

Исчислительный подход к анализу безопасности

Предлагается исчислительный подход к анализу безопасности, при котором атаки определяются исчислением, порожденным множеством возможностей нарушителя. Показано, что модели нарушителя образуют решетку, индуцирующую упорядоченность подсистем безопасности. Каждая информационная система имеет максимальную модель нарушителя, для которой она безопасна. Каждая модель нарушителя определяет минимальную подсистему безопасности. Рассмотрена иерархия моделей нарушителя. Установлена эквивалентность тривиальной модели нарушителя, теоремы безопасности Белла — Лападулы и аксиомы транзитивности. Показано, что отдельный анализ безопасности криптографических средств и управляющих программ в компьютерных системах не может считаться корректным.

Makhovenko E.B., Rostovtsev A.G.,
SPbSPU

Calculus approach to security analysis

Calculus approach to security analysis is presented, where attacks are the results of calculus, which generation rules are determined by the set of intruder's possibilities. It is proved that intruder models form a lattice, that induce ordering of security system sets. Each information system has maximal intruder model, under which it is secure. Each intruder model defines minimal security system. Intruder model hierarchy is considered. It is proved that trivial intruder model, Bell — LaPadula security theorem and transitivity axiom are equivalent. It is shown that separate analysis of cryptographic apparatus and operating programs is not correct for computer systems.

1. Введение

Целью данной статьи является критика подходов, использующих отдельный анализ безопасности криптографических средств защиты информации и управляющих программ, и попытка обосновать необходимость совместного их анализа в рамках синтетического подхода.

В настоящее время существуют два подхода к определению безопасности информационных систем. Первый подход можно назвать *сложностным*: разбиение множества систем на безопасные и небезопасные производится на основе сложности алгоритма, нарушающего информационную безопасность.¹ Этот подход используется при анализе в первую очередь криптографических средств защиты информации.

Достоинствами этого подхода являются возможность описания множества атак по отношению к «продвинутому» нарушителю, в совершенстве владеющему математикой, криптоанализом, знающему алгоритмы работы системы, обладающему не только техническими средствами прослушивания и информационного воздействия на систему, но и соответствующим лабораторным оборудованием.

Недостатком этого подхода является его высокая сложность, а также высокая научная (в том числе математическая, криптографическая, инженерно-физическая, тех-

¹ Сюда же относятся и теоретико-информационный подход, основанный на оценке объема информации, который нарушитель может получить об обрабатываемой информации.

ническая) квалификация, требуемая от экспертов, исследующих безопасность. Эти знания добываются большим трудом и широко не разглашаются — по сути, они являются аналогом оружия. Это влечет за собой ряд негативных последствий. С одной стороны, поскольку квалификация разработчиков в указанных областях обычно ниже, чем квалификация профессионалов-экспертов, то зачастую разработанные подсистемы защиты информации по результатам анализа оказываются нестойкими. Это снижает производительность труда разработчиков. С другой стороны, такая ситуация создает предпосылки для волонтаризма в оценках безопасности — эксперт по своему усмотрению может давать положительное или отрицательное заключение для исследуемой системы.

Второй подход можно назвать *предикатным*: понятие безопасной системы абсолютно. Однако, как показано ниже, такая простота достигается упрощением модели возможностей нарушителя. Этот подход используется в основном для анализа управляющих программ. Достоинством этого подхода является его открытость и прозрачность, при этом анализ безопасности управляющей программы сводится к механической проверке заданных условий и может быть автоматизирован. Недостатком этого подхода, как показано ниже, является то, что он не гарантирует безопасность информационной системы.

2. Определения безопасности информационной системы

Согласно закону об информатизации и защите информации информационная система представляет собой организационно упорядоченную совокупность документов (массивов документов) и информационных технологий, в том числе, с использованием средств вычислительной техники и связи, реализующих процессы сбора, обработки, накопления, хранения, поиска и распространения информации.

Цель создания безопасной (или защищенной) информационной системы может быть достигнута лишь в том случае, если дать четкое определение цели и задач, решаемых на пути к ней. Разные авторы определяют безопасность информационных систем почти одинаково, однако дальнейшее введение вспомогательных определений приводит к взаимоисключающим выводам.

