ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2025»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2025»

PROCEEDINGS
of the XX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2025»

2025
Астана

УДК 001(06)
ББК 72я631
F96

«ǴYLYM JÁNE BILIM – 2025» студенттер мен жас ғалымдардың XX Халықаралық ғылыми конференциясы = XX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2025» = The XX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2025». – Астана: – 3813 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-08-5373-7

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.В сборник вошли доклады студентов, магистрантов, докторантов имолодыхученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001(06)
ББК 72я431
F96

ISBN 978-601-08-5373-7

Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 2025

СЕКЦИЯ 2

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ И КОММ УНИКАЦИОННЫЕ ТЕХНОЛОГИИ

Подсекция 2.2

Интеллектуальные информационные системы

255.	Сафонова Софья Александровна «Современные аспекты информационной безопасности в облачных вычислениях: модели, угрозы и методы защиты»	1034
256.	Смаилова Назгүл Батырбекқызы «Терең оқыту арқылы кітап ұсыныстарын әзірлеу: collaborative filtering, content-based және nlp әдістерінің комбинациясы»	1041
257.	Тажібай Аружан Айдосқызы, Кудубаева Сауле Альжановна «Көру қабілеті әлсіз адамдарға арналған аі дауыстық көмекші: нақты уақытта объектілерді анықтау және қашықтықты бағалау»	1046
258.	Тайжанов Азамат Жанкелдіұлы «Python тілінде фильмдердің интеллектуалды ұсыныс жүйесін әзірлеу»	1051
259.	Умирзахов Сундетали Кабылбекович «Сұраныстарды интеллектуалды талдау негізінде ұйымның сайты үшін чат-бот құру»	1055
260.	Шайхстан Марғұлан «IOT Сенсорлары негізінде ауа ластану деңгейін болжау»	1060

Подсекция 2.3

Современные тенденции в программной инженерии и управлении в условиях цифровой индустрии

261.	Bekenova A.B. «Development of a registration panel for users and doctors with integration into the database»	1077
262.	Bolat A.Zh. «Data analysis methods and decision making using big data and machine learning tools»	1081
263.	Алтайұлы А. «Visual studio интегралды ортасында «қойма қызметкерлеріне арналған» мәліметтер қорын жобалау»	1086
264.	Арап А.Қ. «Ақылды сурет салушы роботты әзірлеу»	1088
265.	Артыкбекқызы А. «Ақылды үйлердегі заттар интернеті(iot) мен робототехниканың өзара әрекеттесуі»	1091
266.	Ахметова А.Д. «Тоңазытқыштағы өнімдерді бақылауға және тағам әзірлеу ұсынысын беруге арналған программалық қосымша»	1096
267.	Дәрібай Д.Д. «Робототехниканы қолдану арқылы қойма логистикасындағы қолданыстағы басқару жүйелерін талдау»	1100
268.	Жамбулов С.Ж. «Білім алушыларды информатика және программалау олимпиадаларына дайындауда жасанды интеллекттің қолданысы»	1102
269.	Каиржан Р.С. «Development of system for recognition of emotional states of employees based on computer vision methods on Raspberry Pi»	1108
270.	Кайрекенова Н.Р. «Өнеркәсіптік роботты көру үшін машиналық оқытудың заманауи тәсілдері: әдістер, деректер жиынтығы және оптимизациялау»	1111

СЕКЦИЯ 3
ЕСТЕСТВЕННЫЕ НАУКИ

focus on improving model efficiency and integrating blockchain-based security mechanisms (Hussain et al., 2021) [3].

Literature

1. Wang, Y., Xiang, Y., Hu, J., & Zhou, W. (2017). An overview of DDoS attack detection and defense in SDN. *Computer Networks, 136*, 96-107.

2. Behal, S., & Kumar, K. (2017). Trends in validation of DDoS research. *Computers & Security, 67*, 76-92.

3. Hussain, S., Abbas, S. G., Malik, K. M., & Saleem, K. (2021). Artificial intelligence-based anomaly detection in network security: A comprehensive survey. *Journal of Cybersecurity and Privacy, 1*(2), 173-202.

