, 2016).

Another issue is BMS (Building Management System), i.e. a completely automated system for managing building installations, which is used more and more often in the case of energy-efficient facilities (Dechnik, Moskwa, 2020). Taking control of the systems governing ventilation, air conditioning, temperature, or energy can immediately force residents to evacuate, thereby facilitating unauthorized access to the building for a potential intruder.

3.3 A method for validating threats in the process of design, construction and use of buildings.

To properly identify potential risks and threats, the author used FMEA (Failure Mode and Effects Analysis). The method is standardly used to analyze the types and effects of defects on a product or product creation process. There are numerous schemes of the FMEA process, the basic one of which is divided into 5 stages (Rychły-Lipińska, 2007):

1. Assembling a team: 4-8 people with a guide and (possibly) an expert;
2. Identification of product/process components;
3. Developing a list of possible errors;
4. Indication of possible effects of the developed errors;
5. Listing possible causes of the errors developed;

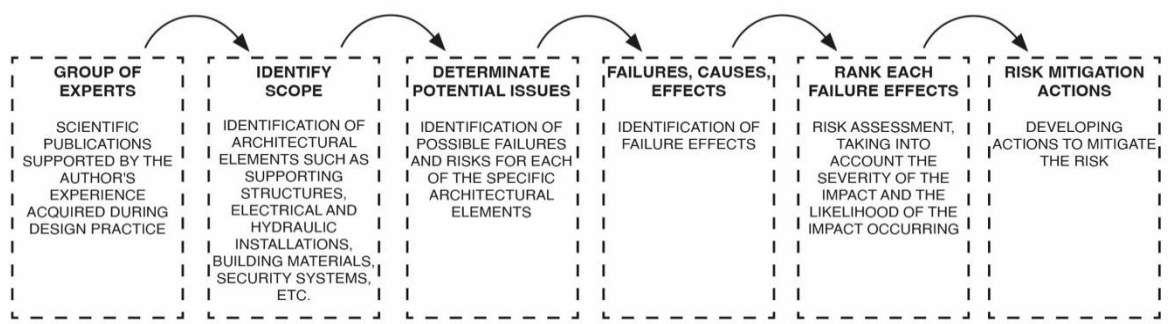


Fig. 1. Adaptation of the FMEA method process to identify risks and threats in the process of design, construction and use of buildings. Source: by author

Figure 1 illustrates the adaptation of the FMEA method to identify risks and threats within the design, construction, and operation processes of buildings, according to established categories. Based on this framework, a study was developed to identify risks associated with digital exclusion and cybercrime for multifamily residential buildings (Table 2). All aspects indicated in Table 2 were analyzed, even though they may not be applicable to the studied area.

Tab. 2. FMEA analysis is aimed at identifying the risk of digital exclusion and cybercrime in the process of design, construction and use of multi-family facilities. Source: by author

Identyfication of architectural elements	**Identification of failures and risks**	**Identification effects of failure**	**Risk assessment**	
			Severity of the effect *	**Probability of an effect occurring ****
DIGITAL INEQUALITY				
Telecommunications infrastructure (internal installations)	Failure to plan appropriate telecommunications infrastructure for the entire facility at the detailed design stage.	It is not possible to connect the housing unit to a permanent connection.	high	high
Telecommunications infrastructure (external networks)	The location of the multi-family building makes it impossible to connect the facility to the telecommunications network due to infrastructure deficiencies.	Long-term lack of access to the Internet by residents, which hinders communication, remote work and access to information.	high	low *(for urbanized areas)* high *(for rural areas)*
Common spaces of the building	Lack of external or internal common spaces enabling open access to the Internet.	Exclusion from access to the Internet of the neediest people who cannot afford to connect to telecommunications services under individual contracts.	high *(for the most at-risk groups)*	high *(for the most at-risk groups)*
Building management (administarion)	It is not possible to rent equipment enabling free access to the Internet.	Exclusion from access to the Internet of the neediest people who cannot afford to purchase equipment providing free access to the Internet.	high *(for the most at-risk groups)*	high *(for the most at-risk groups)*
WIDESPREAD CYBERCRIME AND CYBER INSECURITY				

Identyfication of architectural elements	Identification of failures and risks	Identification effects of failure	Risk assessment	
			Severity of the effect *	Probability of an effect occurring **
Building management systems (BMS)	Taking control of the building management system (BMS) and changing settings such as lighting, heating, ventilation.	Disruption to the normal functioning of the building, for example changes in temperature, lighting or access to rooms.	high	high
Smart home/building systems (IoT) such as smart locks, thermostats	Taking control of systems allowing unauthorized access to the building or changing settings without the consent of residents.	Violating residents' privacy by monitoring their activities or stealing personal information.	high	high
Monitoring and access control systems	Theft of data such as identification data or room plans.	Potential threat to the physical safety of residents through unauthorized access to the building.	high	high

* everity of the effect: low, medium, heigh

** probability of an effect occurring: low, medium, heigh

3.4 CASE STUDY

3.4.1 Case study - characteristics of the research area

As part of the analysis of broadband Internet availability maps (Ministerstwo Cyfryzacji, 2024) for multi-family buildings in Szczecin (Fig.2), the research area was narrowed down to downtown buildings. Two types of quarters are specified:

– with Internet access only in buildings adjacent to the street, outbuildings without Internet access,
– with Internet access for the entire building of the quarter.

Further research identified that quarters distinguished in the urban fabric by comprehensive access to the network were subject to comprehensive revitalizations carried out as part of urban social programs or private activities.

FIg. 2. Internet availability map for a part of the downtown area of Szczecin. Source: by author (Ministerstwo Cyfryzacji 2024)
Ryc.2. Mapa dostępności Internetu szerokopasmowego dla fragmentu śródmieścia miasta Szczecin. Źródło: opracowanie autorki (Ministerstwo Cyfryzacji 2024)

The analysis of the identification of the risk of digital exclusion and cybercrime was performed on quarter 23 (Fig. 3), surrounded by Aleja Wojska Polskiego and the streets Bohaterów Getta Warszawskiego, Królowej Jadwigi and Księdza Piotra Ściegiennego. This area was revitalized in 2012-2016, and its assumptions were: raising the standard and quality of life of the local community, improving the technical condition of the urban fabric, increasing the energy efficiency of buildings, social activities based on the activity of the Social Day Support Center, activating residents in the area of taking care of the nearest surroundings and the building, protecting historical and cultural values, and economic revival (Social Housing Association in Szczecin, 2016). As part of the project activities, the outbuildings, which caused poor lighting in the courtyards of the quarter, were partially eliminated. A new facility was proposed, connecting the abandoned outbuildings and at the same time complementing the line of development along Królowej Jadwigi Street. Thanks to its foundation on pillars, the building created a pedestrian and vehicle passage connecting common spaces, thus creating access to service premises and economic services for the interior of the block.

3.4.2 Application of the method of validation of technological threats in the process of designing, building and using newly constructed facilities and common spaces of Quarter 23 in Szczecin

The author obtained the necessary data for the correct application of the threat validation method during an interview with the designers of the quarter (Studio a4), who permanently cooperate with the Szczecin TBS (Social Building Society), which is responsible for carrying out the revitalization.