Например, согласно работе [2] «защищенная информационная система для определенных условий эксплуатации обеспечивает безопасность (конфиденциальность и целостность) обрабатываемой информации и поддерживает свою работоспособность в условиях воздействия на нее заданного множества угроз». Там же отмечается, что «защищенность является качественной характеристикой системы, ее нельзя измерить в каких-либо единицах, более того, нельзя даже с однозначным результатом сравнивать уровень защиты двух систем — одна будет лучше обеспечивать безопасность обрабатываемой информации в одном случае, другая — в другом».

Согласно работе И. Н. Окова [5] под безопасностью информации понимается состояние ее защищенности, при котором с требуемой вероятностью обеспечивается защита информации, информационных ресурсов и информационных систем от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т. п.

Согласно работе Белла и Лападулы [9] информационная система называется безопасной по чтению (по записи) тогда и только тогда, когда полномочия субъекта по чтению (по записи) соответствуют уровню секретности информации. Информационная система называется безопасной тогда и только тогда, когда она безопасна в этом смысле по чтению и по записи. Из этих определений Белл и Лападула вывели теорему.

Предложение 1 (основная теорема безопасности Белла — Лападулы). Если начальное состояние информационной системы безопасно и переход из состояния в состояние безопасен, то все состояния системы безопасны.

Эта теорема позволяет рассматривать не всю совокупность состояний информационной системы, а только начальное состояние и разрешенные переходы, открывая этим путь к автоматическому доказательству безопасности.

Согласно [5] защищаемая информация может подвергаться различным воздействиям со стороны нарушителя или сил природы. Пути реализации воздействий на информацию называются *угрозами*.

Безопасностью информационной системы называется ее свойство противостоять угрозам со стороны нарушителя. Угрозы безопасности реализуются в виде *атак*. Поскольку любая атака реализуется некоторым алгоритмом, а алгоритм характеризуется сложностью в рамках заданной вычислительной модели, можно определить безопасность информационной системы. Свойство безопасности характеризуется тем, что в рамках заданной модели нарушителя не существуют или не известны атаки, сложность которых превышает пороговую.

Совокупность всевозможных действий нарушителя (атак) определяется его возможностями. Модель нарушителя определяется множеством его возможностей, которые позволяют (но не предписывают) нарушителю действовать так или иначе для достижения своей цели.

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 [4]. Модель нарушителя задает правила вывода исчисления, а результатом исчисления является множество атак. Модель нарушителя в рамках формальной логики является аналогом системы аксиом некоторой теории, а совокупность всевозможных реализуемых атак — аналогом множества истинных или доказуемо истинных утверждений этой теории.

Согласно результатам Геделя, Тарского, Поста, Смаллиана и ряда других логиков [3, 7, 8], множества истинных утверждений и доказуемо истинных утверждений не совпадают: существует истинное утверждение, которое невозможно доказать (а также опровергнуть, поскольку доказательный аппарат считается непротиворечивым). Аналогично существует ложное утверждение, для которого невозможно доказать его ложность (а также истинность, поскольку аппарат доказательства непротиворечив). При этом каждое утверждение является либо истинным, либо ложным.

Назовем информационную систему *доказуемо безопасной*, если существует доказательство того, что ни одна атака, нарушающая безопасность, не может быть реализована в рамках данного исчисления. Назовем информационную систему *доказуемо уязвимой*, если в рамках данного исчисления существует вывод для данной атаки, нарушающей безопасность.

Назовем информационную систему *безопасной*, если ни одна атака, нарушающая безопасность, не может быть реализована в рамках данного исчисления. Назовем информационную систему *уязвимой*, если в рамках данного исчисления существует атака, нарушающая безопасность. Согласно [3, 7, 8] множества безопасных и доказуемо безопасных систем, а также уязвимых и доказуемо уязвимых систем различны.

3. Упорядоченность моделей нарушителя и безопасных систем

Предположим, есть две модели нарушителя, причем вторая как множество возможностей содержит в себе первую. Тогда можно сказать, что вторая модель является более сильной, чем первая, или просто больше первой, у соответствующего нарушителя больше возможностей, а множество атак для второй модели включает в себя множество атак для первой модели. Таким образом, на множестве моделей нарушителя определена *частичная упорядоченность*, заданная упорядоченностью множеств по включению, и индуцирующая *упорядоченность множества атак*.

Упорядоченность моделей нарушителя также индуцирует *упорядоченность безопасных информационных систем*. Система, безопасная по отношению к нарушителю, описываемому меньшей моделью, может не быть безопасной по отношению к нарушителю, описываемому большей моделью. Таким образом, понятие безопасности информационной системы подразумевает указание соответствующей модели нарушителя.

