ISSN 2706-6266
ISSN 3007-1062
ISSN 3007-1070

МРНТИ 81.93.29 **DOI: https://doi.org/10.62724/202510308**

Шатекова Асел Нурбулатовна[1*],
техника ғылымдарының магистрі, аға оқытушы, Батыс Қазақстан инновациялық-технологиялық университеті, Қазақстан Республикасы, 090006, Орал қ., Ықсанов көшесі 44/1, kukesa777@mail.ru, ORCID ID: 0009-0008-1347-3399

АНАЛИЗ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация. Статья посвящена анализу современных систем обеспечения информационной безопасности и защиты информации, с акцентом на их архитектуру, методы и технологии, используемые для предотвращения угроз и защиты конфиденциальности, целостности и доступности данных. Рассматриваются ключевые компоненты информационной безопасности, включая системы контроля доступа, криптографические методы, антивирусные и антишпионские решения, а также средства защиты от вторжений и мониторинга.

Автор статьи анализирует основные угрозы, с которыми сталкиваются организации и пользователи в процессе обработки и хранения данных, включая внешние и внутренние атаки, вирусы, утечку информации и несанкционированный доступ. Особое внимание уделено важности комплексного подхода к обеспечению безопасности, который включает в себя технические, организационные и правовые меры. В статье также рассматриваются современные тенденции в области информационной безопасности, такие как использование искусственного интеллекта и машинного обучения для анализа угроз, а также развитие технологий блокчейн и их применение в защите данных.

Особое внимание уделено анализу угроз безопасности, включая кибератаки, утечку конфиденциальной информации, вредоносные программы, а также угрозы, связанные с человеческим фактором. В статье раскрыты основные технологии защиты данных, такие как криптографические методы (шифрование, цифровые подписи), системы управления доступом, методы аутентификации и авторизации, а также средства мониторинга и реагирования на инциденты безопасности.

В завершение статьи подчеркивается необходимость регулярного обновления и совершенствования систем безопасности, а также обучения сотрудников методам защиты информации и соблюдению норм безопасности в организации.

Ключевые слова. Информационная безопасность, Защита информации, Политика безопасности, Угрозы безопасности, Уязвимости, Риски, Технические средства защиты, Аудит безопасности, Мониторинг, Обучение сотрудников, Киберугрозы, Процедуры безопасности, Оценка рисков, Инциденты безопасности, Комплексный подход

Введение. С развитием цифровых технологий и стремительным ростом объемов обрабатываемой информации вопросы информационной безопасности становятся всё более актуальными. Угрозы в этой сфере разнообразны и включают в себя кибератаки, утечки данных, вирусные инфекции и внутренние нарушения. Эффективная система обеспечения информационной безопасности и защиты информации становится необходимостью для организаций всех уровней — от государственных учреждений до частных компаний.

ISSN 2706-6266
ISSN 3007-1062
ISSN 3007-1070

В современном мире, где информация стала основным ресурсом и движущей силой большинства процессов, защита данных и информационных систем выходит на первый план. В условиях глобализации и интенсивного использования информационных технологий обеспечению информационной безопасности (ИБ) уделяется особое внимание. В статье рассматривается концепция системы обеспечения информационной безопасности, её компоненты, угрозы, а также современные методы защиты информации.

Понятие и цели системы обеспечения информационной безопасности

Система обеспечения информационной безопасности (СОИБ) представляет собой комплекс мер, средств и методов, направленных на защиту информации от угроз, которые могут угрожать её конфиденциальности, целостности, доступности и подлинности. Обеспечение ИБ — это не только применение технических решений, но и разработка организационных и правовых мероприятий для минимизации рисков.

Цель СОИБ заключается в том, чтобы гарантировать сохранность информации, обеспечить её защиту от несанкционированного доступа, а также предотвратить утечку, утрату или повреждение данных. Безопасность информации влияет на функционирование организации, а её утрата или компрометация может привести к серьёзным последствиям, таким как финансовые убытки, репутационные потери или нарушение функционирования критических систем.

Основные компоненты системы обеспечения информационной безопасности

Система обеспечения информационной безопасности делится на несколько ключевых элементов:

Организационные меры: Это совокупность правил, стандартов, политик, направленных на регулирование поведения сотрудников и управление доступом к информации. Разработка инструкций, правил работы с данными, создание подразделений по ИБ, обучение сотрудников — всё это важные компоненты организационного обеспечения безопасности.

Технические меры: Включают использование различных инструментов для защиты информации. Это антивирусные программы, фаерволы, системы защиты от вторжений (IDS), шифрование данных, биометрические системы и другие средства, направленные на защиту информации на техническом уровне.

