практической конференции, Москва, 30 мая 2024 года. – Москва: Российский университет транспорта (МИИТ), 2024. – С. 631-636. – DOI: 10.30932/9785002446094-2024-631-636.

2. *Schneier B., Ferguson N.* Fortuna. A secure pseudorandom number generator. – URL: https://www.schneier.com/academic/fortuna/ (дата обращения 25.09.2024).

3. *Романков С.В.* Методы генерации псевдослучайных чисел // Молодой ученый. – 2022. – № 33 (428). – С. 4-10. – URL: https://moluch.ru/archive/428/94534/ (дата обращения 25.09.2024).

4. *Schneier B., Ferguson N., Kohno T.* Cryptography Engineering: Design Principles and Practical Applications. – Indianapolis: Wiley Publishing, 2010. – 384 p.

5. *Netdata Cloud.* Understanding entropy: the key to secure cryptography and randomness. – URL: https://www.netdata.cloud/blog/understanding-entropy-the-key-to-secure-cryptography-and-randomness/ (дата обращения 25.09.2024).

Ведмедева М.В., Миронова В.Г.

Эволюция информационных систем: от простых решений к комплексным инфраструктурам

Аннотация: В работе рассматриваются особенности отказоустойчивости и безопасности информационных систем в условиях увеличения числа кибератак и расширения поверхности атак. Особое внимание уделено сравнению простых и сложных ИС, их функциональным возможностям, масштабируемости и уровням безопасности. Выявлены основные проблемы, связанные с использованием устаревших методов защиты, и предложены подходы для повышения устойчивости современных ИС.

Ключевые слова: информационные системы, киберугрозы, поверхность атаки, отказоустойчивость, безопасность данных, модели угроз, масштабируемость, безопасность

Информационные системы встречаются практически во всех сферах жизнедеятельности: от финансов и здравоохранения до промышленности и государственного управления. С увеличением их ресурсов и компонентов для функционирования, возрастает и число уязвимостей. Даже если использовать сверхсовременные средства защиты информации, нельзя дать гарантии, что данные не подвержены риску. Только за первую половину 2024 года в сеть утекло в разы больше данных, чем за аналогичный период прошлого года [1], а в общем и целом, доля заказных кибератак увеличилась за год с 10% до 44% [2]. Злоумышленники продолжают совершать различные разного рода атаки на компании, принося не только финансовый, но и репутационный вред. Во избежание значительного ущерба от реализации рисков, связанных с информационной безопасностью, следует анализировать модели поверхности атаки – совокупность всех точек во взаимодействии системы, через которые злоумышленник может попытаться получить несанкционированный доступ.

С увеличением числа взаимосвязанных компонентов и сервисов, а также развитием таких технологий, как облачные вычисления, Интернет вещей и анализ больших данных, современная поверхность для реализации атак значительно расширяется. Традиционные методы защиты, такие как межсетевые экраны и антивирусные программы, зачастую недостаточны для обеспечения безопасности сложных инфраструктур перед лицом новых и более сложных угроз. Например, многие современные кибератаки эксплуатируют уязвимости в программном обеспечении, сетевых протоколах или настройках систем, которые трудно обнаружить с помощью стандартных подходов [3]. Кроме того, большое количество отраслей требует соблюдения требований стандартов информационной безопасности, в частности, ISO/IES 27001, NIST, GDPR и др. Они включают требования по управлению рисками. Для создания надежной системы защиты информации, способной отражать атаки нарушителя необходимо разработать адекватную модель угроз и нарушителя безопасности информации. Модели угроз безопасности информации позволяют разработать надёжную систему защиты и реализовать требования стандартов и нормативных документов в области информационной безопасности. Не менее важным фактором для крупных компаний является

грамотное распределение ресурсов на наиболее критичные области защиты для минимизации потенциальных убытков, поскольку стоимость полной защиты аспектов информационной системы может быть крайне высока.

«Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств» [4]. Однако это определение из Федерального закона дает не совсем полное представление о функционировании и составе информационной системы. Опираясь на изученные учебные материалы [5-9] и полученные знания, было дано следующее определение: «Информационная система представляет собой организационную совокупность взаимосвязанных компонентов, таких как программное и техническое обеспечение, оборудование, базы данных и люди, которая предназначена для сбора, хранения, обработки, управления и распространения информации. Она поддерживает выполнение различных задач, принятие решений и управление деятельностью в рамках организации или других социальных структур».

Информационные системы по уровню структуры, взаимосвязи компонентов и функциональности можно разделить на две категории: простые и сложные.

Использование простых ИС бывает не всегда практично [10]. Например, они не могут обеспечивать достаточный уровень поддержки бизнес-процессов крупных и быстрорастущих компаний. Такие информационные системы плохо адаптируются к изменяющимся условиям и не очень хорошо интегрируются с другими бизнес-системами. Например, организации, использующие простые системы, сталкиваются с трудностями при попытке интегрировать новые функции или расширить систему для поддержки большего числа пользователей [11]. Также, когда мы говорим о крупных компаниях, следует учитывать, что они работают с большим объемом данных, соответственно, им важен высокий уровень автоматизации и аналитических возможностей, что, к сожалению, простая ИС не в силах обеспечить. С функциональными возможностями разобрались, но что насчет безопасности? Приводится пример использования электронных таблиц для клиентской базы и финансовой деятельности [12].

Данные хранились без шифрования и контроля доступа, следовательно, оказались уязвимыми для намеренного изменения. В данном случае, простая ИС не обеспечила базовые механизмы безопасности.

Соответственно, говоря о недостатках простых информационных систем, можно выделить следующие пункты:

Ограниченная функциональность. Простые ИС обычно разрабатываются для решения конкретных задач и не могут справляться со сложными бизнес-процессами, требующими разнообразных функций.

Отсутствие гибкости и интеграции. В современных условиях организации используют множество различных решений, таких как системы управления взаимоотношениями с клиентами – Customer Relationship Management (CRM), системы управления ресурсами предприятия – Enterprise Resource Planning (ERP), решения для бухгалтерского учета, логистики. Если ИС не может интегрироваться с этими решениями, это может привести к разрозненности данных, необходимости дублирования информации и значительным временным затратам на ручную обработку данных.

Проблемы масштабируемости. В крупных организациях с множеством отделов и сотрудников простая ИС может не выдерживать нагрузку, что приведет к снижению производительности и даже сбоям в работе системы.

Недостаточный уровень безопасности. Простая система может не поддерживать современные методы шифрования данных, многофакторную аутентификацию, мониторинг активности пользователей и другие механизмы защиты.

Таким образом, простые ИС могут быть полезны для малого бизнеса или же ранних этапах развития организации. Если же предприятие стремиться к быстрому развитию, увеличению мощностей, расширению клиентской базы, то необходимо пользоваться более усовершенствованными решениями.

Сложные информационные системы, в отличие от простых, обладают широким спектром функций, включая автоматизацию операций, анализ данных и поддержку принятия решений. Такие системы обычно включают в себя множество компонентов, таких как базы данных, сети, пользовательские интерфейсы и бизнес-приложения.

Рассмотрим применение и функционирование сложных ИС, например, использования сложной ИС в здравоохранении [13]. Рассматривается система управления больницей, которая включает модули для учета пациентов, назначения лекарств, хранения медицинских записей и финансового учета. В такой системе каждая функциональная область интегрирована, что позволяет врачам и административному персоналу получать доступ к необходимой информации в реальном времени, что повышает качество обслуживания и уменьшает число ошибок, связанных с человеческим фактором.

В другом примере, из банковского сектора [14], описывается, как банки применяют интегрированные системы управления рисками, которые объединяют информацию из различных источников, таких как финансовая отчетность, рыночные данные и внутренние операционные показатели. Это значительно облегчает работу аналитикам и руководителям и помогает им оперативно реагировать на изменения в финансовом окружении и предотвращать потенциальные угрозы, например, связанные с мошенничеством или колебаниями валютных.

