

## КРИПТОГРАФИЯ И ЗАЩИТА ИНФОРМАЦИИ

Рассматривается связь между криптографией и теорией защиты информации. Для определения предметной области и методов криптографии в рамках теории защиты информации предложено описывать атаки на информационную систему в рамках исчисления, задаваемого моделью возможностей нарушителя. На моделях возможностей установлено отношение порядка, которое индуцирует упорядоченность на безопасных информационных системах. Криптография характеризуется невырожденными моделями возможностей, предполагающими возможность вычислений.

**Rostovtsev A. (SPbSTU)**

### **Cryptography and information security**

Relation between cryptology and theoretical information security is considered. The subject matter and research methods of cryptology as part of information protection science are determined by deducing attack set in the calculus according to the intruder's possibility model. Intruder's possibility models as sets are ordered by inclusion, this order induces the order on set of secure information systems. Cryptography provides protection against non-degenerate intruder's possibility model, which assumes computational and mathematical possibilities.

## 1. Определения криптографии

Теория и техника защиты информации развиваются настолько быстро, что специалисты в различных областях защиты информации иногда с трудом понимают друг друга. Целью этой статьи является ответ на два вопроса: Когда верна основная теорема безопасности<sup>1</sup>? Какое место занимает криптография в защите информации?

Начнем со второго вопроса. В настоящее время существует несколько определений криптографии.

Д. Кан [9] называет криптографией искусство хранить информацию в секрете. Однако хранить информацию в секрете можно, запретив или ограничив доступ к ней (с помощью соответствующей блокировки или с помощью первого отдела).

Согласно Коблицу [10] и Конхейму [11] криптография — это искусство и наука сделать передаваемую информацию доступной только для данного получателя. Однако передаваемую информацию можно спрятать (например, в каблуке ботинка), скрыв сам факт передачи. Очевидно, что такой способ передачи тоже не относится к криптографии.

В работах [12] и [1] под криптографией понимают изучение математических методов, связанных с такими функциями защиты информации,

---

<sup>1</sup> Основная теорема безопасности Белла — Лападулы [5] утверждает, что если информационная система начинает работу из безопасного состояния и переход из состояние в состояние безопасен, то все состояния системы безопасны.

как конфиденциальность и целостность данных. Но конфиденциальность и целостность являются частью защиты от несанкционированного доступа и несанкционированного воздействия на информацию [3], которые с математической точки зрения рассматриваются в работе [5]. Однако методы исследования в этой работе не криптографические. Поэтому такое определение тоже не вполне удовлетворительно.

Для ответа на поставленный вопрос рассмотрим некоторые положения теории информации.

Защищенная информационная система должна противостоять атакам со стороны нарушителя. Безопасность информационных систем можно рассматривать двояко: обеспечивается ли защита от заданных угроз и реализуема ли данная угроза? Ответ на первый вопрос описывается политикой безопасности. Ответ на второй вопрос в определенном смысле является предметом изучения криптографии.

## 2. Исчисление атак

Совокупность всевозможных действий нарушителя (атак) определяется его возможностями, поэтому будем говорить о модели возможностей нарушителя, которая позволяет (но не предписывает) нарушителю действовать так или иначе для достижения своей цели. Модель возможностей нарушителя в рамках формальной логики является аналогом системы аксиом некоторой теории, а совокупность всевозможных реализуемых атак — аналогом множества истинных утверждений этой теории.

Атаки могут быть описаны в терминах теории исчислений. Исчисление отличается от алгоритма тем, что на каждом шаге разрешает то или иное действие в рамках заданных правил вывода, тогда как алгоритм предписывает такое действие.

Чем меньшими (большими) возможностями обладает нарушитель, тем легче (труднее) ему противостоять. В предельном случае, если модель возможностей пустая (нарушитель не может ничего), то любая система является безопасной. Для другого крайнего случая — нарушитель обладает экстрасенсорными способностями и может узнать любой секрет — безопасных систем не существует.

Предположим, есть две модели возможностей нарушителя, причем вторая содержит в себе первую. В этом случае можно сказать, что вторая модель возможностей больше первой, а множество атак для второй модели включает в себя множество атак для первой модели. Таким образом, на множестве моделей возможностей нарушителя и множестве атак определено отношение частичного порядка, индуцированное упорядоченностью множеств по включению.

