УДК 004.056.53 DOI: 10.34708/GSTOU. 2022.13.45.004

# КОНФИДЕНЦИАЛЬНЫЕ ВЫЧИСЛЕНИЯ В УСЛОВИЯХ ЗАЩИЩЕННОЙ ВЫЧИСЛИТЕЛЬНОЙ СРЕДЫ

© К. Е. Румянцев[1], Л. К. Хаджиева[2]
*[1]ЮФУ, Ростов, Россия*
*[2]ГГНТУ им. акад. М. Д. Миллионщикова, Грозный, Россия*

Обеспечение информационной безопасности является немаловажным фактором в настоящее время, особенно это касается вычислительных систем, инфокоммуникационных систем и систем передачи данных. В статье рассмотрена надежность вычислений, изложена концепция вычислений, проведена параллель между физической и логической составляющей защиты информации. Применению больших данных и технологий искусственного интеллекта в наше время уделяется все больше внимания с точки зрения защиты конфиденциальности и адекватного соответствия данных. Методы, которые могут обеспечить безопасность данных и использовать данные для доверенных вычислений в соответствии с требованиями, так называемые конфиденциальные вычисления, привлекают все больше и больше внимания людей. Решение данной проблемы в статье предлагается реализовать с применением технологии TEMPEST, которая применяет экранирование, которое ограничивает утечку электромагнитной информации от внутреннего излучения, предотвращает попадание внешних радиочастотных помех в вычислительные среды.

**Ключевые слова:** информационная безопасность, надежность вычислений, передача данных, технология TEMPEST, оборудование, ЭЛТ-терминалы, обработка больших данных, доверенные вычисления, технология экранирования.

Для начала рассмотрим дисплейный терминал обычных компьютеров, который излучает электромагнитные волны с сигналами, которые могут быть получены и воспроизведены на расстоянии 1000 м. Другие внешние устройства, такие как клавиатуры, диски и принтеры, также излучают электромагнитные волны с сигналами во время работы, в результате чего информация может быть потеряна. Электромагнитная утечка не только наносит вред здоровью людей, находящихся рядом с компьютером, но и вызывает электромагнитные помехи в окружающем электронном оборудовании и даже приводит к утечке информации. Поэтому должны быть приняты специальные технические методы для защиты и предотвращения утечки электромагнитного излучения.

Компьютерное оборудование, включая хост-компьютеры, ЭЛТ-терминалы, дисководы, ленточные накопители и принтеры, во время работы создает электромагнитную утечку в той или иной степени [1]. Например, электромагнитная утечка различных цифровых цепей в хосте, электромагнитная утечка видеосигналов дисплея, электромагнитная утечка, вызванная клавишными переключателями клавиатуры, низкочастотная электромагнитная утечка принтеров, коммуникационного оборудования и линий электропередач и т. д.

Информация внутри компьютера и его периферийных устройств может просачиваться двумя способами. Один излучается в виде электромагнитных волн, что называется утечкой излучения. Другой проводится через различные линии и металлические трубы, что называется утечкой проводимости. Например, линия электропитания компьютерной системы, телефонная линия в компьютерном зале, верхние и нижние водопроводные и отопительные трубы, а также заземляющий провод могут использоваться в качестве проводящих сред. Эти металлические проводники также иногда действуют как антенны, излучая проводимый сигнал. Из этих источников утечки

самым крупным и наиболее фундаментальным источником излучения является провод с током.

Факторы, влияющие на интенсивность излучения компьютера, в основном включают мощность и частоту, расстояние от источника излучения и условия экранирования [2].

Мощность и частота: Теоретический анализ и расчеты показывают, что чем больше сила тока в токопроводящем проводе, тем больше сила источника излучения, в противном случае она меньше. Реальные испытания показывают, что чем больше мощность устройства, тем выше интенсивность излучения. Для кондуктивных полей чем выше частота сигнала, тем выше интенсивность утечки излучения.

Расстояние от источника излучения: При тех же условиях, чем дальше от источника излучения, тем больше затухание поля, а напряженность поля обратно пропорциональна расстоянию. С этой целью рядом с компьютерным залом может быть установлен изолирующий пояс или зона предупреждения, чтобы свести к минимуму ослабление поля излучения компьютера за пределами устройства.

Состояние защиты: наличие у источника излучения средств защиты оказывает большое влияние на интенсивность его излучения.

