УДК 33

Экономико-технологические детерминанты информационной безопасности в современных вычислительных системах

Грушицын Александр Степанович

Старший преподаватель,
Московский финансово-промышленный университет «Синергия»,
125190, Российская Федерация, Москва, просп. Ленинградский, 80;
e-mail: nicifor@bk.ru

Аннотация

В статье рассматривается взаимосвязь между развитием компьютерных архитектур, механизмами защиты информации и экономическими факторами. Анализируется влияние технологических решений на стоимость производства, производительность и безопасность вычислительных систем. Рассмотрены ключевые аспекты, включая эволюцию процессорных архитектур, использование резидентных программ, методы блокировки доступа к вводу-выводу, а также экономические последствия уязвимостей, таких как Spectre и Meltdown. Особое внимание уделено компромиссам между производительностью, безопасностью и затратами на разработку, а также долгосрочной экономической эффективности различных подходов к защите данных.

Для цитирования в научных исследованиях

Грушицын А.С. Экономико-технологические детерминанты информационной безопасности в современных вычислительных системах // Экономика: вчера, сегодня, завтра. 2025. Том 15. № 3А. С. 568-575.

Ключевые слова

Компьютерные архитектуры, информационная безопасность, экономика ИТ, резидентные программы, аппаратная защита, уязвимости процессоров, Spectre, Meltdown, RISC, CISC, шифрование данных, ассемблер, оптимизация затрат.

Введение

Развитие архитектуры компьютеров изначально было тесно связано с экономическими факторами, поскольку каждое технологическое решение влияло как на стоимость производства, так и на потенциальные риски, связанные с безопасностью данных. Первые вычислительные устройства, основанные на лампах и транзисторах, требовали физического изменения схем для модификации их функций, что делало процесс дорогим и негибким. С появлением программируемых транзисторов и микросхем затраты на обновление логики работы снизились, но одновременно возросла уязвимость систем к несанкционированному вмешательству. Это привело к необходимости внедрения механизмов защиты, таких как пароли и шифрование, которые, хотя и увеличивали стоимость разработки, позволяли предотвращать более значительные финансовые потери из-за утечек или повреждения данных.

Основное содержание

Одним из ключевых аспектов экономии в проектировании компьютеров стало использование шинной архитектуры, которая заменила прямое соединение каждого элемента процессора с памятью. Это сократило количество проводников и упростило производство, однако одновременно создало новые уязвимости, поскольку шины могли стать каналом для перехвата информации. Для минимизации этих рисков потребовались дополнительные аппаратные решения, такие как контроллеры шин и разделение на быстрые и медленные каналы передачи данных. Эти меры повысили безопасность, но также увеличили себестоимость устройств, что особенно заметно в высокопроизводительных системах, где защита данных критически важна.

Процессоры, в свою очередь, эволюционировали в сторону оптимизации доступа к памяти за счёт регистров и кэширования, что позволило сократить время обработки команд и снизить энергопотребление. Однако обнаруженные впоследствии уязвимости, такие как Spectre и Meltdown, показали, что повышение производительности иногда достигается за счёт ослабления защиты. Устранение этих недостатков потребовало выпуска программных патчей, которые замедлили работу процессоров, что, в свою очередь, повлияло на их рыночную конкурентоспособность. Производителям пришлось искать баланс между скоростью вычислений и безопасностью, поскольку пользователи и корпоративные клиенты готовы платить больше за надёжные решения, но не за счёт значительного падения производительности.

Механизм прерываний, позволяющий эффективно распределять вычислительные ресурсы между задачами, также имеет экономические последствия. Неправильная настройка обработки прерываний может привести к задержкам или даже отказам системы, что особенно критично в серверных и промышленных решениях, где простои означают прямые финансовые потери. Защищённый режим работы процессора и таблицы векторов прерываний добавляют уровень безопасности, но требуют дополнительных аппаратных ресурсов и усложняют проектирование, что отражается на конечной стоимости устройств.

Сравнение архитектур RISC и CISC также демонстрирует экономический компромисс между сложностью, безопасностью и производительностью. RISC-процессоры, благодаря упрощённому набору команд, дешевле в разработке и менее подвержены уязвимостям, что делает их привлекательными для встраиваемых систем и устройств, где важна надёжность.