Tab. 3. Identification of the risk of digital exclusion and cybercrime in the design, construction and use process for Quarter 23 in Szczecin. Źródło: by autor

Identification of failures and risks	**dentification of whether there are specific failures or risks for the designated category within Quarter 23 in Szczecin.**	**Preventive and corrective actions**	**Action category**
DIGITAL INEQUALITY			
Failure to plan appropriate telecommunications infrastructure for the entire facility at the detailed design stage.	Telecommunications infrastructure designed correctly.	Not required	design stage
The location of the multi-family building makes it impossible to connect the facility to the telecommunications network due to infrastructure deficiencies.	The location of the building allows the buildings included in the quarters to be connected to broadband Internet.	Not required	design stage
Lack of external or internal common spaces enabling open access to the Internet.	Common spaces have been revitalized and adapted to the needs of residents (Fig.4). Apart from the external zones, in one of the buildings focused on senior policy, meeting places (Fig.5) have been designed, but they do not have open access to the Internet.	Introduction of wireless and free Internet zones in common spaces.	design stage + building use
It is not possible to rent equipment enabling free access to the Internet.	No activities enabling equipment rental were demonstrated.		użytkowanie budynku
WIDESPREAD CYBERCRIME AND CYBER INSECURITY			
Taking control of the building management system (BMS) and changing settings such as lighting, heating, ventilation.	Lack of BMS system	Not applicable	Not applicable
Taking control of systems allowing unauthorized access to the building or changing settings without the consent of residents.	Lack of intelligent building systems	Not applicable	Not applicable
Theft of data such as identification data or room plans.	Lack of monitoring systems	Not applicable	Not applicable

Fig. 3. View of quarter 23 from the side of Królowej Jadwigi Street. Source: photo made by author, 2024

Ryc. 3. T Widok elewacji kwartału 23 od strony ul. Królowej Jadwigi. Źródło: fotografia wykonana przez autorkę, 2024

Fig. 4. Interior of quarter 23. Source: photo made by author, 2024

Ryc. 4. Wnętrze kwartału 23. Źródło: fotografia wykonana przez autorkę, 2024

Fig. 5. Inside common space of quarter 23. Source: photo made by author, 2024

Ryc. 5. Wewnętrzne części wspólne kwartału 23. Źródło: fotografia wykonana przez autorkę, 2024

4. RESULTS

The method for validating technological threats in the design, construction, and use of multi-family buildings (Table 2) demonstrated differences in their design and utilization depending on their intended purpose. Facilities with social or assisted living[1] housing are often used by groups most vulnerable to digital exclusion and limited access to broadband networks (Peppel, Computing, 2016). For them, a crucial issue is the design of infrastructure for external and internal common spaces with universal internet access. Simultaneously, during the planning of such investments, municipalities and their subordinate units responsible for these projects should assess the telecommunication capabilities and service coverage of operators for the area under development when allocating suitable land for multi-family residential buildings. It is also worth emphasizing the importance of urban planning regulations (aligned with the planning laws of the given region) in the process of creating areas designated for multi-family residential housing. This ensures not only that they are equipped with appropriate infrastructure but also meet broader development standards.

Developer High-standard developer properties, especially those equipped with automation systems for managing ventilation, heating, access control, and monitoring, are increasingly exposed to hacking attempts, data breaches, and theft through network security vulnerabilities. In such cases, particular attention should be paid to the telecommunication design, which should include guidelines for protecting residents at the network management level. The building design process should take into account the entire lifecycle of the property, making considerations related to its usage an integral component. This includes educational initiatives targeted at residents and estate regulations that outline the principles for the safe use of digital infrastructure, supporting the protection of individual users (Scott, 2023).

The analysis of digital exclusion and cybersecurity risks for the revitalized Quarter 23 (Table 3) demonstrated proper preparation by architects of the project's execution plan, particularly regarding the telecommunication and functional infrastructure of the quarter. Based on the identified needs of

[1] Apartments designed for seniors and individuals with chronic illnesses who wish to live independently but require daily support.

residents, management should consider implementing measures to reduce the risk of digital exclusion, such as public Wi-Fi hotspot zones or the short- and long-term loan of devices that allow unrestricted internet access. In mitigating digital exclusion, technical support for the most vulnerable groups should also be considered, including assistance with device configuration, resolving internet access issues, and using applications.

The analyzed case excludes the risk of cybercrime due to the absence of intelligent building management systems in the quarter. However, as technology progresses and residences become equipped with more smart devices, it is important to provide education for residents and collaborate with reputable service providers who ensure high-quality services and possess up-to-date knowledge about the latest threats and solutions.

In summary, the identified technological threats are not critical for shaping multi-family buildings, apart from the need for proper design of public spaces. However, considering contemporary challenges such as environmental concerns, social and economic issues, and technological risks (World Economic Forum, 2024), architects should view architectural structures not only from the perspective of their form. The European Parliament emphasizes the importance of the full lifecycle assessment (LCA) of construction sector products, including manufacturing, usage, end-of-life, and recycling potential. This approach is one of the fundamental tools for reducing carbon dioxide emissions. Additionally, research indicates that decisions made at the early design stage have the most significant impact on the sustainability of a building, and integrating LCA methodology with BIM technology yields the best results. In this context, identified technological threats to multi-family housing are among the key factors that should be considered during the design and implementation stages.

5. DISCUSSION AND CONCLUSION

The selected case study of the redevelopment of Szczecin's Quarter 23 illustrates a comprehensive approach to revitalization. This approach includes leveling opportunities for residents, thereby preventing exclusion by ensuring internet access across the entire area and creating a functional structure that enables the most vulnerable groups to use the network. According to Louis Suh, a senior architect at the New York branch of the Danish firm Henning Larsen, a growing trend in architecture is adaptive programs focusing on reuse and expansion. The future lies in transforming existing structures without significant carbon emissions, which are typically associated with new construction projects (Lundeholm, Suh, 2023). Considering the scale of the problem of inadequate access to cable and fiber-optic internet in the tenement courtyards of Szczecin's downtown area, similar revitalization efforts should be undertaken on a much larger scale.

In Polish literature, the topic of preventing technological threats within architectural activities is rarely discussed. Numerous publications address the issue of digital exclusion, focusing on disparities in access to technology and the skills required to use it (Batorski, 2009), but without linking it to residential construction. The topic is more extensively discussed in international literature, which emphasizes the importance of autonomy in internet usage and proper planning of housing infrastructure (Peppel, Computing, 2016), as well as the thoughtful design of shared external and internal spaces (Asher, Arnold, Nassau-Brownstone, 2021). In the context of cybercrime, both Polish and international literature highlight the risks associated with using IoT and BMS systems and recommend preventive measures to protect private clients and providers (Blaicke, Rot, 2016). However, it remains unclear who, apart from the individual user, should bear responsibility for implementing adequate security measures—whether it should be the architect, building manager, or interior designer. This article demonstrates that comprehensive and top-down initiatives yield the best results, thereby underscoring the need for regulation of this issue.

In summary, the article performed a risk analysis using the FMEA method, which identified major threats and proposed countermeasures. A practical example is Szczecin's Quarter 23, where appropriate telecommunication infrastructure and shared external and internal spaces were planned to reduce the risk of digital exclusion. The findings suggest the necessity of developing regulations for digital security at the planning and design stages, as well as user education to enhance the safety of residents in multi-family housing complexes. Technological threats were identified based on the

Global Risks Report 2023 (World Economic Forum, 2023). As the World Economic Forum publishes this report annually, the importance of verifying and updating the state of research cannot be overstated.

Architects' competencies evolve alongside technological advancements, changing social needs, and emerging challenges in design and construction. The process of creating buildings increasingly requires collaboration with a broader range of specialists, necessitating the coordination of more issues during the design process. Technological threats represent a new area that should be integrated into the processes of designing, constructing, and operating architecture, including multi-family housing developments.

ANALIZA WPŁYWU ZAGROŻEŃ TECHNOLOGICZNYCH NA ZABUDOWĘ WIELORODZINNĄ

1. WPROWADZENIE

17 listopada 2019 w mieście Wuhan, w prowincji Hubei, w środkowych Chinach rozpoczęła się epidemia, którą 11 marca 2020 r. Światowa Organizacja Zdrowia (WHO) uznała za pandemię COVID-19 – wydarzenie, którego skutków nikt nie mógł przewidzieć. Restrykcje wprowadzane przez poszczególne Państwa, w tym ograniczenia w wychodzeniu z domów czy zamknięcie usług i zakładów pracy spowodowały, iż zakończenie czasów zamknięcia i powrót do codzienności różnił się w wielu aspektach od czasów sprzed zagrożenia wirusem. Państwa wchodzą w coraz to nowe konflikty, a globalne ocieplenie to już fakt i wszystkie istoty żywe będą musiały przystosować się do funkcjonowania w klimacie min. 1,5 stopnia Celsjusza wyższym (Bayley, 2022). Oprócz narastających wyzwań geopolitycznych, ekonomicznych czy klimatycznych rozwój nowych technologii wprowadza świat zarówno w ekscytacje jak i niepokój, a znaczenie tego zagadnienia podkreśla tematyka obrad Światowego Forum Ekonomicznego w Davos z 2023 r.

