УДК 0.004 **Информационные технологии**

Цыбенко Олег Сергеевич, *магистрант,*
Донской государственный технический университет, г. Ростов-на-Дону

АЛГОРИТМИЧЕСКОЕ И АППАРАТНОЕ УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ РЕСУРСОВ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Аннотация: В современную цифровую эпоху информационные системы играют ключевую роль как в деятельности организаций, правительств, так и отдельных лиц. Эти системы хранят и обрабатывают огромные объемы конфиденциальных данных, что делает их выгодными мишенями для злоумышленников, стремящихся использовать уязвимости для получения финансовой выгоды или поставить под угрозу национальную безопасность. Поэтому обеспечение безопасности ресурсов информационной системы имеет первостепенное значение. В статье исследуется важнейшая роль алгоритмического и аппаратного управления в обеспечении информационной безопасности этих ресурсов.

Ключевые слова: информационная безопасность, аппаратное управление, алгоритмическое управление, информационные системы.

Abstract: In the modern digital era, information systems play a key role both in the activities of organizations, governments, and individuals. These systems store and process huge amounts of sensitive data, which makes them profitable targets for attackers seeking to exploit vulnerabilities for financial gain or jeopardize national security. Therefore, ensuring the security of information system resources is of paramount importance. The article examines the most important role of algorithmic and hardware management in ensuring the information security of these resources.

Keywords: information security, hardware management, algorithmic

management, information systems.

Алгоритмическое управление информационной безопасностью

1. Методы шифрования: Шифрование является фундаментальным компонентом информационной безопасности. Продвинутые алгоритмы шифрования, такие как AES и RSA, используют сложные математические процессы для преобразования данных в нечитаемый формат. Выбор алгоритма шифрования и методов управления ключами имеют решающее значение. Кроме того, продолжающаяся разработка квантово-устойчивых алгоритмов становится все более важной, поскольку квантовые вычисления угрожают существующим стандартам шифрования [1].

2. Протоколы аутентификации: Аутентификация - это процесс проверки личности пользователей или устройств, пытающихся получить доступ к системе. Многофакторная аутентификация (MFA) стала стандартной практикой, объединяющей то, что пользователь знает (например, пароль), то, что у пользователя есть (например, смартфон), и то, кем пользователь является (например, биометрические данные). Биометрическая аутентификация, включая сканирование отпечатков пальцев и распознавание лиц, повышает безопасность, гарантируя, что только авторизованные лица могут получить доступ к системе.

3. Модели управления доступом: Алгоритмы управления доступом, такие как управление доступом на основе ролей (RBAC) и управление доступом на основе атрибутов (ABAC), позволяют организациям точно настраивать разрешения для пользователей и устройств. RBAC, например, назначает роли пользователям и предоставляет привилегии доступа на основе этих ролей. ABAC, с другой стороны, рассматривает различные атрибуты пользователей и объектов для принятия решений о доступе. Эти модели обеспечивают детальный контроль над тем, кто и к чему может получить доступ в информационной системе.

4. Обнаружение и предотвращение вторжений: Системы обнаружения и предотвращения вторжений (IDS/IPS) используют алгоритмы для мониторинга

сетевых и системных действий на предмет необычных закономерностей. Аномалии могут указывать на потенциальные нарушения безопасности или кибератаки. Алгоритмы машинного обучения стали неотъемлемой частью этих систем, поскольку они могут адаптироваться и извлекать уроки из возникающих угроз, повышая способность системы эффективно обнаруживать атаки и реагировать на них.

Аппаратное обеспечение управления информационной безопасностью

1. Брандмауэры: Брандмауэры, доступные как в аппаратной, так и в программной формах, действуют как привратники, фильтруя входящий и исходящий сетевой трафик. Аппаратные брандмауэры, часто развертываемые в точках входа в сеть, особенно эффективны для блокирования вредоносного трафика до того, как он достигнет внутренней сети. Брандмауэры нового поколения (NGFWs) сочетают аппаратное обеспечение и сложное программное обеспечение для обеспечения расширенных функций безопасности, таких как глубокая проверка пакетов и фильтрация на уровне приложений [2].

2. Защищенные процессоры и сопроцессоры: Защищенные процессоры и сопроцессоры — это специализированные аппаратные компоненты, предназначенные для безопасной обработки криптографических операций. Эти специализированные чипы гарантируют, что процессы шифрования и дешифрования происходят в среде, защищенной от несанкционированного доступа. Например, расширения Intel Software Guard Extensions (SGX) — это технология, которая обеспечивает безопасные анклавы для запуска конфиденциального кода в защищенной аппаратной среде.

3. Аппаратные модули безопасности (HSM): HSM — это специализированные аппаратные устройства, используемые для безопасного хранения криптографических ключей и выполнения криптографических операций. Они широко используются в приложениях, требующих высокого уровня защиты ключей, таких как обработка платежей и выдача цифровых сертификатов. Системы HSM обеспечивают физическую и логическую защиту от кражи ключей и неправильного использования.

4. Доверенные платформенные модули (TPMS): TPMS интегрируются в компьютеры и устройства для обеспечения целостности процесса загрузки системы и безопасного хранения ключей. TPMS обеспечивают уровень доверия к системе, помогая защитить от атак встроенного ПО и гарантируя, что ключи шифрования остаются в безопасности, даже если устройство скомпрометировано.

Преимущества и проблемы

Комбинированное использование алгоритмических и аппаратных мер безопасности обеспечивает надежную защиту от широкого спектра угроз. Однако важно признать проблемы, которые возникают при таком подходе:

1. Сложность: Управление как алгоритмами, так и аппаратными компонентами может быть сложным и требует квалифицированного персонала. Реализация и поддержание всеобъемлющей стратегии безопасности может привести к нехватке ресурсов и бюджетов.

2. Интеграция: Решающее значение имеет обеспечение того, чтобы алгоритмические и аппаратные меры безопасности работали слаженно вместе. Плохо интегрированные решения могут привести к уязвимостям.

3. Эволюция угроз: Киберугрозы постоянно развиваются, требуя постоянного обновления и адаптации мер безопасности. Алгоритмические и аппаратные решения должны идти в ногу с этими изменениями.

4. Удобство использования по сравнению с другими Безопасность: важно соблюдать баланс между безопасностью и удобством использования. Чрезмерно сложные меры безопасности могут снизить производительность пользователя, в то время как чрезмерно простые могут не обеспечить адекватной защиты.

Заключение

Подводя итог следует отметить, что алгоритмическое и аппаратное управление информационной безопасностью являются неотъемлемыми компонентами защиты ресурсов информационной системы. Хотя эти меры обеспечивают надежную защиту, они должны постоянно обновляться, интегрироваться и сбалансироваться с учетом соображений удобства

использования, чтобы эффективно бороться с постоянно меняющимися методами киберугроз. По мере развития технологий организации должны сохранять бдительность в своих усилиях по защите своих ценных информационных активов.

Библиографический список:

1. Багров Е. В. Мониторинг и аудит информационной безопасности на предприятии. // Вестник ВолГУ. Серия 10. Выпуск 5. 2011 г. В.: Изд-во ВолГу, 2011, стр. 54–55.

2. Никишова А. В., Чурилина А. Е. Программный комплекс обнаружения атак на основе анализа данных реестра// Вестник ВолГУ. Серия 10. Инновационная деятельность. Выпуск 6. 2012 г. В.: Изд-во ВолГУ, 2012, стр. 152–155.