CISC-процессоры, напротив, обеспечивают обратную совместимость и высокую производительность в сложных задачах, но их защита требует больше ресурсов, что увеличивает стоимость как самих чипов, так и систем на их основе.

В конечном итоге любая уязвимость в архитектуре компьютера может привести к значительным финансовым потерям — от прямых убытков из-за краж данных до затрат на восстановление работоспособности систем и репутационного ущерба. Поэтому современные разработчики вынуждены учитывать не только технические, но и экономические аспекты защиты информации, инвестируя в безопасные технологии, которые хоть и повышают первоначальную стоимость устройств, но в долгосрочной перспективе снижают риски и обеспечивают устойчивость бизнеса.

Резидентные программы, включая драйверы, системы шифрования и защиты данных, представляют собой важный класс программного обеспечения, требующий постоянного присутствия в оперативной памяти для обеспечения оперативного реагирования на события в вычислительной системе. С экономической точки зрения, их использование сопряжено с рядом затрат и выгод. С одной стороны, резидентные программы повышают эффективность работы системы за счёт мгновенного выполнения критически важных операций, таких как обработка прерываний или защита данных, что снижает потенциальные убытки от задержек или кибератак. С другой стороны, их функционирование требует выделения части оперативной памяти, что создаёт дополнительные расходы на аппаратные ресурсы, особенно в системах с ограниченной памятью.

Процесс загрузки резидентной программы включает её установку в память, настройку таблицы векторов прерываний и адаптацию к параметрам системы, что требует вычислительных мощностей и временных затрат. После завершения установки управление возвращается системе, а резидентная часть программы остаётся активной, продолжая потреблять ресурсы. Для взаимодействия с такими программами используется прерывание int 2fh, которое предотвращает их повторную загрузку и позволяет корректно выгружать их из памяти. Однако процедура выгрузки сопряжена с техническими сложностями, поскольку требует восстановления исходных векторов прерываний, которые могли быть перехвачены другими резидентными программами. Если этот процесс выполнен некорректно, система может столкнуться с ошибками, приводящими к её нестабильности или зависанию, что влечёт за собой дополнительные затраты на восстановление работоспособности.

Экономические последствия некорректной работы резидентных программ могут быть значительными. Например, если резидентная программа, отвечающая за защиту данных, выгружается с ошибками, это создаёт уязвимости, которые могут быть использованы злоумышленниками, приводя к утечкам информации и финансовым потерям. Кроме того, конфликты между резидентными программами увеличивают нагрузку на систему, снижая её общую производительность и повышая эксплуатационные расходы.

Ещё одним аспектом, требующим экономической оценки, является использование программного прерывания от системного таймера (1Ch) для активации резидентных программ в реальном времени. Хотя этот механизм позволяет эффективно управлять отложенными задачами, такими как периодическая проверка безопасности или выполнение фоновых процессов, его некорректная реализация может привести к избыточному потреблению ресурсов и снижению быстродействия системы. В долгосрочной перспективе это увеличивает затраты на обслуживание и модернизацию оборудования.

Таким образом, резидентные программы, несмотря на их очевидные преимущества в обеспечении безопасности и оперативности обработки данных, требуют тщательного

управления ресурсами и корректной реализации механизмов загрузки и выгрузки. Оптимизация их работы позволяет минимизировать экономические издержки, связанные с потреблением памяти и потенциальными сбоями, что в конечном итоге способствует повышению надёжности и экономической эффективности вычислительных систем.

кономические последствия реализации механизмов блокировки доступа к интерфейсам ввода-вывода требуют комплексного анализа, учитывающего как прямые затраты на внедрение защитных мер, так и потенциальные убытки от возможных нарушений информационной безопасности. Программные методы защиты, основанные на парольной аутентификации и фиксации адресов памяти, представляют собой относительно экономичное решение, однако их эффективность существенно снижается при наличии программных интерфейсов доступа. Полный отказ от поддержки функций чтения данных в микроконтроллерах, хотя и повышает уровень безопасности, одновременно приводит к увеличению эксплуатационных расходов, поскольку требует разработки специализированных аппаратных решений и усложняет процессы отладки и обслуживания системы.