Юридические меры: Законы и нормативные акты, такие как законы о защите персональных данных, нормативы по защите коммерческой тайны, соглашения о неразглашении (NDA), регулирующие вопросы безопасности на правовом уровне.

Физическая защита: Это защитные меры, направленные на физическую охрану инфраструктуры, серверных и рабочих мест, контроль доступа к оборудованию и помещениям, где хранится конфиденциальная информация.

Угрозы информационной безопасности

Для эффективной работы системы безопасности важно понимать, какие угрозы могут повлиять на информацию и на её защиту. Современные угрозы можно разделить на несколько категорий:

Неавторизованный доступ: Включает попытки злоумышленников получить доступ к конфиденциальной информации через хакерские атаки, фишинг, социальную инженерию или использование уязвимостей в системе безопасности.

Вредоносное ПО: Вирусы, трояны, шифровальщики, программы-шифровальщики (ransomware), которые могут повредить или уничтожить данные, а также похитить информацию для дальнейшей её продажи.

ISSN 2706-6266
ISSN 3007-1062
ISSN 3007-1070

Атаки с отказом в обслуживании (DDoS): Эти атаки направлены на перегрузку серверов или систем, что вызывает их недоступность для пользователей и может нарушить работу бизнес-процессов.

Инсайдерские угрозы: Угрозы, исходящие от сотрудников организации, которые могут случайно или намеренно раскрыть, модифицировать или уничтожить информацию.

Ошибки пользователей: Человеческий фактор также играет значительную роль в нарушении информационной безопасности. Это неправильное обращение с данными, использование слабых паролей, несоответствие стандартам безопасности.

Стратегия защиты информации

Для того чтобы эффективно обеспечить защиту информации, организация должна иметь чёткую стратегию. Важные этапы разработки и реализации этой стратегии:

1. **Оценка рисков и угроз**: Оценка возможных угроз, их вероятности и последствий. Такой анализ помогает выявить уязвимости в системе и определить, какие меры необходимо предпринять для их устранения.
2. **Разработка политики безопасности**: На этом этапе разрабатываются внутренние нормативные документы, которые регламентируют работу с информацией. Включают в себя инструкции по защите данных, а также алгоритмы действий в случае инцидентов.
3. **Внедрение средств защиты**: Это включает установку антивирусного ПО, фаерволов, систем шифрования, а также других технологий защиты данных, таких как многофакторная аутентификация и мониторинг.
4. **Обучение сотрудников**: Все сотрудники организации должны быть обучены основам информационной безопасности, знанию угроз и соблюдению стандартов безопасности.
5. **Мониторинг и анализ**: Постоянный мониторинг информационных систем на предмет угроз, а также анализ инцидентов безопасности. Важно иметь систему для обнаружения нарушений и оперативного реагирования на них.

Современные методы и технологии защиты информации

Технологии защиты информации развиваются с каждым годом. Одним из наиболее перспективных направлений являются:

Шифрование: Это процесс преобразования данных в нечитаемую форму, доступную только при наличии ключа для расшифровки. Шифрование используется для защиты конфиденциальных данных, как на этапе их хранения, так и при передаче по сети.

Многофакторная аутентификация (MFA): Для повышения безопасности доступа к данным используется несколько уровней проверки личности пользователя. Это может быть комбинация пароля, отпечатка пальца, смс-кода и других факторов.

Искусственный интеллект и машинное обучение: Современные системы защиты используют ИИ для выявления аномалий в поведении пользователей, предотвращения атак в реальном времени, анализа угроз и их прогноза.

Блокчейн: Технология распределённых реестров, обеспечивающая неизменность данных и защищающая от фальсификации. Она становится всё более популярной в сферах, требующих высокой степени доверия к информации.

Проблемы и вызовы в обеспечении информационной безопасности

Несмотря на развитие технологий и методов защиты, существуют серьезные проблемы и вызовы в области ИБ:

ISSN 2706-6266
ISSN 3007-1062
ISSN 3007-1070

Дефицит специалистов: Высокий спрос на квалифицированных специалистов по информационной безопасности, что приводит к нехватке кадров и затрудняет создание и поддержание эффективных систем безопасности.

Сложность защиты от новых угроз: Хакеры и злоумышленники постоянно совершенствуют свои методы атак, что требует от организаций гибкости в защите и постоянного обновления технологий.

Международные угрозы: В условиях глобализации кибератаки могут иметь международный характер, что затрудняет их нейтрализацию и повышает риски.

Заключение. Обеспечение информационной безопасности является важнейшей частью функционирования любой современной организации. Система обеспечения безопасности должна быть комплексной, учитывая все угрозы и риски, а также вовлекая организационные, технические и правовые меры защиты. Постоянное обновление методов защиты, обучение сотрудников и развитие технологий являются ключевыми для эффективной защиты информации в условиях динамично меняющейся цифровой среды.