Зададим модель нарушителя (градуированным) множеством, элементы которого могут сопровождаться численными значениями, характеризующими возможности нарушителя. Например, если нарушитель обладает вычислительными возможностями, то они могут варьироваться. Назовем модели нарушителя *однотипными*, если они состоят из одинаковых элементов с точностью до их численных значений. На однотипных множествах можно установить отношение порядка, например, упорядочив список возможностей по типам, а затем упорядочив возможности одного и того же типа по их количественным характеристикам.

Предложение 2. Модели нарушителя образуют решетку.

Доказательство. Два неградуированных множества, задающих модель нарушителя, имеют точную верхнюю грань (объединение этих множеств) и точную нижнюю грань (пересечение этих множеств). Два однотипных множества также образуют решетку, в которой точной верхней гранью является более сильная модель, а точной нижней гранью — более слабая модель. Композиция этих двух отношений порядка задает решетку на множестве моделей нарушителя. ■

Предложение 3. Для каждой информационной системы существует (может быть, не единственная) *максимальная модель нарушителя*, для которой система безопасна.

Доказательство. Множество A моделей нарушителя, для которых система безопасна, непусто, так как содержит пустое множество возможностей. Для каждой пары элементов множества A находим точную верхнюю грань и из найденного множества точных верхних граней выбираем наибольшие, содержащиеся среди элементов множества A . Построенное непустое множество точных верхних граней является искомым. ■

На практике защита информации в информационной системе осуществляется подсистемой безопасности. Если безопасность информационной системы может быть обеспечена, то обычно этого можно достичь с помощью различных подсистем безопасности. На множестве подсистем безопасности можно определить отношение частичного порядка. Упорядоченность может задаваться стоимостью, массо-габаритными показателями, номенклатурой используемых средств и т. п.

Легко показать, что всякое упорядоченное множество M содержит не более одного элемента a , удовлетворяющего неравенству $a \leq x$ для всех элементов x из M . Такой элемент, если он существует, называется *наименьшим* элементом; двойственный к нему

элемент упорядоченного множества, если он существует, называется *наибольшим* элементом. Элемент a упорядоченного множества M называется *минимальным*, если неравенство $x < a$ невозможно ни для какого $x \in M$. Двойственно определяется *максимальный* элемент.

Согласно [1] конечное упорядоченное множество содержит хотя бы один минимальный и хотя бы один максимальный элемент. Из этого результата следует

Предложение 4. Среди подсистем безопасности, обеспечивающих защиту по отношению к заданной модели нарушителя, существует *минимальная*.

Таким образом, множество информационных систем можно разбить на классы так, что к одному классу относятся информационные системы, для которых максимальные модели нарушителя совпадают.

При построении и анализе безопасности защищенных информационных систем часто требуется решить три задачи. Первая задача: для заданной модели нарушителя определить, является ли данная информационная система безопасной (существует доказательство безопасности), является ли она небезопасной (существует доказательство уязвимости системы) или неопределенной (отсутствуют доказательства как безопасности, так и уязвимости).² Вторая задача: для заданной информационной системы найти максимальную модель нарушителя. Третья задача: для заданной модели нарушителя найти минимальную подсистему безопасности.

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 [11].

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 и лабораторные 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 обращая установленным порядком к области памяти, где эти данные хранятся. В процессе обработки секретной информации с помощью материальных средств возникают физические поля, которые 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.

² Множество систем можно разбить на два непересекающихся множества: безопасных и небезопасных (уязвимых). В множестве безопасных систем может существовать собственное подмножество доказуемо безопасных систем. Тогда дополнение этого подмножества в указанном множестве соответствует недоказуемо безопасным системам. Аналогично, в множестве уязвимых систем может существовать собственное подмножество доказуемо уязвимых систем и его дополнение.

Математические возможности нарушителя позволяют ему разрабатывать новые эффективные методы и алгоритмы решения массовых математических задач, положенных в основу безопасности.

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.

4. Тривиальная модель нарушителя и предикатный подход

Назовем модель нарушителя *тривиальной*, 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.³

Данная возможность может считаться технической, если информационная 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 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.⁴

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 (БЛП-безопасной) тогда и только тогда, когда она безопасна в этом смысле по чтению и по записи (это определение удобно считать аксиомой безопасности). Известна *основная теорема*

³ Эта модель названа тривиальной потому, что она, по-видимому, является самой слабой среди непустых моделей возможностей нарушителя. Как показывает практика, нарушитель часто использует значительно более широкий арсенал возможностей для того, чтобы узнать секрет.

