Плетнев Никита Сергеевич, курсант
Военная академия защиты информации
им. генерала армии С.М. Штеменко
Pletnev Nikita Sergeevich

Щербаков Максим Николаевич, курсант
Военная академия защиты информации
им. генерала армии С.М. Штеменко
Shcherbakov Maxim Nikolaevich

Сбитнев Егор Алексеевич, Старший преподаватель
Военная академия защиты информации
им. генерала армии С.М. Штеменко
Sbitnev Egor Alekseevich

ВОЗМОЖНОСТИ РЕАЛИЗАЦИИ АППАРАТНО-ПРОГРАММНОЙ КРИПТОГРАФИЧЕСКОЙ САНАЦИИ (АПКС) МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ
POSSIBILITIES OF IMPLEMENTING HARDWARE-SOFTWARE CRYPTOGRAPHIC SANITIZATION (HSCS) OF MACHINE INFORMATION MEDIA

Аннотация. В статье рассматривается проблема экстренного уничтожения информации на современных машинных носителях. Показано, что традиционные методы разрушения обладают рядом критических недостатков. В качестве альтернативы исследуется метод аппаратно-программной криптографической санации (АПКС). Внедрение подобных систем позволяет обеспечить необратимую ликвидацию данных за доли секунды и легко интегрируется в существующую IT-инфраструктуру.

Abstract. The article discusses the problem of emergency data destruction on modern machine media. Traditional destruction methods have critical drawbacks. As an effective alternative, the method of hardware and software cryptographic sanitization (HSCS) is investigated. The implementation of such systems ensures irreversible data elimination in fractions of a second.

Ключевые слова: Информационная безопасность, экстренное уничтожение данных, криптографическая санация, машинные носители информации, деструкция ключей шифрования.

Keywords: Information security, emergency data destruction, cryptographic sanitization, machine information media, encryption key destruction.

Стремительная эволюция архитектуры вычислительных систем и массовый переход корпоративного и государственного секторов на твердотельные накопители (SSD) требуют радикального пересмотра классических парадигм защиты информации, регламентированных базовыми стандартами [1]. В условиях возникновения нештатных ситуаций (несанкционированный физический доступ к серверному оборудованию, компрометация периметра безопасности) критически важным протоколом становится экстренное уничтожение данных, что особенно актуально для объектов критической информационной инфраструктуры [2]. Исторически сложившийся подход, ориентированный на использование магнитных жестких дисков (HDD), предполагал применение мощных электромагнитных импульсов (ЭМИ) или установок грубого механического разрушения. Однако архитектура современной NAND-памяти делает эти методы недостаточно эффективными [4]. Физическое измельчение терабайтного массива NVMe-накопителей занимает время, значительно превышающее допустимое «окно уязвимости», а остаточные фрагменты кремниевых кристаллов в теории могут быть подвергнуты криминалистическому анализу. В связи с этим на первый план выходят методы, использующие математический аппарат [5]. Современные стандарты хранения данных подразумевают аппаратное шифрование информации «на лету» [3].

Это открывает путь для внедрения систем аппаратно-программной криптографической санации (АПКС). Целью данной статьи является исследование теоретических основ криптографической санации и анализ возможностей практической реализации аппаратно-программных комплексов, способных обеспечить сверхбыстрое и гарантированно необратимое уничтожение информации на современных машинных носителях.

Теоретико-алгоритмическая модель АПКС Основой метода АПКС является концепция самошифруемых дисков (Self-Encrypting Drives, SED).

В таких накопителях вся пользовательская информация непрерывно шифруется аппаратным контроллером с использованием надежных симметричных алгоритмов криптографической защиты [6]. Процесс опирается на иерархию ключей: Media Encryption Key (MEK): генерируется на заводе, хранится в защищенной области контроллера диска и используется непосредственно для шифрования данных на чипах памяти. Key Encryption Key (KEK): Ключ, который шифрует сам MEK. Он формируется на основе пользовательского пароля или иных данных авторизации. Суть криптографической санации заключается не в перезаписи ячеек памяти нулями, а в инициации команды, которая мгновенно генерирует новый ключ MEK, необратимо перезаписывая старый [5, 6]. Как только исходный ключ уничтожен, весь массив зашифрованных данных превращается в криптографический шум. Попытки восстановить данные путем анализа остаточных хеш-сумм, прямого чтения ячеек памяти или поиска уязвимостей обхода контроллера математически бессмысленны без знания уничтоженного ключа [3].

Возможности практической реализации, для интеграции метода АПКС в реальную инфраструктуру требуется создание комплекса, состоящего из аппаратного инициатора и программного обработчика. Аппаратный уровень: Разработка автономного контроллера, который оснащен физическими или дистанционными триггерами (радиоканал, GSM-модуль, датчики вскрытия корпуса). Данный модуль должен иметь независимое питание (суперконденсаторы) для обеспечения срабатывания даже при обесточивании основного сервера, что отвечает современным требованиям безопасности в условиях дефицита времени [4].

Программный уровень: при активации триггера контроллер отправляет низкоуровневую команду санации напрямую в контроллер накопителя. Преимущество такой реализации заключается в том, что выполнение команды берет на себя контроллер самого диска, что исключает зависимость от операционной системы и центрального процессора. Время выполнения полного цикла криптографической санации составляет от нескольких десятков до сотен миллисекунд.

Заключение

Внедрение технологии аппаратно-программной криптографической санации (АПКС) представляет собой наиболее перспективный вектор развития систем экстренного уничтожения данных.

В отличие от традиционных физико-химических методов, АПКС лишена проблем с энергоемкостью, пожароопасностью и длительным временем срабатывания. Использование математического аппарата криптографии переводит задачу уничтожения информации из плоскости грубого механического воздействия в плоскость алгоритмического контроля. Практическая реализация таких комплексов позволяет с минимальными затратами интегрировать надежные системы защиты в любую современную IT-инфраструктуру Российской Федерации, обеспечивая мгновенную и стопроцентно необратимую ликвидацию критически важных массивов данных в соответствии с актуальными требованиями регуляторов.

Список литературы:

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.
2. Приказ ФСТЭК России от 25.12.2017 N 239 "Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации".

3. Авраменко В.С. Криптографическая защита информации: учебное пособие.

4. Машкин Н.В., Семенов А.А. Проблемы гарантированного уничтожения информации на современных твердотельных накопителях. Вопросы кибербезопасности.

5. Русаков А.М. Анализ методов и средств экстренного уничтожения данных на твердотельных носителях. Информационная безопасность и защита информации.

6. Бабенко Л.К. Современные алгоритмы защиты машинных носителей информации в условиях дефицита времени. Безопасность информационных технологий.

7. Сбитнев Е.А., Акишин А.В., Дубовцов И.А., Лукьянов Р.В., Пискарев В.С. Разработка рекомендаций руководителю подразделения информационной безопасности предприятия по организации и контролю соблюдения конфиденциальности информации при обращении со средствами криптографической защиты информации в повседневной деятельности.