УДК 004.056

М.А. ИВАНОВ
Государственный университет управления», Москва
Национальный исследовательский ядерный университет «МИФИ», Москва

СТОХАСТИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Отмечается важная роль стохастических методов при решении задач защиты информации, главный результат применения которых – это внесение непредсказуемости в работу защищаемого цифрового объекта и средств обеспечения его безопасности. Базовым элементом в этой ситуации становится непредсказуемый генератор псевдослучайных чисел.

Любая атака на компьютерные системы начинается с исследования атакуемого объекта либо на модели, либо на реальной системе. У нападающей стороны всегда есть резерв времени для поиска уязвимостей в целевой вычислительной системе, при этом ему достаточно обнаружить только одно слабое место в ее защите, чтобы провести успешную атаку. Задача защищающейся стороны значительно сложнее, ей надо выявить и ликвидировать все слабые места в системе, при этом анализ ее защищенности необходимо проводить постоянно и на всех уровнях: элементная база, архитектура, системное ПО, сетевое ПО, прикладное ПО; учитывая, что задачи защиты информации надо решать в динамике, а не в статике.

Кроме того, защита практически никогда не знает, кто ее будет атаковать и когда, что является целью атакующего и какие у него возможности. При этом задачи защиты информации очень часто решаются по остаточному принципу, когда продукт, система или технологии уже созданы, при этом используются реактивные методы защиты, которые развиваются лишь по мере появления новых угроз информационной безопасности и новых механизмов проведения атак на компьютерные системы.

В этой ситуации положение защиты выглядит безнадежным и на вопрос, каким образом она может получить преимущество перед нападением, казалось бы, единственным правильным ответом будет – никогда. Однако выход есть и этот выход – использование стохастических методов защиты информации, которыми принято называть методы, основанные на использовании генераторов псевдослучайных чисел и хеш-генераторов [1–3]. Примеров эффективного применения стохастических

методов защиты накопилось множество [1, 4–6], при этом надо отметить их универсальность, так как они могут использоваться совместно с любым другим методом защиты, автоматически повышая его качество.

Стохастические методы защиты информации являются методами двойного назначения. Первыми, еще в прошлом веке их стали применять создатели компьютерных вирусов (КВ) (пермутирующие, полиморфные, метаморфные КВ), затем уже в 21 веке разработчики других типов вредоносных программ (AdmMutate, Ransomware и пр.).

Наиболее перспективными направлениями использования генераторов псевдослучайных чисел, которые начали развиваться в последние годы, являются Logic Encryption, Design Obfuscation (механизм скрытых функций, многовариантная логика и др.), Moving Target Defense, Control Flow Integrity. При этом последние две технологии являются попытками защититься от атак, основанных на эксплуатации уязвимостей ПО, т.е. речь по сути дела идет о создании стохастического процессора.

Таким образом, актуальной научной задачей является разработка непредсказуемых и статистически безопасных генераторов псевдослучайных чисел (в некоторых случаях с нестандартными графами переходов), ориентированных на использование в задачах защиты информации, и их интеграция в структуру вычислительных систем и их элементов.

Список литературы

1. Осмоловский С.А. Стохастические методы передачи данных. – М.: Радио и связь, 1991. – 240 с.
2. Осмоловский Стохастические методы защиты информации. – М.: Радио и связь, 2003. – 319 с.
3. Осмоловский С.А. Стохастическая информатика: инновации в информационных системах. − М.: Горячая линия–Телеком, 2012. – 320 с.
4. Wenbo Mao. Modern Cryptography: Theory and Practice. Prentice Hall, 2003.
5. М.А. Иванов. Способ обеспечения универсальной защиты информации, пересылаемой по каналу связи. // Вопросы кибербезопасности. – 2019. – № 3(31). – С. 45−50. DOI: 10.21681/2311-3456-2019-3-45-50.
6. Иванов М.А. Основы криптографии. В 2 частях. – М.: ГУУ, 2023.