Технология TEMPEST – чрезвычайно важный проект совместных исследований и разработок. Содержание его исследований в основном включает: механизм электромагнитной утечки оборудования для обработки информации (включая то, как и каким образом полезная информация загружается в излучаемые сигналы, а также влияние электрических характеристик и физической структуры оборудования для обработки информации на утечку и т. д.), информационное излучение, технологию защиты от утечки (включая расположение электрических компонентов, схем и печатных плат, структуру оборудования, влияние проводки и заземления на утечку излучения, различные экранирующие материалы, экранирующий эффект экранирующих конструкций и т. д., чтобы принять наиболее разумные методы и затраты на снижение интенсивности электромагнитного излучения оборудования), технологию извлечения полезной информации (включая технологию приема сигналов и технологию восстановления сигналов), технологию и стандарты испытаний (включая содержание испытаний, метод испытаний, требования к испытаниям, условия испытаний, приборы для испытаний и тесты, анализ результатов и т. д., и сформулировать соответствующие стандарты тестирования) [3,4].

Одним из важных способов пресечения утечки информации в технологии TEMPEST является технология электронного сокрытия, а также – технология физического подавления. Технология электронного сокрытия в основном включает использование помех, скачкообразной перестройки частоты и других технологий для сокрытия рабочего состояния и информации о защите всех компьютеров; технология физического подавления предназначена для подавления утечки всей полезной информации путем экранирования или запуска с линий и оборудования. На рисунке 1 показана классификация технических каналов утечки информации.

Технологию физического подавления можно разделить на метод локализации и метод подавления источника. Метод сдерживания в основном защищает линейные блоки, оборудование и даже системы, чтобы предотвратить утечку электромагнитных волн. Компьютерное оборудование, использующее метод сдерживания, имеет особый внешний вид, чтобы другие могли знать, что компьютер обрабатывает конфиденциальную информацию. Метод сдерживания в основном принимает меры с точки зрения конструкции, технологии и материалов. Метод прост, дорог и подходит для небольшого числа применений. Закон о включении все еще находится в секрете.

Принцип подавления источника начинается с цепей и компонентов и принципиально решает проблему, заключающуюся в том, что компьютер и его внешнее оборудование излучают электромагнитные волны наружу, и устраняет источник сильных электромагнитных волн [5]. Компьютер, использующий этот метод, выглядит как обычный компьютер. Обычно он использует оборудование с низким уровнем излучения и принимает следующие меры: выбирать компоненты с более


Рис. 1. Классификация технических каналов утечки информации

низким напряжением и мощностью; конструкция схемы для уменьшения связи и излучения; использовать фильтры питания и фильтры сигналов; использовать прозрачные пленки, которые блокируют электромагнитные волны; «черная» технология изоляции. На практике метод локализации и метод подавления источника обычно можно использовать в сочетании, чтобы играть роль двойной страховки.

Ниже представлены основные технические меры, принятые технологией TEMPEST в компьютере.

Использование источника шумовых помех уменьшает возможность утечки электромагнитной информации двумя способами. Один из способов заключается в размещении рядом с компьютерным оборудованием генератора шумовых помех. Шум, создаваемый генератором помех, просачивается наружу вместе с информационным излучением, создаваемым компьютерным оборудованием, так что утечку полезной информации, создаваемую компьютерным оборудованием, нелегко устранить. Другой подход заключается в размещении компьютерного оборудования, обрабатывающего важную информацию, посередине, а оборудования, обрабатывающего общую информацию, вокруг него.

Экранирование является важной мерой в технологии TEMPEST. Его назначение: ограничить утечку электромагнитной информации от внутреннего излучения, предотвратить попадание внешних радиочастотных помех в компьютерную систему. Существуют различные методы экранирования, и общее экранирование, экранирование компонентов и экранирование компонентов могут использоваться в соответствии с различными потребностями. Экранирование имеет различные конструкции и материалы, а эффект экранирования связан с такими факторами, как свойства материала, частота излучения и расстояние между конструкцией экрана и источником излучения. Например, герметизирующее экранирование

(с использованием резиновых прокладок, герметиков, уплотнительных полос и т. д.), экранирование рукавов (пластиковые рукава с металлическим напылением или металлическая сетка и т. д.), проводящие покрытия (экранирование окон помещений и токопроводящие покрытия со стеклянным напылением для экранов дисплеев).

Ключ к реализации экранирования заключается в характеристиках экранирующих материалов, особенно прокладка, оказывает большое влияние на эффект экранирования. Экранированный корпус должен быть металлическим. Экранирующий слой кабеля в основном оплетают немагнитными металлическими проволоками. Когда экранирующий слой кабеля должен одновременно обеспечивать электромагнитное экранирование, в качестве экранирующего слоя кабеля можно использовать комбинацию материалов с высокой проводимостью и высокой проницаемостью.