Narzędzia cyfrowe odgrywają coraz większą rolę w funkcjonowaniu miast i będą kluczowe w opracowywaniu rozwiązań na przyszłość. Inteligentne ośrodki miejskie i budynki to już codzienność, a koncepcje wykorzystania narzędzi cyfrowych jako integralnych składowych projektów urbanistycznych i architektonicznych stają się coraz powszechniejsze. Warto tutaj wymienić np. cyfrowe bliźniaki, które umożliwiają tworzenie wirtualnych reprezentacji fizycznych obiektów i przestrzeni miejskich. Integrują one dane pochodzące z Internetu Rzeczy (IoT), sztucznej inteligencji oraz platform chmurowych, co pozwala na szczegółową analizę i symulację warunków oraz dynamiczne zarządzanie infrastrukturą miejską w czasie rzeczywistym co pozwala na modelowanie ruchu ulicznego, monitorowanie hałasu i poziomu zanieczyszczeń (Hämäläinen, 2020) lub Modelowanie Informacji o budynkach (BIM), który dzięki tworzeniu trójwymiarowych modeli obiektów minimalizuje ryzyko błędów podczas koordynacji branżowej, a po zakończeniu budowy wykorzystywany jest jako źródło informacji do zarządzania budynkiem, w tym kontroli sekcji instalacyjnej oraz wsparciem efektywności energetycznej (Beet, Borman, Koch, König, 2018).

Badając związek technologii cyfrowych z architekturą jednym z kluczowych pytań powinny być zagadnienia bezpieczeństwa. Przykładowo cyfrowe bliźniaki opierają się na dużych zbiorach danych zbieranych z urządzeń IoT i czujników, co może pomijać osoby bez dostępu do technologii. To

wykluczenie danych prowadzi do nierównych reprezentacji niektórych grup społecznych, co może skutkować dyskryminacją lub błędnymi decyzjami planistycznymi (The MIT Norman B. Leventhal Center for Advanced Urbanism 2022). W przypadku obiektów architektonicznych Modelowanie Informacji o budynkach (BIM) może stwarzać zagrożenia, jeżeli chodzi o prywatność danych o ich użytkownikach, w tym danych wrażliwych, informacjami o ich obecności i zachowaniach (Bakar, Ghapar, Jørgensen, Sameon, Yussof 2024). Sztuczna inteligencja i automatyzacja od wielu lat rewolucjonizują postęp technologiczny, jednak udostępnienie narzędzia ChatGPT przez OpenAI w 2022 r., spowodowało przyśpieszanie tempa jego rozwoju na niespotykaną dotychczas skalę.

W dobie rozwoju sztucznej inteligencji rolą projektantów jest zwrócenie jeszcze większej uwagi na człowieka, a o jakości ich pracy decydują niuanse, gdyż odpowiedzi na wiele pytań można otrzymać za pomocą jednego przycisku (Lundeholm, 2023). Realne zagrożenia wymagają nowego podejścia do kreowania przestrzeni, które mogą mieć wpływ na społeczeństwo, środowisko naturalne oraz kulturę. Jako obszar badań wybrano zabudowę mieszkaniową wielorodzinną, gdyż to ona w dużej mierze kształtuje przestrzenie miejskie oraz ma bezpośredni wpływ na człowieka jako jednostkę. Mieszkanie odgrywa kluczową rolę w życiu człowieka, zapewniając mu bezpieczeństwo, komfort psychiczny, prywatność, samodzielność, poczucie przynależności, rozwój osobisty oraz wsparcie społeczne.

Celem artykułu jest weryfikacja związku z zabudową wielorodzinną potencjalnego ryzyka i zagrożeń, jakie niesie za sobą rozwój technologiczny dla procesu projektowania, budowy oraz użytkowania osiedli wielorodzinnych oraz wskazanie działań zapobiegawczych mających wpływ na kształtowanie zabudowy i części wspólnych. Zastosowano metody badawcze, które pozwoliły na uzyskanie kompleksowego obrazu badanego zjawiska. Wybór podyktowany był chęcią zrozumienia teoretycznych aspektów zagrożeń, a także praktycznych implikacji ich wpływu na proces projektowy oraz użytkowanie obiektu. Punktem wyjściowym dla artykułu była analiza raportu zagrożeń globalnych (World Economic Forum 2023). Na jej podstawie wyszczególniono kategorie zagrożeń technologicznych, które zostały poddane analizie literatury badawczej. Wykazała ona przewagę publikacji autorstwa organizacji rządowych zajmujących się problematyką budownictwa społecznego oraz wyraźne braki w tematyce ochrony przed zagrożeniami technologicznymi obiektów deweloperskich o różnym standardzie.

2. MATERIAŁY I METODY BADAWCZE

Celem badania jest analiza wpływu zagrożeń technologicznych na proces projektowania, budowy oraz użytkowania zabudowy wielorodzinnej, z jednoczesnym zweryfikowaniem zasadności tego typu analiz. Pierwszym krokiem procesu metodologii badawczej była identyfikacja niebezpieczeństw technologicznych powiązanych z budownictwem wielorodzinnym znajdująca się w rozdziale 3.1. Autorka, posługuje się kategoriami niebezpieczeństw technologicznych, wymienionymi w tabeli: Powiązań skutków rozwoju nowatorskich technologii informatycznych z tematyką budownictwa wielorodzinnego (tab.1). Kategorie wyszczególniono w raporcie zagrożeń globalnych 2023 (World Economic Forum, 2023), jako kluczowe dla przyszłości funkcjonowania świata. Na podstawie wywiadów z ekspertami z dziedziny projektowania architektury obiektów wielorodzinnych autorka identyfikuje te powiązane z właściwą tematyką (tab. 1).

Przegląd literatury (rozdział 3.2) stanowi kolejny etap badania, mający na celu identyfikację istniejących wyników badań dotyczących wpływu technologii cyfrowych i zagrożeń cybernetycznych na różne fazy cyklu życia budynków. W ramach tej części zastosowano podejście systematyczne, które obejmuje przegląd publikacji naukowych oraz raportów branżowych. Szczególną uwagę zwrócono na badania poświęcone wykluczeniu cyfrowemu oraz przestępczości internetowej mogącej mieć wpływ na projektowanie obiektów wielorodzinnych. Dzięki analizie możliwe jest rozpoznanie zagrożeń technologicznych oraz ich skutków, które są podstawą do przeprowadzenia badania analizy ryzyka i jego skutków.

W rozdziale 3.3 autorka stosuje metodę badawczą opartą na analizie zarządzania jakością produktu (FMEA - Failure Mode and Effects Analysis), którą dostosowuje do analizy ryzyka i jego skutków dla projektowania, budowy i użytkowania obiektów architektonicznych. Metodę opracowano w USA w

latach pięćdziesiątych jako zatajona metoda dla potrzeb wojska, lotnictwa i astronautyki. Po jej oddtajeniu w latach siedemdziesiątych i osiemdziesiątych spopularyzowano ją w USA, a następnie w Europie. Obecnie używana jest w wielu branżach umożliwiając ciągłe doskonalenie procesu technologicznego i zarządzanie jakością. Od lat dziewięćdziesiątych wykorzystuje się ją jako narzędzie do zarządzania ryzykiem (Kowalik, 2018). Schemat (ryc.1) wyjaśnia aplikację procesu metody FMEA, w przypadku, gdy jej produktem jest budynek. Na tej podstawie, projektuje się właściwą analizę mająca na celu identyfikację ryzyka dla kategorii, dla których istnieje powiązanie z budownictwem wielorodzinnym w procesie projektowania, budowy i użytkowania obiektów wielorodzinnych (tab.2). Projektowana metoda jest następnie aplikowana na wybranym przypadku zespołu zabudowy wielorodzinnej (tab.3). Wnioski z analizy będą mogły służyć jako wytyczne dla podobnych realizacji.