Аппаратные методы блокировки, такие как подача сверхпредельного напряжения для физического повреждения интерфейсных выводов, обеспечивают более высокий уровень защиты, но сопряжены со значительными экономическими издержками. Процедура восстановления поврежденных портов ввода-вывода требует специального оборудования и квалифицированного персонала, что увеличивает стоимость жизненного цикла устройства. Интеграция аппаратных криптографических модулей непосредственно в кристалл микроконтроллера, несмотря на первоначальное удорожание производства, в долгосрочной перспективе оказывается экономически оправданной, так как позволяет избежать затрат, связанных с разработкой и поддержкой внешних систем шифрования.

Пассивные методы защиты микросхем, включающие внедрение избыточных нефункциональных элементов и усложнение топологии кристалла, увеличивают стоимость проектирования и производства, но обеспечивают экономию за счет снижения вероятности успешного копирования и реверс-инжиниринга защищенных устройств. Однако следует учитывать, что такие решения могут усложнить процесс тестирования и повысить процент бракованных изделий, что негативно скажется на себестоимости продукции. Активные методы защиты, основанные на механизмах самоуничтожения данных при обнаружении несанкционированного доступа, хотя и являются эффективным средством противодействия промышленному шпионажу, требуют тщательного расчета экономических последствий их применения, поскольку выход из строя даже одного элемента системы может привести к значительным убыткам, особенно в критически важных инфраструктурах.

Экономическая целесообразность выбора конкретного метода защиты должна определяться на основе анализа соотношения между стоимостью его реализации и потенциальным ущербом от возможных нарушений информационной безопасности. При этом необходимо учитывать не только прямые затраты на внедрение защитных механизмов, но и косвенные издержки, связанные с возможным снижением производительности, увеличением времени вывода продукта на рынок и необходимостью дополнительного обучения персонала. Оптимальное решение должно обеспечивать баланс между уровнем безопасности, стоимостью реализации и эксплуатационными характеристиками защищаемой системы.

Обеспечение безопасности компьютерных систем представляет собой сложный процесс, требующий взвешенного подхода с точки зрения экономической целесообразности. Современные угрозы информационной безопасности создают серьезные риски для организаций, потенциально приводя к значительным финансовым потерям. Эти потери могут

быть связаны не только с непосредственным ущербом от атак, но и с затратами на восстановление систем, расследование инцидентов, а также с репутационными издержками.

Разработка и внедрение защитных механизмов неизбежно влечет за собой дополнительные расходы. Эти затраты включают в себя как прямые инвестиции в аппаратные и программные решения безопасности, так и косвенные издержки, связанные с возможным снижением производительности систем или усложнением их обслуживания. Однако отказ от соответствующих мер защиты может привести к еще более существенным финансовым последствиям в случае успешной кибератаки.

Особую сложность представляет поиск оптимального баланса между уровнем безопасности и экономической эффективностью. С одной стороны, чрезмерные затраты на защиту могут сделать продукт или систему неконкурентоспособными. С другой стороны, недостаточный уровень безопасности создает существенные риски для бизнеса. Поэтому при разработке стратегии защиты необходимо тщательно анализировать потенциальные угрозы, оценивать стоимость возможного ущерба и сопоставлять эти данные с затратами на реализацию различных защитных механизмов.

Эффективная система безопасности должна учитывать не только технические аспекты защиты, но и экономические факторы. Важно найти разумный компромисс между стоимостью внедрения защитных мер, удобством использования системы и достигаемым уровнем безопасности. Такой подход позволяет создать устойчивую и экономически обоснованную систему защиты, способную противостоять современным угрозам без неоправданного увеличения затрат.

Экономические аспекты использования языка ассемблера в системах защиты информации требуют тщательного анализа соотношения между затратами на разработку и достигаемым уровнем безопасности. Применение низкоуровневого программирования, хотя и сопряжено с повышенными трудозатратами и необходимостью привлечения высококвалифицированных специалистов, во многих случаях оказывается экономически оправданным благодаря существенному повышению эффективности защитных механизмов. Компактный размер ассемблерного кода, превосходящий по этому показателю языки высокого уровня в 4-10 раз, позволяет минимизировать занимаемое пространство в памяти и сократить время выполнения критически важных операций, что особенно значимо для систем реального времени и аппаратно-зависимых компонентов, таких как драйверы устройств.