«Красная» и «черная» изоляции формируются по принципу: «красный» означает опасность утечки информации, «черный» означает безопасность. Красная зона относится к области обработки незашифрованной информации, красная линия относится к линии передачи незашифрованной конфиденциальной информации. Области и линии передачи, не содержащие незашифрованной полезной информации, называются черными областями и черными линиями. Выделение «красного» и «черного», а также предотвращение их объединения – важная часть технологии TEMPEST.

Фильтрация является очень важным компонентом технологии TEMPEST. Фильтры дают эффективный результат для уменьшения и подавления электромагнитной утечки. В основном это включает в себя добавление фильтров на линии передачи сигнала, линии общего заземления и линии электропередач [6].

Обычно используется многослойная разводка и технология поверхностного монтажа, а для уменьшения излучения линий выбираются крупногабаритные интегральные схемы. При прокладке проводки необходимо избегать резких изменений проводки, по возможности применяется сбалансированный метод проводки и устанавливается заземляющий слой для каждого слоя сигнальной проводки, чтобы уменьшить гармоники высокого порядка.

Рассмотрев техническую сторону электромагнитной утечки информации, а также метод решения, а точнее, применение технологии TEMPEST, которая включает механизм электромагнитной утечки оборудования для обработки информации, перейдем непосредственно к защите конфиденциальности вычислений. Так как с применением больших данных и искусственного интеллекта в наше время уделяется все больше внимания защите конфиденциальности и соответствию данных. Таким образом, метод, который может защитить безопасность данных и использовать данные для вычислений в соответствии с требованиями, так называемые конфиденциальные вычисления, привлекает все больше и больше внимания людей.

В научной теории безопасности информации имеется много терминов и понятий, связанных с конфиденциальными вычислениями, такими как надежные вычисления, конфиденциальные вычисления, безопасные вычисления и так далее. Опишем здесь концептуальные различия между ними.

*Надежные вычисления.* С точки зрения происхождения и масштаба доверительные вычисления в настоящее время являются наиболее зрелыми и имеют самый большой охват, который возник из безопасности информационных систем и выдвинул концепцию доверенной схемы и доверенной системы [7].

Определение доверенных вычислений – объекту доверяют, если его поведение всегда достигает ожидаемой цели ожидаемым образом. Стандарт ISO/IEC 15408 определяет надежность как: компоненты, операции или процессы, связанные с вычислениями, предсказуемы в произвольных условиях и устойчивы к вирусам и физическому вмешательству.

В спецификации Trusted Computing Group (Trusted Computing Group – TCG) для доверенных вычислений определены три свойства:

1. Аутентификация: пользователи компьютерной системы могут установить личность тех, с кем они общаются.

2. Целостность: пользователь гарантирует, что информация может быть передана правильно.

3. Конфиденциальность: пользователь доверяет системе сохранять конфиденциальность информации.

С этой точки зрения основной целью доверенных вычислений является широкое использование доверенных вычислительных платформ, поддерживаемых аппаратными модулями безопасности в вычислительных и коммуникационных системах, для повышения безопасности всей системы.

Одним из наиболее важных элементов доверенных вычислений является Trusted Execution Environment (TEE), представляющий собой тип Trusted Platform Module (TPM). Приведем здесь описание основных функций для повышения безопасности конечных систем.

TEE в основном защищает операции и операции, связанные с личными данными, с помощью аппаратных средств и гарантирует, что конфиденциальные данные хранятся, обрабатываются и защищаются в изолированной и надежной среде, предоставляя безопасную зону. В настоящее время относительно надежной системой TEE является расширение набора инструкций на основе TEE, SGX (Intel Software Guard Extension).

Основная цель заключается в выполнении безопасных вычислений с данными в облачной среде. Это можно рассматривать как доверительные вычисления в облаке для обеспечения безопасности данных клиентов. Конфиденциальные вычисления основаны на аппаратной технологии микропроцессора, виртуальных образах и программных средствах в облаке, так что пользователи в облаке могут создать полностью изолированную доверенную среду выполнения, также известную как безопасная область, поскольку конфиденциальные вычисления, используемые или выполняемые, шифруют данные таким образом, что ни операционная система хоста, ни поставщик облачных услуг не могут идентифицировать конфиденциальную информацию в этих анклавах, предотвращая вмешательство третьих лиц в обрабатываемые данные.

