DOI: 10.58168/MoInSyTe2024_275-280
УДК 004.9

АНАЛИЗ МЕТОДОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Н.В. Данилов[1], В.И. Анциферова[1], Н.В. Бурдюг[1], Р.Г. Дмитриев[1], Р.В. Емельянов[1]

[1]ФГБОУ ВО «Воронежский государственный лесотехнический университет имени Г.Ф. Морозова»

Аннотация. В современном мире безопасность данных играет большую роль в различных сферах деятельности и является одной из приоритетных задач. В статье проведен анализ методов обеспечения безопасности, каждый из которых рассматривается в контексте своей эффективности. Проводится анализ сильных и слабых сторон различных методов информационной безопасности. Подводятся итоги и предлагаются рекомендации по выбору и применению наиболее эффективных методов обеспечения безопасности информационных систем.

Ключевые слова: безопасность информационных систем, угрозы информационной безопасности, методы обеспечения безопасности, уязвимости информационных систем, эффективность методов безопасности, рекомендации по безопасности.

ANALYSIS OF METHODS FOR ENSURING INFORMATION SYSTEMS SECURITY

N.V. Danilov[1], V.I. Antsiferova[1], N.V. Burdyug[1], R.G. Dmitriev[1], R.V. Emelyanov[1]

[1]Voronezh State University of Forestry and Technologies named after G.F. Morozov

Abstract. In the modern world, data security plays a big role in various fields of activity and is one of the priorities. The article analyzes security methods, each of which is considered in the context of its effectiveness. An analysis of the strengths and weaknesses of various information security methods is carried out. The results are summarized and recommendations are offered for the selection and application of the most effective methods for ensuring the security of information systems.

Keywords: security of information systems, threats to information security, security methods, vulnerabilities of information systems, effectiveness of security methods, security recommendations.

Введение

В современном мире обеспечение безопасности информационных систем является неотъемлемой частью успешной деятельности как организаций так и отдельных пользователей. Информационные системы хранят, обрабатывают и передают огромные объемы данных, включая конфиденциальную информацию, финансовые данные, личные сведения и т.д. Нарушение безопасности информационных систем может привести к серьезным последствиям, таким как утечка данных, финансовые потери.

Целью данного исследования является анализ методов обеспечения безопасности информационных систем, их эффективности, сильных и слабых сторон, а также предложение рекомендаций по выбору и применению наиболее оптимальных методов.

Для достижения цели были поставлены следующие задачи:

- провести обзор основных методов обеспечения безопасности информационных систем;

- провести анализ эффективности различных методов обеспечения безопасности;

- предложить рекомендации по выбору и применению методов обеспечения информационной безопасности.

Информационная безопасность - состояние защищенности информационных ресурсов (информационной среды) от внутренних и внешних угроз, способных нанести ущерб интересам личности, общества, государства (национальным интересам).

Безопасность информации - защищенность информации от нежелательного (для соответствующих субъектов информационных отношений) ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования.

Основная задача информационной безопасности - сбалансированная защита конфиденциальности, целостности и доступности данных, с учетом целесообразности применения и без какого-либо ущерба производительности организации.

Угрозы информационной безопасности могут происходить как извне, так и изнутри информационной системы. Они включают в себя различные виды атак, мошенничество, вирусы, вредоносные программы, хакерские атаки, утечки данных, а также естественные и технологические катастрофы.

Уязвимости информационных систем могут быть вызваны недостаточной защитой программного обеспечения, отсутствием обновлений, слабыми паролями, недостаточной осведомленностью сотрудников и другими факторами.

Понимание угроз и уязвимостей информационных систем является ключевым шагом к их эффективной защите.

Анализ методов обеспечения информационной безопасности и их эффективности

Обеспечение безопасности информационных систем включает в себя различные методы, которые можно разделить на технические и организационные. Каждый из этих методов имеет свои преимущества и недостатки, рассмотрим основные из них.