Przeprowadzone badania pozwolą na dokonanie oceny zasadności prowadzenia dalszych analiz związanych z zagrożeniami technologicznymi w cyklu życia budynków wielorodzinnych. Autorka odpowie na pytanie, czy istnieją metody ochrony mieszkańców zespołów obiektów wielorodzinnych przed zagrożeniami technologicznymi, dzięki działaniom projektowym oraz właściwej strategii zarządzania obiektem i jego społecznością.

3. REZULTATY – ANALIZA ZAGROŻEŃ TECHNOLOGICZNYCH

3.1 Kategorie zagrożeń technologicznych

Termin „negatywne skutki nowatorskich technologii" odnosi się do narzędzi informatycznych w tym: AI, Internet rzeczy (IoT), interfejsy mózg-komputer (IMK), biotechnologia, informatyka kwantowa, metaświat (World Economic Forum, 2023). Zgodnie z raportem zagrożeń globalnych 2023 (World Economic Forum, 2023) wskazuje się następujące skutki tych działań, które zostały przedstawione i skategoryzowane w tabeli (Tab.1). Związek zagrożeń technologicznych, dla których istnieją powiązania z tematyką budownictwa wielorodzinnego zostanie przeanalizowany w kolejnej części artykułu.

Tab. 1. Powiązanie skutków rozwoju nowatorskich technologii informatycznych z tematyką budownictwa wielorodzinnego. Źródło: opracowanie własne autorki

Nazwa zagrożenia (World Economic Forum, 2023)	**Kategoria zagrożenia**	**Powiązania z tematyką budownictwa wielorodzinnego**
Możliwość awarii systemów informatycznych kluczowych dla sprawnego funkcjonowania społeczeństwa i gospodarki	technologiczne	–
Dezinformacja	społeczne	-
Ataki terrorystyczne	geopolityczne	-
Cyfrowe wykluczenie	technologiczne	+
Koncentracja kluczowych zasobów cyfrowych	technologiczne	-
Powszechność przestępczości internetowej	technologiczne	+

* kategorie zagrożeń: technologiczne, geopolityczne, społeczne, ekonomiczne, klimatyczne (World Economic Forum, 2023)

3.2. Analiza literatury

3.2.1. Cyfrowe wykluczenie

Termin "wykluczenia cyfrowego" odnosi się do osób lub społeczności mających ograniczony dostęp do technologii cyfrowych. Wykluczenie z korzyści jakie daje m. in. dostępność do Internetu oraz

umiejętności korzystania z tych narzędzi prowadzi do wzrostu nierówności społecznych, gospodarczych oraz edukacyjnych (World Economic Forum, 2023).

Problem wykluczenia cyfrowego w kontekście nowoczesnego budownictwa wielorodzinnego w literaturze naukowej pojawia się jeszcze przed rokiem 2021 i pojawieniem się pandemii COVID 19. Już 2016 r. podkreśla się istotę dostępu do Internetu, a w szczególności dostępu do Internetu szerokopasmowego. Rozwój tego narzędzia od lat 90 był błyskawiczny i bardzo szybko zaczęto wykorzystywać jego możliwości w zakresie edukacji, zatrudnienia, zdrowia, usług socjalnych oraz tworzenia i rozpowszechniania wiedzy (Celeste, DiMagio, Hargittai, Shafer, 2003). Doprowadziło to jednocześnie do rosnących dysproporcji społecznych, gdyż to właśnie osoby najbardziej potrzebujące, ludzie młodzi pochodzący z rodzin o ograniczonych dochodach stały się bezbronne w tym obszarze, a długoterminowe skutki życia w edukacji wzbogaconej technologią będą miały wpływ na ich dalszy rozwój. Wyróżnia się 5 kluczowych aspektów wykluczenia cyfrowego (Peppel, Computing, 2016):

- różnice w sprzęcie, t.j. technologie pozwalające na uzyskanie dostępu do Internetu,
- autonomia korzystania z Internetu,
- różnice w poziomie umiejętności korzystania z Internetu i technologii pozwalających na jego dostęp,
- zróżnicowanie w poziomie wsparcia społecznego obejmujące pomoc ze strony rodziny, przyjaciół i instytucji publicznych,
- cele korzystania z technologii cyfrowych obejmujące sposoby, w jakie ludzie korzystają z Internetu w celu zwiększenia swojej produktywności ekonomicznej oraz kapitału politycznego i społecznego.

W kontekście powiązań z budownictwem wielorodzinnym, aspekt autonomii w dostępnie do Internetu może stanowić bezpośredni wpływ na proces projektowy, co oznacza konieczność projektowania infrastruktury umożliwiającej indywidualne połączenia i konfiguracje internetowe. Niezależnie od wyboru dostawcy usług, projektanci muszą uwzględnić niezależne połączenia do każdej jednostki mieszkalnej oraz uwzględnić technologię wspierającą szybki i stabilny Internet. Obejmuje to planowanie punktów dostępowych, instalacji światłowodowych lub systemów 5G, co z kolei wpływa na układ przestrzenny budynku oraz rozplanowanie instalacji elektrycznych i sieciowych. Dostęp do Internetu w domu daje możliwości zwiększonej kontroli nad środowiskiem, większą częstotliwość użytkowania, a co za tym idzie możliwość edukacji, pozyskiwanie informacji oraz zwiększenie zarobków. Jako istotną kwestie dla rodzin wskazuje się także, stworzenie bezpiecznej przestrzeni cyfrowej i kontrola w dostępie do odpowiednich treści (Inglot-Brzęk E. 2011).

Tendencje, o których mowa powyżej przyśpieszyły w niespotykanej dotychczas skali w bardzo krótkim czasie wraz z momentem wybuchu pandemii Covid 19. Konieczność przejścia na usługi internetowe, sprawiła, że dostęp cyfrowy stał się niezbędnym narzędziem do utrzymania zdrowia, ekonomicznego dobrobytu, a także uczestnictwa w życiu społecznym. Tym razem do wcześniej wspomnianej grupy wykluczenia dołączyli seniorzy, dla których telemedycyna stała się powszechnym modelem zarządzania swoimi problemami zdrowotnymi (Asher, Arnold, Nassau-Brownstone, 2021).

Członkowie organizacji Affordable Housing for the Future (SAHF) w swoich badaniach i dzięki swojemu doświadczeniu dostrzegają kluczowe powiązanie między dostępnością cyfrową, zdrowiem i statusem majątkowym. Proponują rozwiązania krótkoterminowe w tym program wypożyczania urządzeń mobilnych i hotspotów oraz długoterminowe ingerujące w zarządzanie i strukturę zespołów obiektów wielorodzinnych składających się z dostępnych ekonomicznie mieszkań mających na celu zaradzeniu wykluczeniu cyfrowemu (Asher, Arnold, Nassau-Brownstone, 2021).

3.2.2. Powszechność przestępczości internetowej i ogólny brak bezpieczeństwa w cyberprzestrzeni

Termin powszechności przestępczości internetowej i ogólnego braku bezpieczeństwa w cyberprzestrzeni, obejmuje różnorodne formy działalności przestępczej prowadzonej za pomocą sieci komputerowych oraz związane z nimi zagrożenia dla bezpieczeństwa danych, systemów informatycznych i użytkowników Internetu (World Economic Forum, 2023). W kontekście budownictwa wielorodzinnego przykładem cyberzbordni może być incydent, który miał miejsce w 2016 r. w mieście

Lappeenranta we wschodniej Finlandii. Hakerzy wykorzystali wówczas atak typu rozproszona odmowa usługi (DDOS), by zablokować system ogrzewania oraz dostawę ciepłej wody w dwóch inteligentnych apartamentowcach.