Ядром конфиденциальных вычислений является TEE в облаке, и технология TEE может использоваться для изоляции данных, таких как отпечатки пальцев, пароли и процессы сбора, хранения и проверки информации о лицах.

Пересечением этих концепций безопасности является криптография, которая также является основой безопасности данных.

Современные методы вычисления конфиденциальности можно классифицировать в зависимости от того, искажены данные или нет. Методы защиты конфиденциальности без искажения данных в основном основаны на криптографических методах, включая гомоморфные схемы шифрования и безопасные многосторонние вычисления.

По концептуальной классификации указанные выше категории относятся к категории доверенных вычислений.

– Доверенные вычисления расширяются за счет доверенных систем, и их объем является самым высоким, включая передачу, хранение, вычисления и другие аспекты.

– Конфиденциальные вычисления – это концепция, расширенная из облачных вычислений, и ее основное применение находится в области безопасных вычислений облачных вычислений.

– Конфиденциальные вычисления – это концепция обеспечения безопасности данных в процессе вычисления данных, и ядром является защита конфиденциальности данных.

– Безопасные вычисления, также известные как безопасные многосторонние вычисления, представляют собой особую технологию реализации конфиденциальных вычислений.

Безопасные вычисления, также известные как безопасные многосторонние вычисления (сокращенно MPC, также называемые SMC или SMPC), являются теоретической основой распределенной криптографии и основной проблемой в исследованиях распределенных вычислений.

В концепции безопасных вычислений можно проследить двухсторонний безопасный метод вычислений, основанный на запутанных цепях, а позже постепенно были созданы различные алгоритмы, основанные на запутанных цепях и совместном использовании секрета.

Ядро основной двухсторонней защищенной вычислительной среды использует два криптографических метода: искаженную цепь и забытую передачу. Общая многосторонняя защищенная вычислительная среда позволяет нескольким сторонам безопасно вычислять результаты любой функции или класса функций.

Безопасные многосторонние вычисления относятся к реализации многосторонних вычислений с целью защиты безопасности данных. То есть в распределенной сети каждый участник имеет секретные входы и надеется совместно завершить вычисление определенной функции, но каждый участник не обязан получать никакой входной информации от других участвующих сущностей, кроме результата вычисления. То есть каждый участник выполняет часть расчета, а окончательный результат расчета осваивается или публично делится некоторыми участниками.

Основа многосторонних безопасных вычислений также основана на криптографических технологиях конфиденциальности, включая гомоморфное шифрование, забывчивую передачу, искаженную цепь, совместное использование секрета и т. д.

*Выводы.* Подводя итоги, можно сказать, что в данной статье рассмотрена проблема электромагнитной утечки, которая не только наносит вред, но и способствует утечке информации. Решение данной проблемы возможно с применением технологии TEMPEST, которая включает механизм электромагнитной утечки оборудования для обработки информации, а также применяет экранирование, которое ограничивает утечку электромагнитной информации от внутреннего излучения, предотвратив попадание внешних радиочастотных помех в компьютерную систему.

**ЛИТЕРАТУРА**


1. *Минцаев М. Ш., Хакимов З. Л., Лабазанов М. А.* Программирование логических контроллеров фирмы SIEMENS // Лабораторный практикум. Грозный, 2021.
2. *Алисултанова Э. Д., Хаджиева Л. К., Исаева М. З.* Профориентационная школьная лаборатория по основам кибербезопасности в сфере интернет вещей (IOT) // Вестник ГГНТУ. Гуманитарные и социально-экономические науки. 2019. Т. 15. №4 (18). С. 51-58.
3. *Алисултанова Э. Д., Тасуева Х. Х.* Особенности и формы в образовании // Вестник ГГНТУ. Гуманитарные и социально-экономические науки. 2019. Т. 15. №1 (15). С. 68.
4. *Моисеенко Н. А., Темирова А. Б.* Научное образование как основа формирования инновационной компетентности в условиях цифровой трансформации общества // Вестник ГГНТУ. Гуманитарные и социально-экономические науки. 2022. Т. 18. №1 (27). С. 60-66.
5. *Моисеенко Н. А., Алисултанова Э. Д., Албакова А. А.* Использование информационных систем для оценки научной деятельности преподавателей вуза // Управление образованием: теория и практика. 2021. №6 (46). С. 19-27.
6. *Румянцев К. Е.* Защита процесса синхронизации в системе квантового распределения ключа с автоматической компенсацией поляризационных искажений // Телекоммуникации. 2017. №3. С. 36-44. https://elibrary. ru/item. asp?id=28860318
7. *Румянцев К. Е., Рудинский Е. А.* Двухэтапный временной алгоритм синхронизации в системе квантового распределения ключа с автоматической компенсацией поляризационных искажений // Известия ЮФУ. Технические науки. 2017. №5. С. 75-89.