Шифрование данных служит основополагающим методом защиты информации путем преобразования открытого текста в зашифрованный, что делает его неразборчивым для неавторизованных лиц. Используя такие алгоритмы, как AES (Advanced Encryption Standard) или RSA (Rivest-Shamir-Adleman), шифрование обеспечивает конфиденциальность и секретность. Однако эффективность шифрования зависит от методов управления ключами и силы используемых криптографических алгоритмов.

Механизмы аутентификации, включая пароли, биометрические данные и многофакторную аутентификацию, проверяют личность пользователей, получающих доступ к системе или сети. В сочетании с надежными протоколами авторизации, которые определяют уровень предоставляемого доступа на основе учетных данных пользователя, эти методы образуют важнейший защитный слой против несанкционированного доступа. Тем не менее, такие уязвимости, как слабые пароли и тактика социальной инженерии, снижают их эффективность.

Брандмауэры выступают в качестве барьеров между внутренними сетями и внешними угрозами, регулируя входящий и исходящий трафик на основе заранее определенных правил безопасности. Будь то аппаратные или программные решения, брандмауэры играют ключевую роль в предотвращении несанкционированного доступа и пресечении вредоносных действий, таких как атаки типа "отказ в обслуживании" (DoS). Однако их эффективность зависит от постоянных обновлений, настройки и мониторинга для адаптации к меняющимся угрозам.

Антивирусное программное обеспечение обнаруживает, предотвращает и удаляет вредоносные программы, известные как вредоносное ПО, с вычислительных устройств. Используя сигнатурное обнаружение, эвристический анализ и мониторинг поведения, эти программы стремятся выявлять и нейтрализовать

угрозы в режиме реального времени. Несмотря на повсеместное распространение, эффективность антивирусных решений варьируется в зависимости от их способности обнаруживать новые штаммы вредоносного ПО и "уязвимость нулевого дня" (Zero-Day Exploit).

Политики информационной безопасности определяют руководящие принципы, процедуры и лучшие практики, регулирующие обработку и защиту конфиденциальных данных в организации. Разграничивая роли, обязанности и требования к соответствию, эти политики создают основу для развития культуры, ориентированной на безопасность. Однако их эффективность зависит от четкой коммуникации, механизмов обеспечения соблюдения и периодического пересмотра с учетом возникающих угроз и изменений в законодательстве.

В соответствии с законодательством Российской Федерации организации обязаны придерживаться определенных правовых норм, направленных на защиту личной и конфиденциальной информации. К таким нормативным актам относятся Федеральный закон "О персональных данных" (№ 152-ФЗ) и различные отраслевые нормы и стандарты, которые обязывают организации применять специальные меры безопасности для защиты личной и конфиденциальной информации. Соответствие этим нормам предполагает использование шифрования, контроля доступа, политики хранения данных и процедур реагирования на инциденты для снижения рисков и обеспечения подотчетности. Тем не менее возникают проблемы, связанные с приведением организационной практики в соответствие с нормативными требованиями и обеспечением операционной эффективности.

Аудиты безопасности подразумевают систематическую оценку состояния информационной безопасности организации, включающую технические средства контроля, политики и процедуры. Проводимые собственными силами или сторонними аудиторами, они выявляют уязвимости, оценивают риски и подтверждают эффективность мер безопасности. Однако успех аудита безопасности зависит от тщательности, независимости и усилий по устранению выявленных недостатков и повышению устойчивости к киберугрозам.

Заключение

В заключение следует отметить, что сфера информационной безопасности многогранна и включает в себя широкий спектр технических и организационных методов, направленных на защиту конфиденциальных данных. Несмотря на то что каждый из методов обладает определенными преимуществами в снижении рисков безопасности, их эффективность зависит от различных факторов, таких

как внедрение, обслуживание и адаптация к меняющимся угрозам. Организации должны применять комплексный подход, объединяющий как технические инновации, так и надежные организационные методы для укрепления защиты и обеспечения целостности, конфиденциальности и доступности информационных ресурсов.