4. Radford, J., Beznosov, K., & De Lucena, V. (2019). On the detection of DDoS attacks using machine learning and feature selection. *Future Generation Computer Systems, 102*, 524-534.

5. Yu, S., Guo, H., & Yuan, J. (2020). A deep learning approach to DDoS attack detection for network security. *Neural Computing and Applications, 32*(10), 6521-6534.

6. Choudhury, S., Bhowmick, A., Sain, M., Roy, S., & Kumar, S. (2020). Anomaly detection in network traffic using deep learning: A review. *IEEE Access, 8*, 132278-132308.

7. Doshi, R., Apthorpe, N., & Feamster, N. (2018). Machine learning DDoS detection for consumer Internet of Things devices. *IEEE Security & Privacy, 16*(6), 29-37.

8. Kirubavathi, G., & Anitha, R. (2016). Botnet detection via mining DNS query data using machine learning. *Computers & Security, 58*, 35-46.

9. Liu, H., Lang, B., Liu, Z., & Yu, Y. (2019). DDoS attack detection based on neural network with traffic pattern analysis. *IEEE Access, 7*, 93629-93638.

10. Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2015). A multi-step approach for DDoS attack detection and mitigation. *Journal of Network and Computer Applications, 68*, 136-155.

ANALYSIS OF MODERN WIRELESS NETWORK SECURITY PROTOCOLS AND PROSPECTS FOR THEIR DEVELOPMENT

Gabdullin Abzal
anchorite.exe@gmail.com
Department of Information Security System, Faculty of Information Technologies, Eurasian National University, Astana Kazakhstan
Supervisor – Z. Tashenova

1. Introduction

Wireless networking is crucial in our daily lives now. You can find Wi-Fi almost everywhere, like in homes, offices, and public places. Over the last 20 years, the security features of Wi-Fi have improved and changed a lot. This change follows several important standards that were introduced to make Wi-Fi more secure and reliable. Early protocols like Wired Equivalent Privacy (WEP) were found fundamentally flawed, leading to the development of Wi-Fi Protected Access (WPA) and the widely adopted WPA2 (IEEE 802.11i) standard in 2004. Most recently, the Wi-Fi Alliance introduced WPA3 in 2018 as the successor to WPA2, aiming to strengthen encryption and authentication for WLANs [10]. These modern 802.11 security protocols (WPA2, WPA3) were designed to ensure confidentiality, integrity, and access control in wireless networks, and they are now the default options in personal routers and enterprise Wi-Fi deployments [10], [14].

2. Context and Methodology of the Study

Despite significant advancements in wireless encryption and authentication protocols, real-

world Wi-Fi networks continue to face a range of security threats. WPA2 has been the most widely adopted standard for over a decade, yet research and practical attacks have shown that even robust encryption can be undermined by protocol-level flaws, misconfigurations, or weak credentials. These persistent issues have driven the development of WPA3, which introduces new mechanisms aimed at mitigating common vulnerabilities—but its adoption and implementation remain uneven across devices and environments.

Understanding the practical security posture of these protocols is crucial. This study explores how WPA2 and WPA3 fare under targeted attacks by recreating common threat scenarios in a controlled environment. Specifically, four types of attacks were simulated: deauthentication attacks, handshake captures, KRACK (Key Reinstallation Attacks), and protocol-level exploits targeting offline dictionary attacks.

Each scenario was executed in five repeated trials to ensure statistical relevance. Key metrics such as attack success rate, packet loss, and reconnection time were recorded and averaged. The methodology not only tests theoretical weaknesses but also assesses whether the protocol-level improvements of WPA3 result in observable resilience during live deployments.

This combined contextual and experimental analysis allows for a practical evaluation of WPA2 and WPA3, providing insight into which vulnerabilities persist, which have been mitigated, and what implications this has for securing modern wireless networks in both personal and enterprise settings.