W ostatnich latach wzrosła ilość cyberataków, co w dużej mierze spowodowane było pandemią COVID -19 (Scott, 2023). Poskutkowało to zwróceniem większej uwagi na ochronę danych cyfrowych oraz połączeń sieciowych w wielu sektorach budownictwa, jednakże analiza literatury wskazuje, że obiekty wielorodzinne nie poddały się tej strategii, lub zrobiły to tylko w niewielkim stopniu (Scott, 2023). W fazie projektowania architekci jako koordynatorzy projektu wielobranżowego oraz inżynierowie mają możliwość uwzględnienia aspektów cyberbezpieczeństwa na etapie projektu wykonawczego lub technicznego, jak również dając odpowiednie wytyczne dla użytkowania obiektu. W ramach analizy publikacji naukowych autorka nie znalazła artykułów, które wprost poruszają problem ogólnego braku bezpieczeństwa w cyberprzestrzeni w powiązaniu z tematyką zabudowy wielorodzinnej. Jednakże, w mediach publicystycznych możemy spotkać liczne nawiązania do niebezpieczeństwa, jaki tworzy przestępczość internetowa dla obiektów mieszkaniowych.

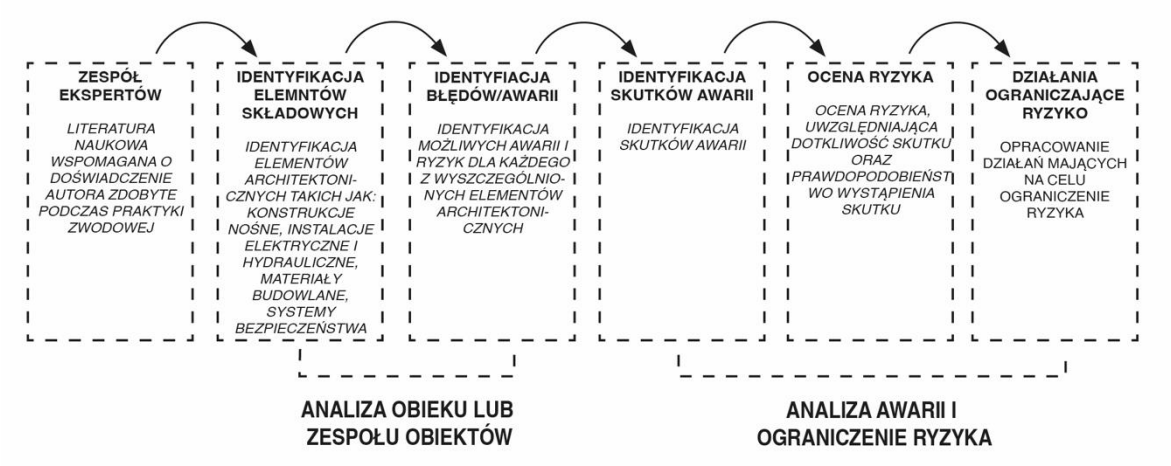
„Cyberprzestępczość jest coraz większym problemem w coraz bardziej połączonym świecie" (Parlament Europejski 2020). Dzięki Internetowi rzeczy (IoT- Internet of Things), który odnosi się do sieci urządzeń podłączonych do Internetu, mamy możliwość otwierania i zamykania drzwi czy bram garażowych, sprawdzania monitoringu w naszych telefonach, a nawet podgrzewania piekarnika w drodze do domu, do tego dochodzą elektroniczne nianie, lodówki, odkurzacze i wiele innych urządzeń typu smart (Alahi, Ghayvat, Gui, Liu, Mukhopadhyay, 2015). Tworzy to sieć informacyjną nie tylko jednostek, ale też systemów i urządzeń, które mogą działać niezależnie od człowieka (Kabrońska, Wysocki, 2016). Jeśli w gospodarstwie domowym, znajduje się wiele połączonych ze sobą sprzętów cyberprzestępcy przejmując jeden z nich mają dostęp do bogatej bazy danych związanych z trybem funkcjonowania ich właściciela co może ułatwić im potencjalny napad lub próbę wyłudzenia danych (Blaicke, Rot, 2016).

Kolejnym zagadnieniem jest BMS (Building Management System), czyli całkowicie zautomatyzowany system zarządzania instalacjami w budynku, który wykorzystywany jest coraz częściej w przypadku obiektów efektywnych energetycznie (Dechnik, Moskwa, 2020). Przejęcie kontroli nad systemami sterowania, wentylacji, klimatyzacji, temperatury, czy energii może w natychmiastowy sposób zmusić mieszkańców do ewakuacji, powodując ułatwiony dostęp do obiektu dla potencjalnego przestępcy.

3.3. Metoda walidacji zagrożeń w procesie projektowania, budowy i użytkowania budynków

Aby właściwie zidentyfikować potencjalne ryzyko i zagrożenia autorka posłużyła się analizą FMEA Metodę standardowo wykorzystuje się do analizy rodzajów i skutków wad dla produktu lub procesu tworzenia produktu. Istnieją liczne schematy procesu FMEA, z czego ten bazowy dzieli się na 5 etapów (Rychły-Lipińska, 2007):

1. Powołanie zespołu: 4-8 osób wraz z przewodnikiem i (ewentualnie) ekspertem;
2. Identyfikacja elementów składowych produktu/procesu;
3. Opracowanie listy możliwych błędów;
4. Wskazanie ewentualnych skutków opracowanych błędów;
5. Wypunktowanie możliwych przyczyn opracowanych błędów.



Ryc. 1. Aplikacja procesu metody FMEA do identyfikacji ryzyka i zagrożeń w procesie projektowania, budowy i użytkowania budynków. Źródło: opracowanie własne autorki

Schemat Ryc. 1 pokazuje dostosowanie procesu metody FMEA, aby mogła identyfikować ryzyko i zagrożenia dla procesu projektowania, budowy i użytkowania budynków, dla przyjętych kategorii. Na tej podstawie, opracowano badanie identyfikacji ryzyka występowania zagrożeń wykluczenia cyfrowego oraz cyberprzestępczości dla budownictwa wielorodzinnego (Tab.2). Omawiane ryzyka można analizować w kontekście innych rodzajów zabudowy, również niemieszkalnej, co jest perspektywą rozwoju badań.

Tab. 2. Analiza mająca na celu identyfikację ryzyka wykluczenia cyfrowego oraz cyberprzestępczości w procesie projektowania, budowy i użytkowania obiektów wielorodzinnych. Źródło: opracowanie własne autorki

Identyfikacja elementów budynku	**Identyfikacja awarii i ryzyka**	**Identyfikacja skutków awarii**	**Ocena ryzyka**	
			Dotkliwość skutku*	**Prawdopodobieństwo wystąpienia skutku****
CYFROWE WYKLUCZENIE				
Infrastruktura telekomunikacyjna (instalacje wewnętrzne)	Brak zaplanowania odpowiedniej infrastruktury telekomunikacyjnej dla całego obiektu, na etapie projektu technicznego lub wykonawczego.	Brak możliwości przyłączenia jednostki mieszkaniowej do łącza stałego.	wysokie	wysokie
Infrastruktura telekomunikacyjna (sieci)	Lokalizacja budynku wielorodzinnego uniemożliwia podłączenie obiektu do sieci telekomunikacyjnej ze względu na braki w infrastrukturze.	Długotrwały brak dostępu mieszkańców do Internetu, co utrudnia komunikację, pracę zdalną i dostęp do informacji.	wysoka	niskie *(dla obszarów zurbanizowanych)* wysokie *(dla obszarów wiejskich)*
Przestrzenie wspólne budynku	Brak przestrzeni wspólnych zewnętrznych lub wewnętrznych dający możliwość otwartego dostępu do Internetu.	Wykluczenie z dostępu do Internetu osób najbardziej potrzebujących, których nie stać przyłączenie się do usług telekomunikacyjnych na umowach indywidualnych.	wysoka *(dla grup najbardziej zagrożonych)*	wysokie *(dla grup najbardziej zagrożonych)*