⁴ Вместо модели Белла — Лападулы можно рассмотреть любую другую мандатную модель управления доступом.

безопасности Белла — Лападулы: если начальное состояние системы безопасно и каждый переход из предыдущего состояния в последующее состояние безопасен, то система безопасна (всюду имеется в виду БЛП-безопасность). Таким образом, дополнением множества безопасных систем является множество уязвимых систем.

Тривиальная 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 тривиальной моделью.

Предложение 5. Все атаки исчисления, порожденного тривиальной 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 [3], 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. ■

Назовем информационную систему *транзитивной*, если для любой цепочки переходов $a_1 \rightarrow a_2 \rightarrow \dots \rightarrow a_n$ из безопасности каждого отдельного перехода следует безопасность результирующего перехода $a_1 \rightarrow a_n$. Основная теорема безопасности БЛП утверждает, что транзитивность следует из БЛП-безопасности. Рассмотрим зависимость между аксиомой тривиальности модели нарушителя, аксиомой БЛП и аксиомой транзитивности.

Предложение 6. Справедливы следующие утверждения.

1. Аксиома безопасности БЛП и аксиома тривиальности эквивалентны.
2. Любая из аксиом БЛП и тривиальности влечет аксиому транзитивности.

Доказательство. Из аксиомы тривиальности следует аксиома безопасности БЛП, так как для нарушителя единственный способ нарушить конфиденциальность — выполнить операцию считывания, а единственный способ нарушить подлинность — выполнить операцию записи.

Из аксиомы безопасности БЛП следует аксиома тривиальности, так как никакие другие возможности нарушителя, кроме чтения и записи, не предусмотрены. Таким образом, каждая из аксиом БЛП-безопасности и тривиальности влечет другую.

Из аксиомы БЛП-безопасности согласно основной теореме безопасности БЛП следует аксиома транзитивности. В силу эквивалентности аксиом тривиальности и БЛП-безопасности, аксиома тривиальности также влечет аксиому транзитивности. ■

Следствие 7. Если аксиома транзитивности неверна, то ни аксиома тривиальности, ни аксиома БЛП-безопасности не выполняются.

5. Безопасность в случае нетривиальных возможностей нарушителя

Иногда 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 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.

Покажем, что для этой модели возможностей нарушителя основная теорема безопасности БЛП не выполняется.

Предложение 8. Существует информационная система, для которой не выполняется аксиома транзитивности при наличии у нарушителя математических возможностей.

Доказательство. 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 [6]. В качестве генератора случайных чисел выберем генератор BBS (Блюма — Блюма — Шуба) [10], формирующий периодическую псевдослучайную криптографически стойкую последовательность⁵. 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. ■

Следствие 9. Если нарушитель обладает математическими, вычислительными и криптоаналитическими возможностями, а в системе используются криптографические алгоритмы, основанные на вычислительной сложности, то не существует криптосистем, для которых аксиома транзитивности справедлива.

Доказательство. Практическая стойкость криптографических методов защиты информации непрерывно снижается и при неограниченно длительной эксплуатации системы стойкость станет недопустимо низкой [6]. ■

⁵Генератор 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, 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.

Рассмотрим случай лабораторных возможностей. 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 возникает ситуация, что одиночный переход безопасен (сигнал слабее шума), но несколько таких переходов могут не являться безопасными. Для любого опасного сигнала существует некоторое число n такое, что n и более повторов опасного сигнала позволяют выделить его из шума и вскрыть ключ.

В рамках данной модели нарушителя ни одна программа для персонального компьютера, использующего криптографические программные средства, не может гарантировать безопасность.

6. О раздельном анализе безопасности криптографических средств и управляющей программы.

На практике подсистема безопасности обычно использует криптографические средства защиты, стойкость которых основана на вычислительной сложности некоторой математической задачи. Анализ криптографических алгоритмов и протоколов и особенностей их реализации выполняется на основе сложностного подхода. Управляет работой информационной системы в целом (включая криптографические средства) управляющая программа. Безопасность управляющей программы обычно определяется на основе предикатного подхода.⁶

Рассмотрим подробнее свойства раздельного применения таких подходов.

Предложение 10. Пусть в информационной системе используются криптографические средства, предусмотренные стандартами шифрования и подписи. В данном наборе высказываний любое из них влечет два остальных:

1. Справедлива аксиома безопасности БЛП.
2. Модель возможностей нарушителя тривиальна.
3. Справедлива аксиома транзитивности.