С экономической точки зрения, реализация на ассемблере таких защитных механизмов, как предотвращение переполнения буфера, технология DEP и ASLR, обеспечивает значительное снижение рисков успешных кибератак, что в долгосрочной перспективе компенсирует повышенные затраты на разработку. Особенно это актуально для систем, обрабатывающих конфиденциальные данные или выполняющих критически важные функции, где потенциальный ущерб от нарушения безопасности может многократно превышать стоимость внедрения защитных мер.

Вопросы шифрования данных также требуют экономического обоснования выбора между статическими и динамическими методами. Хотя статическое шифрование всего диска проще в реализации и требует меньших вычислительных ресурсов, оно оставляет уязвимым содержимое оперативной памяти. Динамическое шифрование отдельных блоков данных, особенно с использованием различных ключей и цепочек CBC, обеспечивает более высокий уровень защиты, но требует дополнительных затрат на разработку и может снижать производительность системы. Однако для организаций, работающих с особо важной информацией, эти дополнительные расходы часто оказываются оправданными, так как позволяют избежать

значительно больших потерь в случае утечки данных.

Использование структурированных обработчиков исключений (SEH) для защиты критически важных функций от перехвата аргументов представляет собой пример экономически эффективного решения, позволяющего повысить безопасность без существенного увеличения сложности системы. Такой подход минимизирует потенциальные убытки от атак, направленных на перехват управления, сохраняя при этом приемлемый уровень производительности и не требуя значительных дополнительных ресурсов. В целом, выбор конкретных методов защиты должен основываться на тщательной оценке соотношения между стоимостью их реализации, потенциальным ущербом от возможных атак и требованиями к производительности системы.

Заключение

Развитие компьютерных архитектур и систем защиты информации неразрывно связано с экономическими факторами, поскольку каждое технологическое решение требует баланса между стоимостью, производительностью и безопасностью. Исторически переход от ламповых и транзисторных систем к программируемым микросхемам снизил затраты на модификацию логики работы, но одновременно повысил уязвимость к кибератакам, что привело к необходимости внедрения дополнительных защитных механизмов.

Шинная архитектура, кэширование памяти и оптимизация процессорных команд позволили сократить производственные издержки и повысить эффективность вычислений, однако параллельно возникли новые риски, такие как уязвимости Spectre и Meltdown. Устранение этих недостатков потребовало компромиссов между скоростью работы и безопасностью, что напрямую влияет на рыночную конкурентоспособность продуктов.

Резидентные программы, аппаратные методы блокировки ввода-вывода и низкоуровневая разработка на ассемблере демонстрируют, что повышение безопасности часто сопряжено с увеличением затрат на аппаратные ресурсы, квалифицированных специалистов и обслуживание систем. Однако в долгосрочной перспективе инвестиции в защиту данных оказываются экономически оправданными, поскольку предотвращают значительные финансовые потери от утечек информации, простоев оборудования и репутационного ущерба.

Таким образом, современные разработчики вынуждены постоянно искать оптимальное соотношение между стоимостью, производительностью и безопасностью. Эффективная стратегия защиты должна основываться на тщательном анализе потенциальных угроз, оценке возможного ущерба и выборе решений, которые минимизируют риски без чрезмерного увеличения затрат. Только такой сбалансированный подход позволяет создавать надежные, экономически устойчивые системы, способные противостоять вызовам цифровой эпохи.

Библиография

1. Мамаева Л. Н. Характерные проблемы информационной безопасности в современной экономике //Информационная безопасность регионов. – 2016. – №. 1 (22). – С. 21-24.
2. Графов А. А., Мордовец В. А. Информационная безопасность в системе экономической безопасности. – 2018.
3. Иванченко П. Ю. и др. Математическое моделирование информационной и экономической безопасности на предприятиях малого и среднего бизнеса //Фундаментальные исследования. – 2013. – №. 10-13. – С. 2860-2863.
4. Балдин К., Уткин В. Информационные системы в экономике. – Litres, 2022.
5. Горбачев Д. В., Кононова М. В. Комплексный подход к организации деятельности службы экономической безопасности предприятия //Интеллект. Инновации. Инвестиции. – 2013. – №. S. – С. 165-170.
6. Советов Б. Я., Колбанёв М. О., Татарникова Т. М. Технологии инфокоммуникации и их роль в обеспечении