Упорядоченность моделей возможностей нарушителя индуцирует и упорядоченность информационных систем по безопасности: чем больше возможности нарушителя, тем сложнее противостоять атакам. Система, безопасная по отношению к меньшей модели, может не быть безопасной

по отношению к большей модели. Таким образом, понятие безопасности информационной системы справедливо только для определенной моделей возможностей.

При построении и анализе безопасности защищенных информационных систем часто требуется решать две задачи. Первая задача: в рамках заданной модели возможностей нарушителя определить, является ли данная система безопасной (существует доказательство безопасности), небезопасной (существует доказательство небезопасности) или неопределенной (отсутствуют доказательства безопасности и небезопасности). Вторая задача: для данной информационной системы найти максимальную модель возможностей, для которой система безопасна (существует доказательство безопасности). Для того чтобы указанные доказательства имели смысл, система аксиом, задаваемых моделью возможностей нарушителя, должна быть непротиворечивой.

### **3. Модели возможностей нарушителя и безопасность**

На практике модель возможностей нарушителя определяется в нормативных документах и уточняется в техническом задании на разработку. История защиты информации показывает, что для достижения цели нарушитель может предпринимать атаки, связанные с комплексным использованием вычислительных, математических, криптоаналитических, технических, организационных и других способов нападения [9].

Вычислительные возможности нарушителя учитывают тип вычислительной модели, ее производительность, объем памяти. Атаку на информационную систему в рамках заданной вычислительной модели можно описать вероятностным алгоритмом, который характеризуется временной и емкостной сложностью и вероятностью успеха. Результатом атаки является реализация некоторой угрозы. Как правило, если данная угроза реализуема в рамках модели возможностей, то она может быть реализована с использованием различных вероятностных алгоритмов. Из нескольких алгоритмов лучшим является тот, который при одинаковой вероятности успеха имеет наименьшую сложность. Система является безопасной, если сложность наилучшего известного алгоритма превышает пороговую при заданной вероятности реализации угрозы.

Технические возможности нарушителя описывают инструмент, реализующий атаку. В частности, технические возможности могут позволять нарушителю не только использовать компьютер для доступа в систему, но и получать дополнительную информацию о секретных данных, не обращаясь установленным порядком к области памяти, где эти данные хранятся. В процессе обработки секретной информации с помощью материальных средств возникают физические поля, которые (по крайней мере, теоретически) могут быть измерены с помощью лабораторных методов и средств и несут нарушителю некоторую информацию о защищаемом секрете. В некоторых случаях нарушитель может воздействовать на аппаратуру защиты

информации с помощью физических полей с целью снижения ее защитных качеств. Если конфиденциальная информация была записана в памяти компьютера (магнитной, полупроводниковой и т. п.), то стирание этой информации должно исключать возможность восстановления ее лабораторными методами.

Математические возможности нарушителя позволяют ему разрабатывать новые эффективные методы и алгоритмы решения массовых математических задач, положенных в основу безопасности. Например, уже многие годы наблюдается стабильный прогресс в построении все более быстрых алгоритмов разложения числа на множители, что вызывает необходимости периодического увеличения длины составного числа в системе RSA [4].

Криптоаналитические возможности нарушителя позволяют разрабатывать алгоритмы взлома данного криптоалгоритма с использованием как универсальных, так и специальных методов анализа. Отличие этих возможностей от математических заключается в использовании методов криптоанализа, а также в том, что решается не массовая, а частная задача.

Организационные возможности нарушителя позволяют ему использовать соответствующие способы получения дополнительной информации, потенциально способной снизить уровень безопасности. Эти возможности включают в себя трудно формализуемый список, например:

- получение открытых текстов, соответствующих данным шифrogramмам;
- доступ к шифровальной аппаратуре для тестирования ее с помощью подобранных открытых текстов;
- доступ к ключам шифрования, выведенным из действия;
- возможность подмены существующих программ;
- вербовка помощников среди обслуживающего персонала и т. п.

Указанные возможности нарушителя могут использоваться комплексно, усиливая и дополняя друг друга. Рассмотрим некоторые типовые модели возможностей нарушителя, с учетом их упорядочения.

### **3.1. Вырожденная модель возможностей нарушителя**

Назовем модель нарушителя вырожденной, если единственный способ для нарушителя получить сведения о секретной информации — выполнить ее чтение установленным порядком, а единственный способ для нарушителя изменить информацию — выполнить запись установленным порядком<sup>2</sup>.