Список литературы

1. Баранова, Е. К. Информационная безопасность и защита информации: учебное пособие / Е.К. Баранова, А.В. Бабаш. – 4-е изд., перераб. и доп. – Москва: РИОР: ИНФРА-М, 2022. — 336 с.

2. Гришина, Н. В. Основы информационной безопасности предприятия: учебное пособие / Н.В. Гришина. – Москва: ИНФРА-М, 2021. — 216 с.

3. Овчинников, А. И. Основы национальной безопасности: учеб. пособие / А.И. Овчинников, А.Ю. Мамычев, П.П. Баранов. – 2-е изд. – Москва : РИОР: ИНФРА-М, 2019. — 224 с.

4. Защита информации: учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва: РИОР: ИНФРА-М, 2023. – 400 с.

5. Суханов, В.В. Методика логического проектирования информационного обеспечения распределенных информационных систем критического применения / В.В. Суханов, О.В. Ланкин // Моделирование систем и процессов. – 2021. – Т. 14, № 3. – С. 67-73. – DOI: 10.12737/2219-0767-2021-14-3-67-73.

6. Суханов, В.В. Аналитическое обеспечение организации данных в распределенных информационных системах критического применения / В.В. Суханов // Моделирование систем и процессов. – 2021. – Т. 14, № 3. – С. 60-67. – DOI: 10.12737/2219-0767-2021-14-3-60-67.

7. Модель индивидуально группового назначения доступа к иерархически организованным объектам критических информационных систем с использованием мобильных технологий / Е.А. Рогозин, В.А. Хвостов, В.В. Суханов [и др.]// Моделирование систем и процессов. – 2021. – Т. 14, № 1. – С. 73-79. – DOI: 10.12737/2219-0767-2021-14-1-73-79.

8. Полуэктов А.В., Макаренко Ф.В., Ягодкин А.С. Использование сторонних библиотек при написании программ для обработки статистических данных // Моделирование систем и процессов. – 2022. – Т. 15, № 2. – С. 33-41.

References

1. Baranova, E.K. Information security and information protection: textbook / E.K. Baranova, A.V. Babash. – 4th ed., revis. and add. – Moscow: RIOR: INFRA-M, 2022. – 336 p.

2. Grishina, N.V. Fundamentals of enterprise information security: textbook / N.V. Grishina. – Moscow: INFRA-M, 2021. – 216 p.

3. Ovchinnikov, A. I. Fundamentals of national security: textbook. allowance / A.I. Ovchinnikov, A.Yu. Mamychev, P.P. Baranov. – 2nd ed. – Moscow : RIOR : INFRA-M, 2019. — 224 p.

4. Information protection: textbook / A.P. Zhuk, E.P. Zhuk, O.M. Lepeshkin, A.I. Timoshkin. — 3rd ed. — Moscow: RIOR: INFRA-M, 2023. — 400 p.

5. Sukhanov, V.V. Methodology for logical design of information support for distributed information systems of critical application / V.V. Sukhanov, O.V. Lankin // Modeling of systems and processes. – 2021. – T. 14, No. 3. – P. 67-73. – DOI: 10.12737/2219-0767-2021-14-3-67-73.

6. Sukhanov, V.V. Analytical support for data organization in distributed information systems of critical application / V.V. Sukhanov // Modeling of systems and processes. – 2021. – T. 14, No. 3. – P. 60-67. – DOI: 10.12737/2219-0767-2021-14-3-60-67.

7. Model of individual group assignment of access to hierarchically organized objects of critical information systems using mobile technologies / E.A. Rogozin, V.A. Khvostov, V.V. Sukhanov [et al.]// Modeling of systems and processes. – 2021. – T. 14, No. 1. – P. 73-79. – DOI: 10.12737/2219-0767-2021-14-1-73-79.

8. Poluektov A.V., Makarenko F.V., Yagodkin A.S. The use of third-party libraries when writing programs for processing statistical data // Modeling of systems and processes. - 2022. – Vol. 15, No. 2. – pp. 33-41.