Identyfikacja elementów budynku	Identyfikacja awarii i ryzyka	Identyfikacja skutków awarii	Ocena ryzyka	
			Dotkliwość skutku*	**Prawdopodobieństwo wystąpienia skutku****
Zarządzanie budynkiem	Brak możliwości wypożyczenia sprzętu umożliwiającego swobodny dostęp do Internetu.	Wykluczenie z dostępu do Internetu osób najbardziej potrzebujących, których nie stać na zakup sprzętu dającego swobodny dostęp do Internetu.	wysoka *(dla grup najbardziej zagrożonych)*	wysokie *(dla grup najbardziej zagrożonych)*
POWSZECHNOŚĆ PRZESTĘPCZOŚCI INTERNETOWEJ I OGÓLNY BRAK BEZPIECZEŃSTWA W CYBERPRZESTRZENI				
Systemy zarządzania budynkiem (BMS)	Przejęcie kontroli nad systemem zarządzania budynkiem (BMS) i zmiana ustawień, takich jak oświetlenie, ogrzewanie, wentylacja	Zakłócenie normalnego funkcjonowania budynku, na przykład zmiana temperatury, oświetlenia czy dostępu do pomieszczeń.	wysoka	wysokie
Systemy inteligentnego budynku (IoT) takie jak inteligentne zamki, termostaty.	Przejęcie kontroli nad systemami umożliwiającymi nieautoryzowany dostęp do budynku lub zmianę ustawień bez zgody mieszkańców.	Naruszenie prywatności mieszkańców poprzez monitorowanie ich działań lub kradzież danych osobowych.	wysoka	wysokie
Systemy monitorowania i kontroli dostępu	Kradzież danych takich jak dane identyfikacyjne czy plany pomieszczeń	Potencjalne zagrożenie dla bezpieczeństwa fizycznego mieszkańców poprzez nieautoryzowany dostęp do budynku.	wysokie	wysokie

* dotkliwość skutku: niska, umiarkowana, wysoka

** prawdopodobieństwo wystąpienia skutku: niskie, umiarkowane, wysokie

3.4. Analiza przypadku

3.4.1. Analiza przypadku – charakterystyka obszaru badawczego

W ramach analiz map dostępności Internetu szerokopasmowego (Ministerstwo Cyfryzacji, 2024) dla obiektów wielorodzinnych w Szczecinie (Ryc.2), obszar badawczy zawężono do zabudowy śródmiejskiej. Wyszczególniono dwa typy kwartałów:

– z dostępem do Internetu jedynie budynków przylegających do ulicy, oficyny bez dostępu do Internetu;
– z dostępem do Internetu całej zabudowy kwartału.

Na ich podstawie zidentyfikowano, że kwartały wyróżniające się w tkance miejskiej całościowym dostępem do sieci poddane były kompleksowym rewitalizacjom, przeprowadzonym w ramach miejskich programów społecznych lub były wynikiem interwencji prywatnych.

Analizie identyfikacji ryzyka wykluczenia cyfrowego oraz cyberprzestępczości poddano kwartał 23 (Ryc.3), otoczony Aleją Wojska Polskiego i ulicami Bohaterów Getta Warszawskiego, Królowej Jadwigi oraz Księdza Piotra Ściegiennego. Obszar ten został poddany rewitalizacji w latach 2012-2016, a jego założeniami były: podniesienie standardu i jakości życia lokalnej społeczności, poprawa stanu technicznego tkanki miejskiej, podwyższenie efektywności energetycznej budynków, działania społeczne oparte o działalność Społecznego Ośrodka Wsparcia Dziennego, aktywizacja mieszkańców w zakresie dbałości o najbliższe otoczenie i budynek, ochrona wartości historycznych i kulturowych oraz ożywienie gospodarcze (Towarzystwo Budownictwa Społecznego w Szczecinie, 2016). W ramach działań projektowych częściowo zlikwidowano oficyny, które powodowały niedoświetlenie podwórek kwartału. Zaproponowano nowy obiekt, łączący pozostawione oficyny oraz będący jednocześnie uzupełnieniem linii zabudowy wzdłuż ulicy Królowej Jadwigi. Budynek dzięki posadowieniu

na słupach utworzył pasaż pieszo-jezdny łączący przestrzenie wspólne tworząc tym samym dojścia do lokali usługowych oraz obsługę gospodarczą wnętrza kwartału.

3.4.2. Zastosowanie metody walidacji zagrożeń technologicznych w procesie projektowania, budowy i użytkowania nowopowstałych obiektów i przestrzeni wspólnych Kwartału 23 w Szczecinie

Niezbędne dane do prawidłowego zastosowania metody walidacji zagrożeń autorka uzyskała w ramach wywiadu z projektantami kwartału (Studio a4), którzy na stałe współpracują ze Szczecińskim TBS (Towarzystwem Budownictwa Społecznego), który jest odpowiedzialny za przeprowadzenie rewitalizacji. Analizie poddano wszystkie aspekty wskazane w tabeli 2, choć w odniesieniu do badanego obszaru nie mają zastosowania.

Tab. 3. Identyfikacja ryzyka wykluczenia cyfrowego oraz cyberprzestępczości w procesie projektowania, budowy i użytkowania dla Kwartału 23, w Szczecinie. Źródło: opracowanie własne autorki

Możliwe awarie i ryzyka	**Zidentyfikowanie czy występują określone dla danej kategorii awarie lub ryzyka dla Kwartału 23 w Szczecinie**	**Działania zapobiegawcze i naprawcze**	**Kategoria działań**
WYKLUCZENIE CYFROWE			
Brak zaplanowania odpowiedniej infrastruktury telekomunikacyjnej dla całego obiektu.	Infrastruktura telekomunikacyjna zaprojektowana poprawnie.	Nie wymagane	projektowanie budynku
Lokalizacja budynku wielorodzinnego uniemożliwia podłączenie obiektu do sieci telekomunikacyjnej ze względu na braki w infrastrukturze.	Lokalizacja budynku pozwoliła na przyłączenie obiektów wchodzących w skład kwartałów do Internetu szerokopasmowego.	Nie wymagane	projektowanie budynku
Brak przestrzeni wspólnych zewnętrznych lub wewnętrznych dający możliwość otwartego dostępu do Internetu.	Przestrzenie wspólne zostały zrewitalizowane i dostosowane do potrzeb mieszkańców (Ryc.4). Poza strefami zewnętrznymi, w jednym z budynków ukierunkowanym na politykę senioralną, zaprojektowano miejsca spotkań (Ryc.5), jednakże brak w nich otwartego dostępu do Internetu.	Wprowadzenie w przestrzeniach wspólnych strefy bezprzewodowego i bezpłatnego Internetu	projektowanie + użytkowanie budynku
Brak możliwości wypożyczenia sprzętu umożliwiającego swobodny dostęp do Internetu.	Nie wykazano działań umożliwiających wypożyczenie sprzętu.		użytkowanie budynku
POWSZECHNOŚĆ PRZESTĘPCZOŚCI INTERNETOWEJ I OGÓLNY BRAK BEZPIECZEŃSTWA W CYBERPRZESTRZENI			
Przejęcie kontroli nad systemem zarządzania budynkiem (BMS) i zmiana ustawień, takich jak oświetlenie, ogrzewanie, wentylacja	Brak systemu BMS	Nie dotyczy	Nie dotyczy
Przejęcie kontroli nad systemami umożliwiającymi nieautoryzowany dostęp do budynku lub zmianę ustawień bez zgody mieszkańców.	Brak systemów inteligentnego budynku	Nie dotyczy	Nie dotyczy
Kradzież danych takich jak dane identyfikacyjne czy plany pomieszczeń	Brak systemu monitoringu	Nie dotyczy	Nie dotyczy