---

<sup>2</sup> Эта модель действий нарушителя названа вырожденной, так как вся многовековая история защиты информации от несанкционированного доступа и несанкционированного воздействия показывает, что если нарушитель действительно хочет узнать то, что ему не положено, он обычно применяет значительно более широкий спектр действий. Например, для того чтобы вскрыть секретную переписку короля Испании Филиппа II, придворный криптоаналитик короля Франции Генриха Наваррского Франсуа Виет

Данная возможность может считаться технической, если система построена с использованием компьютеров, или организационной, например, если система представляет собой обычную библиотеку. Поэтому безопасность может быть обеспечена техническими или организационными мерами — нужно обеспечить необходимые блокировки, обеспечивающие доступ информации только при наличии соответствующего разрешения. Способ реализации этих блокировок (организационный или технический) в системном плане непринципиален.

Если в защищаемая информация упорядочена по уровню своей секретности, а субъекты системы (пользователи, аппаратура, программы и т. п.) — по своим полномочиям, которые соответствуют грифам информации, то в рамках этой же модели возможностей получается модель безопасности Белла — Лападулы.

Система называется безопасной по чтению (по записи) в смысле Белла — Лападулы тогда и только тогда, когда полномочия субъекта по чтению (по записи) соответствуют уровню секретности информации.

Система называется безопасной в смысле Белла — Лападулы тогда и только тогда, когда она безопасна в этом смысле по чтению и по записи.

Вырожденная модель действий нарушителя в рамках системы с иерархией субъектов и объектов взаимно однозначно соответствует понятию безопасности в смысле Белла — Лападулы. Действительно, при указанных возможностях нарушителя определения безопасности по записи и чтению вполне осмысленны и корректны. Обратно, из определений безопасности по Беллу — Лападуле следует, что возможности нарушителя ограничены вырожденной моделью.

**Теорема 1.** Все атаки исчисления, порожденного вырожденной моделью возможностей нарушителя, соответствующей модели безопасности Белла — Лападулы, описываются на языке логики предикатов первого порядка.

Набросок доказательства. Любая атака представлена в виде последовательности действий пользователей системы и нарушителя. Такая последовательность содержит конечное число действий (чтение или запись), каждое из которых можно описать с использованием переменных (имена субъектов, объектов и их грифов), а также элементов матрицы доступа, операций чтения и записи, скобок и кванторов существования и всеобщности. Такая грамматика определяет язык теории множеств Цермело — Френкеля [2], который относится к языкам предикатов первого порядка. При этом все вхождения переменных в формулы оказываются связанными с помощью кванторов существования и всеобщности. Этот язык позволяет описывать в атаке состояния, полученные на предыдущих шагах исчисления. Отсюда следует заключение теоремы. ■

---

(известный как один из родоначальников алгебры) не получал разрешения с печатью испанского короля — он неоднократно делал это без разрешения [10].

Язык логики предикатов позволяет каждой атаке сопоставить логическую функцию, которая принимает значение 1 тогда и только тогда, когда эта атака выводима в рамках данной модели возможностей нарушителя.

**Следствие 2.** В модели безопасности Белла – Лападулы множество допустимых атак является разрешимым (для логической функции, описывающей выводимость атаки, может быть доказана ее истинность или ее ложность).

Доказательство следует из теоремы 1 и теоремы Геделя о полноте [6], справедливой для логики предикатов первого порядка. ■

Понятие безопасности в смысле Белла — Лападулы является абсолютным: безопасная система всегда остается безопасной. В рамках этого исчисления справедлива основная теорема безопасности: система безопасна тогда и только тогда, когда начальное состояние системы безопасно и переход из состояния в состояние безопасен [5]. Эта теорема является важным инструментом анализа безопасности систем в рамках указанной модели возможностей нарушителя. Она позволяет рассматривать не всю «историю» работы системы, а только одиночные переходы из безопасного состояния в безопасное же состояние.

Вырожденная модель возможностей нарушителя, хотя и является одной из самых слабых в иерархии моделей, обладает рядом преимуществ по сравнению с моделями более высокого уровня. Она позволяет использовать хорошо разработанный аппарат логики предикатов первого порядка. Каждая атака представляет собой вывод в исчислении предикатов, корректность каждого шага в выводе может быть легко проверена.

### **3.2. Невырожденная модель (с вычислительными, математическими, криптоаналитическими возможностями)**

Иногда для того чтобы узнать секретную информацию, нарушителю не надо выполнять операцию чтения — эту информацию можно найти иначе. Например, секретный ключ шифрования или подписи обычно можно вычислить (по крайней мере, теоретически).