СПИСОК ЛИТЕРАТУРЫ

1 Сычёв, А. Н. Основы информационной безопасности: [Текст] Учебное пособие. — М.: Наука, 2020.

2 Лаврентьев, А. С. Защита информации в компьютерных системах. [Текст] — СПб.: Питер, 2021.

3 https://www.consultant.ru/document/cons_doc_LAW_314813/

4 ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements.

5 Куренков, С. В. Управление рисками в области информационной безопасности. [Текст] — М.: Инфра-М, 2019.

6 Бояркин, И. В. Кибербезопасность: угроза и защита. [Текст] — М.: Юрайт, 2022.

7 Герасименко, А. А. Информационная безопасность: [Текст] Учебник для вузов. — М.: Издательство Юрайт, 2020.

8 Клименко, В. С. Актуальные угрозы и методы защиты информации в современном мире. [Текст] — М.: Лаборатория знаний, 2021.

9 Кириллов, С. А. Основы информационной безопасности: [Текст] Учебник. — М.: Юрайт, 2020.

10 Петров, В. В. Информационная безопасность: [Текст] Учебное пособие. — СПб.: Питер, 2019.

11 Курочкин, А. В. Защита информации: Теория и практика. [Текст] — М.: БХВ-Петербург, 2021.

12 Романов, Д. Н. Современные технологии защиты информации. [Текст] — М.: КноРус, 2022.

13 Шапошников, И. А. Анализ угроз и уязвимостей в информационных системах. [Текст] — М.: Наука, 2021.

14 Смирнов, А. С. Управление информационной безопасностью: Стандарты и практики. [Текст] — М.: Аспект Пресс, 2020.

15 Александров, Р. Н. Криптография и безопасность информации. [Текст] — М.: Радио и связь, 2019.

16 Гусев, И. В. Системы защиты информации: Технологии и методики. [Текст] — М.: Инфра-М, 2021.

ISSN 2706-6266
ISSN 3007-1062
ISSN 3007-1070

REFERENCE

1 Sychyov, A. N. Osnovy informacionnoj bezopasnosti: [Fundamentals of information security]. Uchebnoe posobie. M.: Nauka, (2020). – (In Rus)

2 Lavrent'ev, A. S. Zashchita informacii v komp'yuternyh sistemah. [Information protection in computer systems.]. SPb.: Piter, (2021). – (In Rus)

3 https://www.consultant.ru/document/cons_doc_LAW_314813/

4 ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements.

5 Kurenkov, S. V. Upravlenie riskami v oblasti informacionnoj bezopasnosti. [Information security risk management.]. M.: Infra-M, (2019). – (In Rus)

6 Boyarkin, I. V. Kiberbezopasnost': ugroza i zashchita. [Cybersecurity: threat and protection.]. M.: Yurajt, (2022). – (In Rus)

7 Gerasimenko, A. A. Informacionnaya bezopasnost': [Information security] Uchebnik dlya vuzov. M.: Izdatel'stvo Yurajt, (2020). – (In Rus)

8 Klimenko, V. S. Aktual'nye ugrozy i metody zashchity informacii v sovremennom mire. [Current threats and methods of information protection in the modern world.]. M.: Laboratoriya znanij, (2021). – (In Rus)

9 Kirillov, S. A. Osnovy informacionnoj bezopasnosti: [Fundamentals of information security] Uchebnik. M.: Yurajt, (2020). – (In Rus)

10 Petrov, V. V. Informacionnaya bezopasnost': [Information security] Uchebnoe posobie. — SPb.: Piter, (2019). – (In Rus)

11 Kurochkin, A. V. Zashchita informacii: Teoriya i praktika. [Information protection: Theory and practice.]. M.: BHV-Peterburg, (2021). – (In Rus)

12 Romanov, D. N. Sovremennye tekhnologii zashchity informacii. [Modern information security technologies.].M.: KnoRus, (2022). – (In Rus)

13 Shaposhnikov, I. A. Analiz ugroz i uyazvimostej v informacionnyh sistemah. [Analysis of threats and vulnerabilities in information systems.]. M.: Nauka, (2021). – (In Rus)

14 Smirnov, A. S. Upravlenie informacionnoj bezopasnost'yu: Standarty i praktiki. [Information Security Management: Standards and Practices.]. M.: Aspekt Press, (2020). – (In Rus)

15 Aleksandrov, R. N. Kriptografiya i bezopasnost' informacii. [Cryptography and information security.]. M.: Radio i svyaz', (2019). – (In Rus)

16 Gusev, I. V. Sistemy zashchity informacii: Tekhnologii i metodiki. [Information security systems: Technologies and techniques.]. M.: Infra-M, (2021). – (In Rus)