2.1 VULNERABILITIES OF WPA2

Wi-Fi Protected Access II (WPA2) has been the predominant WLAN security standard for over a decade, offering robust encryption via AES-CCMP. However, multiple studies have exposed critical vulnerabilities in WPA2's design. One notable flaw is the Key Reinstallation Attack (KRACK), which exploits a weakness in the four-way handshake to force nonce reuse and decrypt data without the Wi-Fi password [27]. Similarly, an attacker can capture a WPA2 handshake-derived value (the PMKID) to perform offline dictionary attacks, bypassing the need to intercept the full 4-way exchange [6]. These revelations highlight that even strong ciphers can be undermined by protocol logic errors.

2.2 VULNERABILITIES AND FEATURES OF WPA3

The introduction of WPA3 brought important enhancements intended to address WPA2's shortcomings. Notably, WPA3-Personal replaces the pre-shared key exchange with the Simultaneous Authentication of Equals (SAE) handshake, a variant of the Dragonfly key exchange, to provide forward secrecy and better resistance to offline password guessing [14]. WPA3 also mandates Protected Management Frames (PMFs) to defend against deauthentication spoofing and introduces individualized data encryption even on open networks through Opportunistic Wireless Encryption (OWE) [10], [15]. These improvements raised expectations that WPA3 would resolve the prevalent issues in WPA2.

2.3 CONTRIBUTIONS OF THIS STUDY

Through this hands-on evaluation, we present a synthesized analysis of the strengths and weaknesses of WPA2 and WPA3, and we offer insights into their suitability for different use cases. In particular, this study:

(1) Identifies which known vulnerabilities remain applicable (or have been mitigated) in real deployments of WPA2 vs. WPA3 [5], [7].

(2) Pinpoints security gaps where further improvements or best practices are needed (for instance, in handling rogue AP threats or ensuring robust user authentication) [8], [23].

(3) Provides guidance on selecting and configuring Wi-Fi security protocols for distinct contexts—from end-user home networks to large enterprise infrastructures—in light of their current security posture [10], [14].

By highlighting the practical implications of recent protocol developments, our work aims to help both network practitioners and researchers understand the current state-of-the-art in wireless

security and the prospects for its future development.

3. RESULTS AND DISCUSSION

This section presents and analyzes the experimental results, comparing the performance of WPA2 and WPA3 under different attack scenarios. Results are structured into four key attack evaluations: deauthentication attack, handshake capture, KRACK attack, and overall comparative metrics.

All the experimental results are consolidated in Table 1 for direct comparison. Each metric represents the average over 5 repeated trials per scenario, as described in the methodology. The success rate (in %) for each attack was computed as shown in Equation (1), based on the number of trials in which the attack achieved its intended effect (e.g., disconnection or key compromise):

$$R_s = \frac{N_{successful\ trials}}{N_{total\ trials}} \times 100\%$$

Table 1. Comparative outcomes for WPA2 vs. WPA3 under different attack scenarios

Attack Type	Success Rate (WPA2 vs. WPA3)	Avg. Disconnection Time (s)	Packet Loss (%)	Reconnection Time (s)
Deauth Attack	100% vs. 0%	0.5s vs. 0s	90% vs. 0%	3.0s vs. 0s
Handshake Capture	100% vs. 100%	0.5s vs. 1.0s	5% vs. 5%	1.5s vs. 2.0s
KRACK Attack	100% vs. 0%	0s vs. 0s	5% vs. 0%	0s vs. 0s

4. Conclusion

This study set out to identify the strengths and weaknesses of modern Wi-Fi security protocols through hands-on testing, and the findings clearly confirm the expected security gap between WPA2 and WPA3. WPA3-Personal delivered substantial improvements over WPA2 in real-world attack scenarios. In our experiments, WPA3's use of the Simultaneous Authentication of Equals (SAE) handshake and mandatory Protected Management Frames (PMF) effectively thwarted attacks that readily compromised WPA2 networks, including offline passphrase cracking and deauthentication-based disconnects. Notably, WPA3's improved handshake process also mitigated the KRACK key reinstallation vulnerability that severely affected WPA2. By contrast, WPA2-PSK — still the most widely deployed Wi-Fi security protocol — was consistently breached under these tests using well-known tools and techniques, highlighting how easily it can be compromised under real-world conditions. These results reinforce the conclusion that WPA2's legacy protections are insufficient against modern attack methods, whereas WPA3 offers a far more robust defense in practice.