Порождающие правила в рамках этого исчисления, помимо перечисленных в п. 3.1, предполагают возможность использования методов математики и криптоанализа, направленных на вскрытие секретной информации (ключа). Для этой модели система является безопасной, если она, во-первых, безопасна в смысле Белла — Лападулы, а во-вторых, сложность вскрытия секретной информации наилучшим (известным) алгоритмом превышает пороговую.

Однако методы криптоанализа и вычислительная техника постоянно совершенствуются. Это обуславливает относительность понятия безопасности: система, безопасная сегодня, может не быть безопасной завтра. Отсюда следует необходимость периодической переаттестации системы на

предмет безопасности, то есть необходимость научного (в первую очередь математического и криптографического) сопровождения системы в ходе всего срока ее эксплуатации.

Если разработчик старается обеспечить безопасность системы в течение всего срока эксплуатации, то нарушитель старается эту безопасность нарушить. Для того чтобы минимизировать ущерб от возможного взлома подсистемы безопасности в ходе эксплуатации, разработчик должен обнаружить возможность взлома до того, как этим воспользуется нарушитель, и принять соответствующие меры. Таким образом, между разработчиком и нарушителем происходит непрерывное соревнование в развитии методов нарушения информационной безопасности (в первую очередь, методов криптоанализа). Как правило, на начальном этапе разработчик владеет более перспективными методами анализа данного шифра, чем нарушитель. В идеале такое положение должно выполняться в течение всего срока эксплуатации системы. Таким образом, разработчик вынужден постоянно разрабатывать новые методы взлома системы безопасности, чтобы опережать в этом нарушителя.

Покажем, что для этой модели возможностей нарушителя основная теорема безопасности может не выполняться. Пусть в информационной системе используется алгоритм электронной цифровой подписи по ГОСТ Р 34.10–2001, предусматривающий использование случайного числа. Ключ создания подписи является охраняемой конфиденциальной информацией. Алгоритм подписи характеризуется тем, что повторение дважды одного и того же случайного числа влечет вскрытие секретного ключа создания подписи, причем случай повтора можно эффективно распознать [4]. В качестве генератора случайных чисел выберем генератор BBS (Блюма — Блюма — Шуба) [8], формирующий периодическую псевдослучайную криптографически стойкую последовательность<sup>3</sup>. При достаточно длительной эксплуатации системы последовательность случайных чисел начнет повторяться, что позволит нарушителю вскрыть секретный ключ. Характеристику кольца можно выбрать так, что сложность предсказания последующего числа при известном предыдущем будет сколь угодно велика, а период повторения окажется небольшим. В этом случае каждый переход системы из предыдущего состояния в последующее, рассматриваемый отдельно, оказывается безопасен, но после определенного числа таких переходов система не будет безопасной.

По-видимому, в рамках этой модели не существует криптосистем, для которых теорема Белла — Лападулы справедлива. Это объясняется тем, что практическая стойкость криптографических методов защиты информации непрерывно снижается и при неограниченно длительной эксплуатации системы стойкость станет недопустимо низкой [4].

---

<sup>3</sup> Генератор BBS вырабатывает рекуррентную последовательность  $x_{i+1} \equiv x_i^2 \pmod{n}$ , где  $n = pq$  — составное число с неизвестным разложением. Период повторения является кратным порядков циклических групп с образующей 2 в  $(\mathbf{Z}/(p-1)\mathbf{Z})^*$  и  $(\mathbf{Z}/(q-1)\mathbf{Z})^*$ .

В данной модели множество допустимых атак является неразрешимым. Действительно, для симметричного шифра (например, DES, ГОСТ 28147–89, RIJNDAEL) на практике невозможно доказать, что не существует атаки (алгоритма вскрытия ключа), сложность которой меньше заданного уровня. Это обстоятельство затрудняет формализацию процедуры оценки безопасности системы.

Для криптографии характерно использование таких моделей возможностей нарушителя. Методы криптографии основаны не на теории предикатов, а на теории сложности, алгебре, криптоанализе, вычислительной математике.

### **3.3. Модель с лабораторными возможностями**

Эта модель отличается от модели из примера 3.2 тем, что нарушитель может использовать лабораторные методы для получения информации о секретных данных, обрабатываемых в системе. Поскольку безопасность для этой модели зависит от аппаратного построения средств защиты информации, управляющая программа не может контролировать безопасность — работоспособность аппаратуры не означает, что стойкость к лабораторным методам исследований со временем не снизилась (и даже что эта стойкость изначально была достаточной).