4. PODSUMOWANIE WYNIKÓW

Metoda walidacji zagrożeń technologicznych, dla procesu projektowania, budowy i użytkowania obiektów wielorodzinnych (Tab.2) wykazała różnice w ich projektowaniu i użytkowaniu w zależności od przeznaczenia. Z obiektów z mieszkaniami socjalnymi lub wspomaganymi[2], korzystają często grupy najbardziej zagrożone wykluczeniem cyfrowym i ograniczeniami w dostępie do sieci szerokopasmowej (Peppel, Computing, 2016). Dla nich istotną kwestią jest projektowana infrastruktura zewnętrznych i wewnętrznych przestrzeni wspólnych z ogólnym dostępem do internetu. Jednocześnie podczas planowania podobnych inwestycji, gminy oraz podległe im jednostki odpowiedzialne, przeznaczając właściwy teren pod obiekty wielorodzinne powinny weryfikować możliwości teletechniczne oraz obsługę operatorów dla terenu będącego obszarem opracowania. Warto tu również zaznaczyć istotę regulacji urbanistycznych (dostosowanych do prawa planistycznego danego regionu), w procesie tworzenia obszarów dla zabudowy mieszkaniowej wielorodzinnej, tak aby nie tylko były one wyposażone w odpowiedną infrastrukturę.

Obiekty deweloperskie, zwłaszcza te o podwyższonym standardzie, gdzie projektowana jest automatyka zarządzania wentylacją, ogrzewaniem, kontrolą dostępu czy monitoringiem narażone są na ataki hakerskie, próby wyłudzenia danych oraz kradzieże bazujące na łamaniu zabezpieczeń sieciowych. W tym przypadku szczególną uwagę należy zwróć na projekt teletechniczny zawierający w sobie wytyczne do ochrony mieszkańców na poziomie zarządzania siecią. Projektowanie budynku powinno odbywać się z uwzględnieniem całego cyklu życia obiektu, w związku z tym jego integralnym elementem powinny być kwestie związane z użytkowaniem włączając w to działania edukacyjne skierowane do mieszkańców oraz regulamin użytkowania osiedla, który określa zasady bezpiecznego korzystania z infrastruktury cyfrowej, wspierając ochronę indywidualnych użytkowników (Scott, 2023).

Analiza występowania ryzyka wykluczenia cyfrowego oraz cyberprzestępczości dla zrewitalizowanego Kwartału 23 (Tab.3), wykazała, dobre przygotowanie przez architektów projektu wykonawczego w ramach infrastruktury telekomunikacyjnej i funkcjonalnej kwartału. Po rozpoznaniu potrzeb mieszkańców, na poziomie zarządzania obiektem należy rozważyć wprowadzenie działań mogących ograniczyć ryzyko wykluczenia cyfrowego, takie jak dostępne dla mieszkańców strefy hot spot, czy możliwość krótko i długoterminowego wypożyczenia sprzętu, który umożliwi swobodny dostęp do Internetu. W ramach działań ograniczających wykluczenie cyfrowe należy pamiętać o możliwości wsparcia technicznego dla grup najbardziej potrzebujących w zakresie konfiguracji urządzeń, rozwiązywania problemów związanych z dostępem do Internetu czy korzystania z aplikacji.

Przeanalizowany przykład wyklucza zagrożenie cyberprzestępczości ze względu na fakt, iż w kwartale obecnie nie występują m.in. inteligentne systemy zarządzania budynkiem. Jednakże w raz z postępem technologicznym mieszkania wyposażone są w coraz większą ilość urządzeń typu smart dlatego warto zadbać o edukację mieszkańców, a także podejmować współpracę z renomowanymi dostawcami usług, którzy zapewniają wysoką jakość oraz posiadają aktualną wiedzę na temat najnowszych zagrożeń i rozwiązań.

Podsumowując, wykryte zagrożenia technologiczne nie są znaczące dla kształtowania budynku wielorodzinnego, poza istotą odpowiedniego kreowania przestrzeni publicznych. Należy jednak podkreślić, że biorąc pod uwagę współczesne wyzwania takie jak: troska o środowisko, problemy społeczne i ekonomiczne oraz zagrożenia technologiczne (Word Economic Forum, 2024), architekci powinni postrzegać obiekt architektoniczny nie tylko przez pryzmat jego formy. Parlament Europejski podkreśla istotność pełnego cyklu życia (LCA) produktów sektora budowlanego, na który składa się fazy wyrobu, użytkowania, końca życia oraz potencjału recyklingowego. Jest to jedno z podstawowych narzędzi redukcji ilości dwutlenku węgla emitowanego do atmosfery. Ponadto badania wskazują, że decyzje podejmowane na wczesnym etapie projektowym mają największy wpływ na zrównoważony rozwój budynku, a włączenie do metody LCA technologii BIM daje najlepsze efekty. W tym

[2] (z ang. assited living) mieszkania przeznaczone dla seniorów i osób przewlekle chorych, które chcą żyć samodzielni, ale wymagają codziennego wsparcia.

kontekście zidentyfikowane zagrożenia technologiczne dla zabudowy wielorodzinnej są jednym z istotnych czynników, które należy brać pod uwagę na etapie projektowania i realizacji.

5. DYSKUSJA I PODSUMOWANIE

Wybrany do analizy przykład przebudowy szczecińskiego Kwartału 23 obrazuje kompleksowe podejście do rewitalizacji. Polega ono m.in. na wyrównaniu szans mieszkańców, a tym samym zapobieganiu wykluczenia w zaopatrzeniu całej strefy w dostęp do Internetu oraz stworzenie właściwej struktury funkcjonalnej umożliwiającej korzystanie z sieci grupom najbardziej zagrożonym. Zadaniem Louis Suh, senior architektki nowojorskiego oddziału duńskiej pracowni Henning Larsen, trendem w architekturze w coraz większym stopniu będą projekty skupiające się na programie adaptacyjnym, ponownym wykorzystaniu i rozbudowach. Przyszłością będzie transformacja istniejących konstrukcji bez dużej emisji dwutlenku węgla, do której zwykle przyczynia się nowy projekt budowlany (Lundeholm., Suh, 2023). Biorąc pod uwagę skalę problemu braku dostępu do Internetu kablowego i światłowodowego w oficynach szczecińskiego śródmieścia, wskazuje się, iż podobne działania rewitalizacyjne powinny odbywać się w dużo większej skali.

W literaturze polskiej temat zapobiegania zagrożeniom technologicznym w ramach działań architektonicznych jest poruszany w bardzo niewielkim zakresie. Istnieją liczne publikacje nawiązujące do tematyki wykluczenia cyfrowego, gdzie poruszana jest tematyka różnic w dostępie do technologii oraz do umiejętności potrzebnych do korzystania z nich (Batorski, 2009), jednak bez związku z budownictwem mieszkaniowym. Szerzej temat jest omawiany w literaturze zagranicznej, gdzie zwraca się szczególną uwagę na istotę autonomii w korzystaniu z Internetu i właściwym planowaniem infrastruktury lokalowej (Peppel, Computing, 2016), a także odpowiednym planowaniu przestrzeni wspólnych zewnętrznych i wewnętrznych (Asher, Arnold, Nassau-Brownstone, 2021). W tematyce cyberprzestępczości zarówno w literaturze polskiej, jak i zagranicznej podkreśla się skalę niebezpieczeństwa jakie niesie za sobą korzystanie z systemów IoT czy BMS oraz wskazuje się działania prewencyjne mające na celu zabezpieczenie klientów prywatnych i dostawców (Blaicke, Rot, 2016). Nie jest jednak jasne kto poza użytkownikiem indywidualnym powinien być odpowiedzialny za wprowadzanie odpowiednich zabezpieczeń: architekt, zarządca budynku czy projektant wnętrz. W artykule wykazano, natomiast, że działania kompleksowe i założenia odgórne przynoszą najlepsze rezultaty, dlatego wskazuję się na potrzebę regulacji tego zagadnienia.