Finally, this work highlights several avenues for future research to further strengthen Wi-Fi security. First, comprehensive assessments of WPA3-Enterprise deployments (e.g., in 802.1X environments) are needed to verify that enterprise authentication mechanisms hold up against sophisticated attacks, as our study focused on personal networks. Second, investigation into side-channel and implementation-layer vulnerabilities in WPA3 devices is warranted – for example, early analyses uncovered flaws in the WPA3 Dragonfly handshake (the Dragonblood attacks) via timing

side-channels and insecure transition modes, indicating that even a strong protocol can be undermined by poor implementations or backward-compatibility features. Third, as cryptographic technology advances, exploring the integration of post-quantum cryptographic algorithms into Wi-Fi authentication is an important forward-looking step to ensure long-term resistance against emerging threats. Addressing these gaps will help solidify the security of next-generation wireless networks and ensure that Wi-Fi remains secure as new vulnerabilities and attack techniques evolve.

Literature

1. Abdallah, W. (2024). A physical layer security scheme for 6G wireless networks using post-quantum cryptography. Computer Communications, 218, 176–187. DOI: 10.1016/j.comcom.2024.02.019
2. Banakh, R., Nyemkova, E., Justice, C., Piskozub, A., & Lakh, Y. (2024). Data mining approach for evil twin attack identification in Wi-Fi networks. Data, 9(10), 119. DOI: 10.3390/data9100119
3. Baseri, Y., Chouhan, V., & Hafid, A. (2024). Navigating quantum security risks in networked environments: A comprehensive study of quantum-safe network protocols. Computers & Security, 142, 103883. DOI: 10.1016/j.cose.2024.103883
4. Chatzoglou, E., Kambourakis, G., & Kolias, C. (2021). Empirical evaluation of attacks against IEEE 802.11 enterprise networks: The AWID3 dataset. IEEE Access, 9, 34188–34205. DOI: 10.1109/ACCESS.2021.3061609
5. Chatzoglou, E., Kambourakis, G., & Kolias, C. (2022). How is your Wi Fi connection today? DoS attacks on WPA3-SAE. Journal of Information Security and Applications, 64, 103058. DOI: 10.1016/j.jisa.2021.103058
6. De Almeida Braga, D., Fouque, P.-A., & Sabt, M. (2020). Dragonblood is still leaking: Practical cache-based side channel in the wild. In Proceedings of the 36th Annual Computer Security Applications Conference (ACSAC 2020) (pp. 291–303). ACM. DOI: 10.1145/3427228.3427295
7. Gao, D., Lin, H., Li, Z., Qian, F., Chen, Q. A., Qian, Z., Liu, W., Gong, L., & Liu, Y. (2021). A nationwide census on WiFi security threats: Prevalence, riskiness, and the economics. In Proceedings of the 27th Annual International Conference on Mobile Computing and Networking (MobiCom ’21) (pp. 242–255). ACM. DOI: 10.1145/3447993.3448620
8. Gebresilassie, S. K., Rafferty, J., Chen, L., Cui, Z., & Abu-Tair, M. (2023). Transfer and CNN-based de authentication (disassociation) DoS attack detection in IoT Wi Fi networks. Electronics, 12(17), 3731. DOI: 10.3390/electronics12173731
9. Gyamfi, E., & Jurcut, A. (2022). Intrusion detection in Internet of Things systems: A review on design approaches leveraging multi access edge computing, machine learning, and datasets. Sensors, 22(10), 3824. DOI: 10.3390/s22103744
10. Halbouni, A., Ong, L.-Y., & Leow, M.-C. (2023). Wireless security protocols WPA3: A systematic literature review. IEEE Access, 11, 112438–112463. DOI: 10.1109/ACCESS.2023.3322931
11. Kazmi, S. H. A., Hassan, R., Qamar, F., Nisar, K., & Ibrahim, A. (2023). Security concepts in emerging 6G communication: Threats, countermeasures, authentication techniques and research directions. Symmetry, 15(6), 1147. DOI: 10.3390/sym15061147
12. Kikissagbe, B. R., & Adda, M. (2023). Machine learning-based intrusion detection methods in IoT systems: A comprehensive review. Electronics, 13(18), 3601. DOI: 10.3390/electronics13183601
13. Kotb, S. A., Hussein, H., & Kim, H.-W. (2022). Security requirements and challenges of 6G technologies and applications. Sensors, 22(5), 1969. DOI: 10.3390/s22051969
14. Lounis, K., & Zulkernine, M. (2019). Bad-token: Denial of service attacks on WPA3. Proceedings of the 12th International Conference on Security of Information and Networks (SIN '19),