Доказательство. Импликация $2 \rightarrow 1$ следует из того, что в аксиоме безопасности участвуют только возможности чтения и записи. Импликация $1 \rightarrow 3$ следует из доказательства теоремы БЛП. Импликация $3 \rightarrow 2$ эквивалентна импликации «не $2 \rightarrow$ не 3 ». Предположим, что возможности нарушителя нетривиальны и согласно классификации множество возможностей содержат математические или лабораторные возможности. Согласно изложенному выше эта импликация имеет место. ■

⁶ Предикатный подход определяет доказуемо стойкие системы, а сложностной — доказуемо уязвимые системы.

Таким образом, если в информационной системе используются криптографические средства, то три утверждения последней теоремы эквивалентны и любое из них может считаться аксиомой безопасности.

Следствие 11. Если модель нарушителя нетривиальна, а в системе используются стандартные алгоритмы шифрования и подписи, то аксиома транзитивности не выполняется и теорема Белла — Лападулы неверна.

Назовем средство криптографической защиты *транзитивно безопасным*, если оно удовлетворяет аксиоме транзитивности.

Предложение 12. Раздельные подходы к анализу безопасности корректны тогда и только тогда, когда криптографические средства являются транзитивно безопасными.

Доказательство. Предположим, что раздельный подход является корректным. Тогда криптографические средства должны удовлетворять аксиоме транзитивности, то есть быть транзитивно безопасными. Предположим, что криптографические средства транзитивно безопасны. Тогда они (и информационная система в целом) удовлетворяют аксиоме транзитивности, и управляющая программа может гарантировать безопасность системы. ■

В действительности ни одно криптографическое средство, использующее стандартные криптографические алгоритмы, не может быть транзитивно безопасным. В частности, выполнение определенного числа генерации подписи ведет к нарушению секретности ключа и обрушению безопасности системы в целом. То же справедливо и для шифров.

Существующий раздельный анализ безопасности управляющей программы и криптографических средств в рамках общей нетривиальной модели возможностей приводит к тому, что управляющая программа безопасна лишь постольку, поскольку она не может управлять криптографическими средствами, в частности не может вызывать криптографические программы и функции. Следовательно, должна быть дополнительные «управляющие программно-аппаратные средства», которые управляют совместно упомянутой управляющей программой и криптографическими средствами. Продолжение этой цепочки очевидно ведет в тупик.

Возможным выходом из создавшегося положения является использование криптографических средств ограниченной транзитивности: результирующий переход $a_1 \rightarrow a_2 \rightarrow \dots \rightarrow a_n$ безопасен при безопасности всех единичных переходов тогда и только тогда, когда число шагов не превышает порогового значения. Для продления безопасной эксплуатации необходимо сменить ключ или даже параметры криптосистемы.

Это ведет к тому, что основная теорема БЛП (и ее аналоги в случае мандатной модели управления доступом) справедлива лишь для ограниченного числа переходов.

Библиографический список

1. Биркгоф Г. Теория решеток. — М.: Наука, 1984.
2. Зегжда Д. П., Ивашко А. М. Как построить защищенную информационную систему / под ред. П. Д. Зегжды и В. В. Платонова. — СПб.: Мир и Семья, 1997.
3. Манин Ю. И. Доказуемое и недоказуемое. (Кибернетика). — М.: Сов. Радио, 1979.
4. Математический энциклопедический словарь. — М.: Сов. энциклопедия, 1988.

5. Оков И. Н. Криптографические системы защиты информации. — СПб.: ВУС, 2001.
6. Ростовцев А. Г., Маховенко Е. Б. Введение в криптографию с открытым ключом. — СПб.: Мир и Семья, Интерлайн, 2001.
7. Смаллиан Р.М. Принцесса или тигр? — М.: Мир, 1985.
8. Успенский В. А., Семенов А. Л. Теория алгоритмов: основные открытия и приложения. — М.: Наука, 1987.
9. Bell D., LaPadula L. Secure Computer System: A mathematical model, ESD-TR-73-278. V. II. MITRE Corporation.
10. Blum L., Blum M., Shub M. A simple unpredictable pseudo-random number generator // SIAM Journal on Computing. 1986. V. 15. P. 364–383.
11. Kahn D. The Codebreakers. — Sphere books Ltd, London, 1973.