Говоря о безопасности, можно рассмотреть пример использования системы управления информационной безопасностью (Security Information and Event Management, SIEM) в финансовом учреждении для предотвращения кибератак [15]. Система позволяет собирать и анализировать логи из разных источников, таких как сетевые устройства, серверы, приложения и базы данных. Она выявляет аномальные действия и подозрительные активности, что помогает специалистам по безопасности оперативно реагировать на потенциальные угрозы. Благодаря автоматизации анализа и функции корреляции данных SIEM позволила снизить количество ложных срабатываний и ускорить обнаружение инцидентов. В книге также приводится пример, когда SIEM-система выявила необычную активность, связанную с попыткой несанкционированного доступа к финансовым данным, что помогло предотвратить утечку информации.

Подведем итог по четырем основным параметрам системы:

Функциональность. Выполнение широкого спектра функций, например, автоматизация простых или повторяющихся задач.

Также можно говорить про возможность обработки большого объема данных, а также соответствующих инструментов для этого.

Гибкость и интеграция. Сложные ИС могут быть интегрированы с внешними системами, такими как облачные сервисы, другие корпоративные системы или даже системы партнеров. Кроме того, они отличаются модульностью: состоят из нескольких элементов, которые легко заменяются и добавляются без необходимости полной модернизации системы.

Масштабируемость. Предполагает добавление новых серверов для распределения нагрузки или же увеличение мощности существующих серверов. Поддерживает облачную инфраструктуру: позволяет динамически увеличивать или уменьшать вычислительные ресурсы.

Безопасность. Использование многоуровневой защиты, аудита, управления доступом и соответствий стандартов безопасности.

Эти четыре аспекта делают сложные информационные системы мощными инструментами, обеспечивающими комплексное управление данными и безопасностью, а также поддерживающими гибкость и масштабируемость в меняющемся бизнес-ландшафте.

Литература:

1. Число кибератак в России и в мире. – URL: https://www.tadviser.ru/index.php/Статья:Число_кибератак_в_России_и_в_мире (дата обращения 10.10.2024).

2. Крупные кибератаки и утечки первой половины 2024 года в России. – URL: https://blog.cortel.cloud/2024/05/23/krupnye-kiberataki-i-utechki-pervoj-poloviny-2024-goda-v-rossii/ (дата обращения 10.10.2024).

3. *Остапенко Г.А., Куликов С.С., Коноплин А.В., Остапенко А.А.* Разработка архитектуры киберполигона для повышения качества и результативности учебного процесса в исследовании атак на информационные системы и сети // Информация и безопасность. – 2023. – Т. 26. Вып. 1. – С. 101-108.

4. Федеральный закон РФ от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».

5. *Жданов С.А., Соболева М.Л., Алфимова А.С.* Информационные системы: учебник для студентов учреждений

высшего образования / под ред. В.Л. Матросова. – Москва: Прометей, 2015. – 302 с.

6. *О'Брайен Дж. А.* Введение в информационные системы. – Москва: Вильямс, 2007. – 432 с.

7. *Лаудон К., Лаудон Д.* Информационные системы в управлении. – Санкт-Петербург: Питер, 2014. – 688 с.

8. *Баженов Ю.В.* Информационные системы: теоретические и прикладные аспекты. – Москва: Академический проект, 2003. – 352 с.

9. *Shelly G.B., Cashman T.J., Vermaat M.* Discovering Computers: Fundamentals. – Boston: Cengage Learning, 2011. – 700 p.

10. *Laudon K.C., Laudon J.P.* Management Information Systems: Managing the Digital Firm. 16th ed. – Boston: Pearson Education, 2020. – 720 p.

11. *О'Брайен Дж. А.* Введение в информационные системы. – Москва: Вильямс, 2007. – 432 с.

12. *Stair R., Reynolds G.* Principles of Information Systems. 13th ed. – Boston: Cengage Learning, 2020. – 672 p.

13. *Rainer R.K., Turban E.* Information Systems for Managers. 4th ed. – Hoboken: Wiley, 2020. – 496 p.

14. *Davis G.B., Olson M.H.* Modern Information Systems. 2nd ed. – Boston: McGraw-Hill Education, 2021. – 540 p.

15. *Whitman M.E., Mattord H.J.* Principles of Information Security. 6th ed. – Boston: Cengage Learning, 2019. – 704 p.