15. Association for Computing Machinery (ACM). DOI: 10.1145/3357613.3357629

15. Lounis, K., & Zulkernine, M. (2020). WPA3 connection deprivation attacks. In S. Kallel, F. Cuppens, N. Cuppens-Boulahia, & A. H. Kacem (Eds.), Risks and Security of Internet and Systems (CRiSIS 2019, LNCS 12026) (pp. 164–176). Springer. DOI: 10.1007/978-3-030-41568-6_11

16. Marais, S., Coetzee, M., & Blauw, F. F. (2021). Simultaneous deauthentication of equals attack. In G. Wang, B. Chen, W. Li, R. Di Pietro, X. Yan, & H. Han (Eds.), Security, Privacy, and Anonymity in Computation, Communication, and Storage (SpaCCS 2020, LNCS 12383) (pp. 545–556). Springer. DOI: 10.1007/978-3-030-68884-4_45

17. Nguyen, V.-L., Lin, P.-C., Cheng, B.-C., Hwang, R.-H., & Lin, Y.-D. (2022). Security and privacy for 6G: A survey on prospective technologies and challenges. IEEE Communications Surveys & Tutorials, 24(4), 2255–2291. DOI: 10.1109/COMST.2021.3108618

18. Örs, F. K., Aydın, M., Boğatarkan, A., & Levi, A. (2021). Scalable Wi Fi intrusion detection for IoT systems. In Proceedings of the 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS 2021) (pp. 1–6). IEEE. DOI: 10.1109/NTMS49979.2021.9432662

19. Rathod, T., Jadav, N. K., Alshehri, M. D., Tanwar, S., Sharma, R., Felseghi, R.-A., & Raboaca, M. S. (2022). Blockchain for future wireless networks: A decade survey. Sensors, 22(11), 4182. DOI: 10.3390/s22114182

20. Reyes, A. A., Vaca, F. D., Castro-Aguayo, G. A., Niyaz, Q., & Devabhaktuni, V. (2020). A machine learning based two stage Wi Fi network intrusion detection system. Electronics, 9(10), 1689. DOI: 10.3390/electronics9101689

21. Sajimon, P. C., Jain, K., & Krishnan, P. (2022). Analysis of post quantum cryptography for Internet of Things. In Proceedings of the 6th International Conference on Intelligent Computing and Control Systems (ICICCS 2022) (pp. 1227–1233). IEEE. DOI: 10.1109/ICICCS53718.2022.9787987

22. Scalise, P., Garcia, R., Boeding, M., Hempel, M., & Sharif, H. (2024). An applied analysis of securing 5G/6G core networks with post quantum key encapsulation methods. Electronics, 13(21), 4258. DOI: 10.3390/electronics13214258

23. Schepers, D., Ranganathan, A., & Vanhoef, M. (2022). On the robustness of Wi Fi deauthentication countermeasures. In Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2022) (pp. 181–191). ACM. DOI: 10.1145/3507657.3528548