Podsumowując w artykule przeprowadzono analizę ryzyka przy użyciu metody FMEA, która pozwoliła na identyfikację głównych zagrożeń. Zaproponowano środki zaradcze. Przykładem praktycznym jest szczeciński Kwartał 23, gdzie zaplanowano właściwą infrastrukturę teletechniczną oraz przestrzenie wspólne zewnętrzne i wewnętrzne mogące wpływać na obniżenie ryzyka cyfrowego wykluczenia. Wyniki sugerują konieczność opracowania regulacji dotyczących zabezpieczeń cyfrowych, zarówno na etapie planistycznym oraz projektowym, a także edukację użytkowników, co zwiększyłoby bezpieczeństwo mieszkańców w wielorodzinnych kompleksach mieszkalnych. Zagrożenia technologiczne zostały wyszczególnione na podstawie raportu Zagrożeń Globalnych 2023 (World Economic Forum, 2023). Światowe forum ekonomiczne publikuje raport corocznie, dlatego należy zwrócić uwagę na istotę weryfikacji i aktualizacji stanu badań.

Kompetencje architektów ewoluują wraz z postępem technologicznym, zmieniającymi się potrzebami społecznymi oraz nowymi wyzwaniami związanymi z projektowaniem i budową. Proces tworzenia obiektów wymaga współpracy z coraz szerszą rzeszą specjalistów, co wiąże się z koordynacją większej ilości zagadnień na etapie procesu projektowania. Zagrożenia technologiczne, to nowe zagadnienia, które powinny zostać włączone w proces projektowania, realizacji i użytkowania architektury, w tym zabudowy wielorodzinnej.

BIBLIOGRAPHY

Alahi, M. E. E, Ghayvat, H., Gui, X., Liu, J., Mukhopadhyay S. C., (2015) 'Internet of Things for smart homes and buildings: Opportunities and Challenges', Journal of Telecommunications and the Digital Economy, DOI: 10.18080/ajtde.v3n4.23.

Asher, L., Arnold, A., Nassau-Brownstone, A., (2021) Bridging the Digital Divide in Affordable Housing Communities A Practitioner's Resource for Multifamily Operators, Available at: https://www.sahfnet.org/sites/default/files/uploads/digital_access_playbook_publish_w_bookmarks_2_0.pdf, (Accessed: 03-02-2021).

Bakar A., Ghapar A., Jørgensen B., Sameon S.,Yussof S.(2024), 'A Review of Privacy Concerns in Energy-Efficient Smart Buildings: Risks, Rights, and Regulations', Energies 2024, 17(5), p.977, https://doi.org/10.3390/en17050977.

Batorski, D., (2009) 'Wykluczenie Cyfrowe w Polsce', Społeczeństwo Informacyjne, 3(19)2009, pp. 223-249, ISSN 2080-2404.

Bayley, R., (2022) 'Missing the Mark - 2022 analysis of global cdp temperature ratings', available at: ,https://www.oliverwyman.com/our-expertise/insights/2022/sep/cdp-temperature-ratings.html, (Accessed: 01-09-2022).

Beet J., Borman A., Koch C., König M., (2018) 'Building Information Modeling: Why? What? How?: Technology Foundations and Industry Practice', Building Information Modeling, pp.1-24, DOI:10.1007/978-3-319-92862-3_1.

Blaicke B., Rot A., (2016) 'Zagrożenia wynikające z implementacji koncepcji Internetu rzeczy. rekomendacje dla organizacji i dostawców rozwiązań', Informatyka Ekonomiczna, (3)41, ISSN 1507-3858.

Celeste, C., DiMagio, P., Hargittai, E., Shafer, S., (2003) 'From Unequal Access to Differentiated Use: A Literature Review and Agenda for Research on Digital Inequality'.

Dechnik. M., Moskwa S. (2020), 'Systemy zarządzania budynkami BMS', Murator: Instalacje elektryczne, Oświetlenie, Zabezpieczenia. Poradnik dla profesjonalistów, 2/2020, pp.62-65, ISSN 1641-1005.

Dudek-Burlikowska, M, (2011), 'Application of FMEA method in enterprise focused on quality", Journal of Achievements of Materials and Manufacturing Engineering, 45, ISSN: 1734-8412.

Favaro M., Kuchn U., Renic N., (2022) 'Negative Multiplicity: Forecasting the Future Impact of Emerging Technologies on International Stability and Human Security' Institute for Peace Research and Security Policy, DOI: https://doi.org/10.25592/ifsh-research-report-010.

Hämäläinen M, (2020) 'Smart city development with digital twin technology' http://bledconference.org/, DOI:10.18690/978-961-286-362-3.20.

Inglot-Brzęk E., (2011) 'Brak dostępu do internetu jako wskaźnik wykluczenia społecznego', Nierówności Społeczne, a Wzrost Gospodarczy, 19, pp.374-385.

Kabrońska J., Wysocki M., (2016), 'Nowe Technologie w Architekturze', Wybrane problemy przebudowy obiektów budowlanych, Gdańsk, Wydawnictwo Politechniki Gdańskiej, ISBN 8373486836.

Kowalik K. (2018) 'Metoda FMEA w teorii i praktyce zarządzania jakością', Archiwum wiedzy inżynierskiej, 3(2), pp. 23-25.

Lundeholm S., Suh L., (2023) 'Three trends for 2023: What will bring about real change?', Avaiable at: https://henninglarsen.com/news/three-trends-for-2023, (Accesed; 30-01-2023).

Ministerstwo Cyfryzacji (2024) 'Interaktywna Mapa Dostępu do Internetu', Available at: https://internet.gov.pl.

The MIT Norman B. Leventhal Center for Advanced Urbanism (2022) 'Digital Urbanism, Avaiable at: https://lcau.mit.edu/research/digital-urbanism.

Parlament Europejski, (2020) 'Jak chronić się przed cyberprzestępczością?', Avaiable at: https://www.europarl.europa.eu/topics/pl/article/20200327STO76003/jak-chronic-sie-przed-cyberprzestepczoscia, (Accessed: 01-04-2024).

Peppel, M., Computing S., (2016) Evidence Matters. Housing, Community Development, and the Digital Divide, Available at: https://www.huduser.gov/portal/periodicals/em/fall16/highlight2.html, (Accessed: 01-11-2016).

Rychły-Lipińska A., (2007) 'FMEA- analiza rodzajów błędów oraz ich skutków'. Zeszyty Naukowe Instytutu Ekonomii i Zarządzania, 11, pp. 47-59.

Scott L., (2023) 'Why ransomware attacks pose a unique threat to real estate', Avaiable at: https://global.lockton.com/, (Accessed: 26-10-2024).

Szczecińskie Towarzystwo Budownictwa Społecznego, (2016) 'Rewitalizacja RAZEM – KWARTAŁ 23' http://www.stbs.pl/index.php/rewitalizacja-razem-kwartal-23.html (Accessed: 10-05-2024).

World Economic Forum, (2023) 'Global Risks Report 2023 18-th edition, Available at: https://www.weforum.org/publications/global-risks-report-2023/, (Accessed: 05-11-2024), ISBN-13: 978-2-940631-36-0.

AUTHOR'S NOTE

Graduate of the West Pomeranian University of Technology in Szczecin, Faculty of Civil Engineering and Architecture. Member of the West Pomeranian District Chamber of Architects. Deals with the issues of multi-family housing in the context of human needs in comparison with the needs of a sustainable city in the face of the challenges of the modern world.

O AUTORZE

Absolwentka Zachodniopomorskiego Uniwersytetu Technologicznego w Szczecinie, Wydziału Budownictwa i Architektury. Członkini Zachodniopomorskiej Okręgowej Izby Architektów. Zajmuje się zagadnieniami budownictwa wielorodzinnego w kontekście potrzeb człowieka w zestawieniu z potrzebami zrównoważonego miasta w obliczu wyzwań współczesnego świata.

Contact | Kontakt: katarzyna.florysiak@zut.edu.pl