гаемым методом этой базы работники банка получат численное значение надежности их решения, которое опирается на предыдущий опыт работы банка.

Отличием и преимуществом данного подхода от уже существующих состоит в том, что он опирается на информационные оценки и деревья решений, что достаточно просто для понимания и наглядно по сравнению с нейронными сетями, сетью связей (connectionist network) и т.д.

Таким образом, в данной работе рассмотрены сущность, подходы и этапы процесса моделирования данных, а также показана актуальность проблемы надежности хранящихся данных.

ТЕХНОЛОГИЯ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

И. Шешко
Белорусский государственный экономический университет

Наше поколение столкнулось с решением очень важной проблемы – обеспечением компьютерной безопасности. По выражению Платона, безопасность есть предотвращение зла, а борьба со злом – это вечная проблема. Именно поэтому в странах, где высок уровень компьютеризации, компьютерная преступность уже давно стала занимать один из самых важных и, к сожалению, нерешенный на данный момент, вопрос.

Дело в том, что компьютерная информация легко передается, копируется, блокируется или изменяется с огромной скоростью на значительном от нее расстоянии, что обусловлено самой природой компьютерной информации, которая может являться как носителем следов, так и следами совершения преступлений.

В наступившей эпохе всеобщей информатизации, приведшей к полной зависимости от средств электронной обработки данных, тема рисков зазвучала совершенно по-новому. Речь идет о риске потерять информацию. Именно поэтому возникла серьезная необходимость ограничивать круг лиц, для которых она предназначена. Так появилась криптография, которая является ровесницей письменности. Именно в наш век электронно-вычислительные машины позволили криптографии перейти из области искусства в область науки. Желающие защитить свои секреты получили для этого такие возможности, о которых не смели прежде и мечтать, а в распоряжении злоумышленников оказались невероятно хитрые приспособления для проникновения в чужие тайны. Баланс на поле информационной войны сохранился, но само противостояние продолжилось уже на новом витке развития – криптография приобрела второе дыхание.

Вследствие развития информационных технологий, и особенно с использованием Интернета, защита конфиденциальной информации стала одной из актуальнейших задач современности. Следует также отметить, что с течением времени характер криптографии постоянно изменяется, а задачи ее постоянно усложняются и расширяются. Так, в последнее время эта наука пополнилась такими задачами, которые не связаны напрямую с засекречиванием информации – разработка систем электронной цифровой подписи, протоколов выборов, под-

писания контрактов, а также появление методов, позволяющих избежать получения ложных сообщений, создание средств защиты систем электронных платежей.

В настоящее время применение криптографических алгоритмов для закрытия информации уже не является особо сложной задачей. В процессе компьютерной обработки информация может подвергаться шифрованию несколько раз, причем не всегда с ведома создателя или потребителя этой информации. Однако до сих пор существует вероятность несанкционированного просмотра информации, обусловленная определенными недостатками алгоритмов шифрования.

Криптосистема работает по определенной методологии (процедуре) и состоит из одного или более алгоритмов шифрования (математических формул); ключей, используемых этими алгоритмами шифрования; системы управления ключами; незашифрованного текста и зашифрованного текста (шифротекста).

Согласно методологии, сначала к тексту применяются алгоритм шифрования и ключ для получения из него шифротекста, который затем передается к месту назначения, где тот же самый алгоритм используется для его расшифровки, чтобы получить снова текст. Также в методологию входят процедуры создания ключей и их распространения.

Какие же требования предъявляются сегодня к криптографическим алгоритмам? Надежность, устойчивость к попыткам взлома – это главное, чего ждут от нового шифра. Однако все, что человек закрыл, человеком может быть и открыто. Таким образом, никто и никогда не дает 100 %-ю гарантию, что информация не попадет в чужие руки. Если даже для вскрытия шифра теоретически требуются миллионы лет, всегда есть вероятность, что его взломают за час.

Последствия компьютерных преступлений лежат в диапазоне от назойливых помех до катастроф. Акция шпионажа, совершаемая с помощью компьютера, для национальной безопасности может принести огромный ущерб. Проделки взломщиков могут быть безобидными, а могут вызвать серьезные нарушения, влияющие на деятельность фирмы. Одни компьютерные преступления совершаются для удовольствия, другие – имеют социальные или политические причины, а третьи – являются бизнесом профессиональных преступников.

Анализ вышеизложенного материала дает возможность назвать следующие причины уязвимости многих проектов:

– отсутствие четких и ясных определений предмета и объекта защиты, а также возможных потенциальных угроз предмету и объекту защиты;

– различие в понимании целей и задач безопасности информации разработчиками системы и ее элементов.

Эти обстоятельства являются также причиной того, что имеющиеся на сегодняшний день стандарты по безопасности информации неполны, противоречивы и не отражают действительную картину возможных событий.

Изложенное выше позволяет надеяться на то, что в пределах развивающейся информации нашего общества будет внесен вклад в решение проблемы уровня безопасности информации в автоматизированных системах, ее хранения, обработки и передачи.

В заключение необходимо отметить, что каждый из способов реализации криптографических средств защиты информации обладает как достоинствами, так и недостатками. Выбор определяется поставленными задачами с учетом особенностей реализации, эксплуатации и финансовых возможностей, при этом необходимо принимать во внимание используемые аппаратные средства, необходимую степень защиты информации. Недостатком является то, что на пути реализации эффективной защиты информации существует множество технологических трудностей. Но соответствующие аппаратно-программные средства стремительно развиваются, что позволяет рассчитывать на появление новых решений, которые будут лишены существующих недостатков.

Ситуация складывается так, что в недалеком будущем знакомство с криптографией потребуется каждому пользователю электронных средств обмена информацией. Поэтому вскоре криптография станет «третьей грамотностью» – по аналогии со «второй грамотностью», как называют владение компьютером и информационными технологиями.