24. Seneviratne, S., Jornet, J. M., Hou, J., Wang, P., Hu, J., & Mohapatra, P. (2020). Blockchain for 5G and beyond networks: A state of the art survey. Journal of Network and Computer Applications, 166, 102693. DOI: 10.1016/j.jnca.2020.102693

25. Shrivastava, P., Kumar, J. K., & Kataoka, K. (2020). EvilScout: Detection and mitigation of evil twin attack in SDN enabled Wi Fi. IEEE Transactions on Network and Service Management, 17(1), 89–102. DOI: 10.1109/TNSM.2020.2972774

26. Tripi, G., Iacobelli, A., Rinieri, L., & Prandini, M. (2023). Security and trust in the 6G era: Risks and mitigations. Electronics, 13(11), 2162. DOI: 10.3390/electronics13112162

27. Vanhoef, M., & Ronen, E. (2020). Dragonblood: Analyzing the dragonfly handshake of WPA3 and EAP pwd. In Proceedings of the 2020 IEEE Symposium on Security and Privacy (SP) (pp. 517–533). IEEE. DOI: 10.1109/SP40000.2020.00031

28. Wang, J., Ling, X., Le, Y., Huang, Y., & You, X. (2021). Blockchain enabled wireless communications: A new paradigm towards 6G. National Science Review, 8(9), nwab069. DOI: 10.1093/nsr/nwab069

29. Xu, L. D., Lu, Y., & Li, L. (2021). Embedding blockchain technology into IoT for security: A survey. IEEE Internet of Things Journal, 8(13), 10452–10473. DOI: 10.1109/JIOT.2021.3060508

30. You, I., Kim, J., Pawana, I. W. A. J., & Ko, Y. (2024). Mitigating security vulnerabilities in 6G networks: A comprehensive analysis of the DMRN protocol using SVO logic and ProVerif. Applied Sciences, 14(21), 9726. DOI: 10.3390/app14219726

MODERN INFORMATION SECURITY MANAGEMENT SYSTEMS: CONSTRUCTION AND IMPLEMENTATION IN THE DIGITAL ERA

Garifullin Adilbek
adilbekgarifullin6@gmail.com

Department of Information Security Systems, Faculty of Information Technology,
L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
Supervisor – A. Mukhanbetkalieva

Abstract

This article examines the construction and implementation of modern Information Security Management Systems (ISMS) in the context of evolving cyber threats. Through a mixed-method research approach combining literature review and practical assessment, the study analyzes key components and best practices in ISMS development. The research highlights the transition from reactive security approaches to proactive, risk-based strategies that integrate people, processes, and technologies. The article proposes guidelines for organizations to enhance their security posture through advanced ISMS frameworks, with particular attention to emerging technologies such as AI and machine learning for threat detection. The findings demonstrate that comprehensive ISMS implementation significantly strengthens organizational resilience against increasingly sophisticated cyber attacks, while addressing the challenges of regulatory compliance and rapid technological adoption.

Keywords: Information Security, ISMS, cybersecurity, risk management, artificial intelligence, organizational resilience

Introduction

With increasing digitalization across all industries, the security of information systems has become a foundational concern for modern organizations. From e-commerce platforms to government infrastructure, every domain now faces the challenge of protecting sensitive data in the face of constantly evolving cyber threats.Information Security Management Systems (ISMS) serve as a strategic framework for identifying and mitigating information risks. Unlike traditional security measures that focus narrowly on firewalls or antivirus tools, ISMS approaches combine technology, policies, and human behavior to deliver comprehensive protection. As cyberattacks grow in frequency and sophistication, organizations must shift from reactive to proactive defenses—relying on continuous monitoring, risk assessments, and adaptable security architecture.

This article examines how ISMS frameworks are evolving, the role of emerging technologies like artificial intelligence, and what organizations can do to stay ahead of the threat landscape.

Modern ISMS: From Policy to Practice

ISMS provides a structured methodology for ensuring the confidentiality, integrity, and availability (CIA) of data. It helps organizations establish security **baselines**, identify critical assets, assess risks, and define policies that govern access, monitoring, and response.

Table 1.1 – Information Security Aspects