# CONFIDENTIAL COMPUTING IN A PROTECTED COMPUTING ENVIRONMENT

© K. E. Rumyantsev[1], L. K. Khadzhieva[2]
*[1]SFU, Rostov, Russia*
*[2]GSTOU, Grozny, Russia*

Ensuring information security is no small important factor at present, especially for computing systems, infocommunication systems and data transmission systems. Since electromagnetic leakage not only harms the health of people who are near the computer, but also causes electromagnetic interference in the surrounding electronic equipment and leads to information leakage, this article discusses methods for protecting information and preventing leakage of electromagnetic radiation, analyzes methods for protecting information and their applications. The TEMPEST shielding technology, which includes the mechanism of electromagnetic leakage of information processing equipment, is considered. In addition to electromagnetic information leakage, the article considers the reliability of calculations, outlines the concept of calculations, draws a parallel between the physical and logical components of information protection.

**Keywords**: information security, reliability of calculations, data transmission, TEMPEST technology, equipment, CRT terminals, data processing.

**REFERENCES**

1. Mintsaev, M. Sh., Khakimov, Z. L. and Labazanov, M. A. (2021) Programmirovanie logicheskikh kontrollerov firmy SIEMENS. [Programming logic controllers from SIEMENS. Laboratory workshop Laboratornyi praktikum]. Grozny.
2. Alisultanova E. D., Khadzhieva L. K., Isaeva M. Z. (2019) Proforientatsionnaya shkol'naya laboratoriya po osnovam kiberbezopasnosti v sfere internet veshchei (IOT) [Vocational guidance school laboratory on the basics of cybersecurity in the field of the Internet of Things (IOT). Herald of GSTOU. Humanitarian, social and economical sciences]. *Vestnik GGNTU. Gumanitarnye i sotsial'no-ekonomicheskie nauki.* V. 15, № 4 (18), pp. 51-58
3. Alisultanova, E. D. and Tasueva, Kh. Kh. (2019) 'Osobennosti i formy v obrazovanii'. [Peculiarities and forms in education. Herald of GSTOU. Humanitarian, social and economical sciences]. *Vestnik GGNTU. Gumanitarnye i sotsial'no-ekonomicheskie nauki.* V. 15, № 1 (15), p. 68.
4. Moiseenko, N. A. and Temirova, A. B. (2022) 'Nauchnoe obrazovanie kak osnova formirovaniya innovatsionnoi kompetentnosti v usloviyakh tsifrovoi transformatsii obshchestva'. [Scientific education as the basis for the formation of innovative competence in the context of the digital transformation of society. Herald of GSTOU. Humanitarian, social and economical sciences]. *Vestnik GGNTU. Gumanitarnye i sotsial'no-ekonomicheskie nauki.* 2022. T. 18. № 1 (27). S. 60-66.
5. Moiseenko, N. A., Alisultanova, E. D. and Albakova, A. A. (2021) 'Ispol'zovanie informatsionnykh sistem dlya otsenki nauchnoi deyatel'nosti prepodavatelei vuza'. [The use of information systems to assess the scientific activities of university teachers. Management of education: theory and practice]. *Upravlenie obrazovaniem: teoriya i praktika.* № 6 (46), pp. 19-27.
6. Rumyantsev, K. E. (2017) 'Zashchita protsessa sinkhronizatsii v sisteme kvantovogo raspredeleniya klyucha s avtomaticheskoi kompensatsiei polyarizatsionnykh iskazhenii'. [Protection of the synchronization process in a quantum key distribution system with automatic compensation of polarization distortions. Telecommunications]. *Telekommunikatsii.* № 3, pp. 36-44, available at: www://elibrary. ru/item. asp?id=28860318
7. Rumyantsev, K. E. and Rudinskii, E. A. (2017) 'Dvukhetapnyi vremennoi algoritm sinkhronizatsii v sisteme kvantovogo raspredeleniya klyucha s avtomaticheskoi kompensatsiei polyarizatsionnykh iskazhenii. [Two-stage temporal synchronization algorithm in a quantum key distribution system with automatic compensation of polarization distortions. Izvestiya of SFU. Technical sciences]. *Izvestiya YuFU. Tekhnicheskie nauki*. № 5, pp. 75-89.