Для этой модели основная теорема безопасности также неверна. Действительно, в процессе перехода системы из состояния в состояние возникают сигналы, несущие информацию о секрете. Для приема таких сигналов может использоваться техника выделения сигналов из шума, позволяющая принять сигнал и получить информацию о секрете, если число повторов достаточно велико. При этом может возникнуть ситуация, что одиночный переход безопасен (сигнал слабее шума), но несколько таких переходов могут не являться безопасными.

В рамках данной модели персональный компьютер с установленными сколь угодно сложными криптографическими программными средствами и произвольной управляющей программой не может гарантировать безопасность. Изучением методов защиты информации в условиях такой модели занимается теория и техника связи и техническая физика.

## **4. Заключение**

Получены ответы на вопросы, поставленные в начале статьи. По первому вопросу: основная теорема безопасности верна только в случае вырожденной модели возможностей нарушителя. Существуют модели возможностей нарушителя и информационные системы, для которых основная теорема безопасности неверна.

Ответ на второй вопрос можно сформулировать следующим образом. Криптография — математическая дисциплина, которая изучает вопросы защиты информации от несанкционированного доступа и несанкционированного воздействия в рамках исчисления атак, порожденных невырожден-

денной моделью нарушителя с вычислительными, математическими и криптоаналитическими возможностями. При этом атаки, выводимые в рамках заданной модели возможностей нарушителя, можно охарактеризовать временной и емкостной сложностью; множество атак не является разрешимым. Безопасность криптографических средств защиты информации основана на сложности решения математической задачи. Методы криптографии используют аппарат алгебры, теории сложности, криптоанализа, а также областей математики, к которой относится указанная математическая задача.

Для построения защищенной информационной системы наряду с криптографией и теорией предикатов необходимо использовать методы технической физики, теории и техники связи.

Средства защиты информации часто используют физические или криптографические механизмы. Если два варианта выполняют одну и ту же защитную функцию, возникает вопрос: какой из них нарушителю труднее преодолеть? Криптографический подход позволяет линейно упорядочить способы защиты по сложности наилучших известных алгоритмов преодоления защиты. Такое упорядочение позволяет сравнивать варианты защиты и выбирать наилучший. Другие подходы обычно этого не допускают. Например, на вопрос, какой из способов опознавания пользователя — по сетчатке глаза и по отпечаткам пальцев — сложнее преодолеть, нет неоспоримо однозначного ответа.

Преимуществами криптографических средств защиты информации по сравнению с другими являются:

- эквивалентность или сводимость угрозы к математической задаче, что позволяет доказать безопасность информационной системы при условии, что указанная задача является сложной;
- возможность прогнозирования безопасности информационной системы;
- возможность сравнения однотипных средств защиты информации, обеспечивающих защиту от одних и тех же угроз, и выбора наилучшего варианта.

## Литература

1. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии. — М., Гелиос АРВ, 2001.
2. Манин Ю. И. Доказуемое и недоказуемое. (Кибернетика). — М.: Сов. Радио, 1979.
3. Оков И. Н. Криптографические системы защиты информации. — СПб.: ВУС, 2001.
4. Ростовцев А. Г., Маховенко Е. Б. Введение в криптографию с открытым ключом. — СПб.: Мир и Семья, Интерлайн, 2001.
5. Теория и практика обеспечения информационной безопасности. Под ред. П. Д. Зегжды. — М., Изд-во Агентства «Яхтсмен», 1996.

6. Успенский В. А., Семенов А. Л. Теория алгоритмов: основные открытия и приложения. — М.: Наука, 1987.
7. Bell D., LaPadula L. Secure Computer System: A mathematical model, ESD-TR-73-278, v. II, MITRE Corporation.
8. Blum L., Blum M., Shub M. A simple unpredictable pseudo-random number generator // SIAM Journal on Computing, v. 15, 1986, pp. 364–383.
9. Kahn D. The codebreakers. — Sphere books ltd, London, 1973.
10. Koblitz N. A Course in Number Theory and Cryptography. — Springer-Verlag, 1987.
11. Konheim A. Cryptography. A Primer. — J. Wiley & Sons, New York, 1981.
12. Menezes A., Oorschot P. van, Vanstone S. Handbook of applied cryptography. — CRC Press, 1997.