информационной безопасности //Геополитика и безопасность. – 2014. – №. 1. – С. 69-77.
7. Богачев В. Я., Редин В. В. Информационная безопасность как составная часть национальной безопасности Российской Федерации //Стратегия гражданской защиты: проблемы и исследования. – 2012. – Т. 2. – №. 2. – С. 785-797.
8. Мирошниченко М. А., Бондаренко А. А., Пиналова Е. В. Актуальные проблемы обеспечения информационной безопасности систем электрон-ного документооборота в рамках цифровой трансформации //Вестник академии знаний. – 2020. – №. 1 (36). – С. 137-142.
9. Аносов В. Д., Стрельцов А. А. О доктрине информационной безопасности Российской Федерации //Информационное общество. – 1997. – №. 2-3. – С. 3-9.
10. Казьмина И. В., Маслов В. И. Обеспечение безопасности информации в экономической информационной системе управления высокотехнологичных предприятий //Организатор производства. – 2016. – №. 2 (69). – С. 33-40.

Economic and Technological Determinants of Information Security in Modern Computing Systems

Aleksandr S. Grushitsyn

Senior Lecturer,
Moscow University of Industry and Finance "Synergy",
125190, 80, Leningradsky ave., Moscow, Russian Federation;
e-mail: nicifor@bk.ru

Abstract

This article examines the interdependence between computer architecture development, information security mechanisms, and economic factors. The study analyzes how technological solutions impact production costs, performance, and security of computing systems. Key aspects include the evolution of processor architectures, use of resident programs, input/output access blocking methods, and economic consequences of vulnerabilities like Spectre and Meltdown. Particular attention is given to trade-offs between performance, security, and development costs, as well as long-term cost-effectiveness of different data protection approaches.

For citation

Grushitsyn A.S. (2025) Ekonimiko-tekhnologicheskie determinanty informatsionnoy bezopasnosti v sovremennykh vychislitelnykh sistemakh [Economic and Technological Determinants of Information Security in Modern Computing Systems]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 15 (3A), pp. 568-575.

Keywords

Computer architectures, information security, IT economics, resident programs, hardware protection, processor vulnerabilities, Spectre, Meltdown, RISC, CISC, data encryption, assembler, cost optimization

References

1. Mamaeva L. N. Characteristic problems of information security in the modern economy //Information security of the regions. – 2016. – №. 1 (22). – Pp. 21-24.
2. Grafov A. A., Mordovets V. A. Information security in the economic security system. – 2018.

3. Ivanchenko P. Yu. and others. Mathematical modeling of information and economic security in small and medium-sized businesses //Fundamental Research. - 2013. – No. 10-13. – pp. 2860-2863.
4. Baldin K., Utkin V. Information systems in economics. – Litres, 2022.
5. Gorbachev D. V., Kononova M. V. An integrated approach to the organization of the company's economic security service //Intelligence. Innovation. Investment. – 2013. no. S. – pp. 165-170.
6. Sovetov B. Ya., Kolbanev M. O., Tatarnikova T. M. Infocommunication technologies and their role in ensuring information security //Geopolitics and security. - 2014. – No. 1. – pp. 69-77.
7. Bogachev V. Ya., Redin V. V. Information security as an integral part of the national security of the Russian Federation //Civil protection strategy: problems and research. 2012. Vol. 2. no. 2. pp. 785-797.
8. Miroshnichenko M. A., Bondarenko A. A., Pinalova E. V. Actual problems of ensuring information security of electronic document management systems in the framework of digital transformation //Bulletin of the Academy of Knowledge. – 2020. – №. 1 (36). – Pp. 137-142.
9. Anosov V. D., Streltsov A. A. On the information security doctrine of the Russian Federation //The Information Society. 1997. – 2-3. pp. 3-9.
10. Kazmina I. V., Maslov V. I. Information security in the economic information management system of high–tech enterprises //Production organizer. – 2016. – №. 2 (69). – Pp. 33-40.