АҚПАРАТТЫҚ ҚАУІПСІЗДІК ПЕН АҚПАРАТТЫ ҚОРҒАУДЫ ҚАМТАМАСЫЗ ЕТУ ЖҮЙЕСІН ТАЛДАУ

Аңдатпа. Мақала қауіптердің алдын алу және деректердің құпиялылығын, тұтастығы мен қолжетімділігін қорғау үшін қолданылатын архитектурасына, әдістері мен технологияларына назар аудара отырып, ақпараттық қауіпсіздік пен ақпаратты қорғаудың заманауи жүйелерін талдауға арналған. Ақпараттық қауіпсіздіктің негізгі компоненттері, соның ішінде кіруді бақылау жүйелері, криптографиялық әдістер, антивирустық және тыңшылыққа қарсы шешімдер, сондай-ақ кіруден қорғау және бақылау құралдары қарастырылады.

Мақала авторы ұйымдар мен пайдаланушылардың деректерді өңдеу және сақтау процесінде кездесетін негізгі қауіптерін, соның ішінде сыртқы және ішкі шабуылдарды, вирустарды, ақпараттың ағып кетуін және рұқсатсыз кіруді талдайды. Техникалық, ұйымдастырушылық және құқықтық шараларды қамтитын қауіпсіздікті қамтамасыз

ISSN 2706-6266
ISSN 3007-1062
ISSN 3007-1070

етудің кешенді тәсілінің маңыздылығына ерекше назар аударылады. Мақалада сонымен қатар қауіп-қатерді талдау үшін жасанды интеллект пен машиналық оқытуды қолдану, сондай-ақ блокчейн технологияларын дамыту және оларды деректерді қорғауда қолдану сияқты ақпараттық қауіпсіздіктің заманауи тенденциялары қарастырылады.

Қауіпсіздік қатерлерін, соның ішінде кибершабуылдарды, құпия ақпараттың ағып кетуін, зиянды бағдарламаларды, сондай-ақ адам факторына байланысты қауіптерді талдауға ерекше назар аударылады. Мақалада криптографиялық әдістер (шифрлау, цифрлық қолтаңбалар), қол жеткізуді басқару жүйелері, аутентификация және авторизация әдістері және қауіпсіздік оқиғаларын бақылау және оларға жауап беру құралдары сияқты деректерді қорғаудың негізгі технологиялары ашылады. Мақаланың соңында қауіпсіздік жүйелерін үнемі жаңартып отыру және жетілдіру, сондай-ақ қызметкерлерді ақпаратты қорғау әдістеріне үйрету және ұйымдағы қауіпсіздік нормаларын сақтау қажеттілігі атап өтіледі.

Кілт сөздер. Ақпараттық қауіпсіздік, ақпаратты қорғау, қауіпсіздік саясаты, қауіпсіздік қатерлері, осалдықтар, тәуекелдер, техникалық қорғаныс құралдары, қауіпсіздік аудиті, мониторинг, қызметкерлерді оқыту, киберқауіптер, қауіпсіздік процедуралары, тәуекелдерді бағалау, қауіпсіздік инциденттері, кешенді тәсіл

ANALYSIS OF THE INFORMATION SECURITY AND INFORMATION PROTECTION SYSTEM

Abstract. The article is devoted to the analysis of modern information security and information protection systems, focusing on their architecture, methods and technologies used to prevent threats and protect confidentiality, integrity and availability of data. Key components of information security are considered, including access control systems, cryptographic methods, anti-virus and anti-spyware solutions, and intrusion protection and monitoring tools.

The author of the article analyzes the main threats faced by organizations and users in the process of data processing and storage, including external and internal attacks, viruses, information leakage and unauthorized access. Special attention is paid to the importance of an integrated approach to security, which includes technical, organizational and legal measures. The article also discusses current trends in information security, such as the use of artificial intelligence and machine learning to analyze threats, as well as the development of blockchain technologies and their application in data protection.

Special attention is paid to the analysis of security threats, including cyberattacks, confidential information leakage, malware, and threats related to human factor. The article reveals the main data protection technologies, such as cryptographic methods (encryption, digital signatures), access control systems, authentication and authorization methods, as well as means of monitoring and responding to security incidents.

The article concludes by emphasizing the need to regularly update and improve security systems, as well as to train employees in information protection methods and compliance with security standards in the organization.

Keywords. Information Security, Information Protection, Security Policy, Security Threats, Vulnerabilities, Risks, Technical Protection Tools, Security Audit, Monitoring, Employee Training, Cyber Threats, Security Procedures, Risk Assessment, Security Incidents, Comprehensive Approach