Оценка рисков доверия к кибербезопасности компьютеризированных систем

А. А. Кононов

При использовании любой компьютеризированной системы (КС) пользователь, доверяя этой системе, полагается на безопасность ее компьютерных компонентов, т. е. на кибербезопасность КС. Задача состоит в том, чтобы оценить риски из-за возможной недостаточной кибербезопасности КС. Назовем эти риски рисками доверия.

Итак, **риски доверия** — это те риски, которые объективно существуют для пользователя, если он полагается на недостаточно надежную, недостаточно защищенную и, в итоге, недостаточно безопасную для пользователей КС.

Основной технологической составляющей любой КС является автоматизированная информационная система (АИС).

Современные подходы к созданию безопасных АИС [1–3] предполагают, что для того, чтобы на безопасность АИС можно было положиться, должны быть построены модели угроз АИС, модели защиты, оценены риски нарушения безопасности, приняты меры по обеспечению безопасности, приобретены и внедрены необходимые средства обеспечения безопасности. При этом на всех этапах создания и эксплуатации АИС существуют системы требований, которые должны выполняться, для того чтобы безопасности АИС можно было бы доверять. При этом требования предъявляются как к АИС в целом, так и каждой из ее структур, к отдельным компонентам, а также к технологическим и бизнес-процессам и точкам этих процессов (рис. 1).

Система требований должна быть настолько полна, чтобы ее выполнение позволяло полностью парировать все чреватые существенными рисками угрозы. Только в этом случае можно будет мерить уровень доверия к безопасности используемой системы уровнем выполнения требований.

Применительно к проблемам безопасности АИС принято использовать термин — «информационная безопасность». При выполнении системы требований информационной безопасности (ИБ) могут возникнуть следующие проблемы:

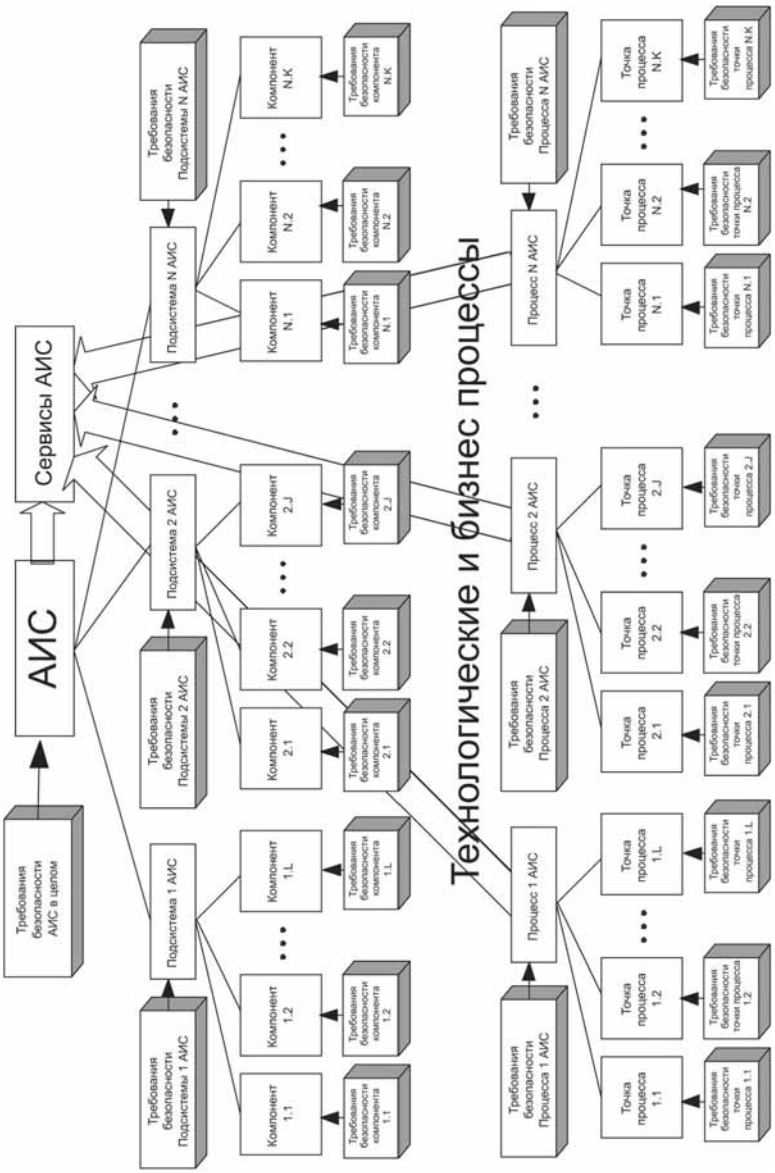

Рис. 1. Распределение требований безопасности по структурным составляющим, технологическим и бизнес-процессам АИС

- исполнение всех возможных требований по обеспечению ИБ может быть невозможно из-за слишком высокой стоимости их реализации;
- требования по безопасности могут не выполняться из-за отсутствия достаточно эффективного контроля за выполнением требований;
- требования могут не выполняться, поскольку они плохо усвоены исполнителями.

Во всех трех перечисленных случаях контроль за выполнением требований может дать большой положительный эффект.

Если часть требований не может быть реализована из-за недостатка средств на их реализацию, контроль должен позволить не упускать из вида существующие проблемы и решать их по мере появления средств на повышение ИБ с учетом показателей важности решения указанных проблем.

При отсутствии эффективного контроля за выполнением требований со стороны исполнителей могут проявляться тенденции оптимизировать свою работу за счет игнорирования требований по безопасности. Поэтому постоянный контроль за выполнением требований помимо прочего призван внушить исполнителям важность выполнения требований.

В системах, где организован всеобъемлющий контроль всех требований, как правило, помимо огромного числа инструкций, приказов, законодательных и подзаконных актов, в которых формулируются требования, составляются списки требований по подконтрольным структурам и процессам. Наличие такого рода списков позволяет как контролерам, так и исполнителям быстрее вникать во всю систему требований, быстрее ее осваивать и, соответственно, лучше их исполнять

Очевидно, что эффективный контроль за выполнением большого числа требований, отнесенным к большому количеству компонентов, процессов и исполнителей, невозможен без измеряемых характеристик и показателей, которые позволили бы судить о реальных уровнях выполнения требований по структурным подразделениям, по процессам обработки и хранения информации, выявлять наиболее проблемные («узкие») места и возможные источники наибольших проблем с обеспечением ИБ.

При этом очевидно, что возможности количественной оценки выполнения требований с учетом всех существующих взаимосвязей между отдельными требованиями, между отдельными структурными частями организации, между всеми процессами и точками этих процессов в реальной ситуации крайне ограничены. Единственно возможным практически реализуемым способом контроля ситуации с выполнением требований может стать использование индексных показателей (индексов).

Классическое определение индексов принадлежит Ф. Эджворту: «Я предлагаю определить индексное число как число, приспособленное для того, чтобы своими вариациями указывать увеличение или уменьшение величины, не допускающей точного измерения» [2].

Применительно к оценке рисков в информационных системах можно утверждать, что практически все рассчитываемые показатели этих оценок являются, по сути, индексами, каждый из которых, как правило, обладает своими достоинствами и недостатками.

В этой работе в качестве показателя оценки рисков предложен индексный показатель (индекс) оценки рисков, вытекающих из невыполнения требований, названный «оценкой рисков доверия».

Ниже представлена логика построения этого индекса, которую следует иметь в виду при практической оценке рисков доверия для большей корректности получаемых результатов.

Пусть значение показателя риска пользователя определяется по 100-балльной (процентной) шкале. Стопроцентный риск будет означать, что пользователь, доверяя АИС, за год теряет 100 процентов своей собственности, зависящей от результатов работы АИС.

Предположим, что для обеспечения безопасности АИС должно быть выполнено **одно** требование. Пусть возможно только два состояния — «выполнено» и «не выполнено». Таким образом, оценка выполнения требования о корректном функционировании системы будет иметь одно из двух значений — «система функционирует корректно» или «система функционирует некорректно».

Тогда, если требование выполнено, и АИС функционирует корректно, то риск пользователя будет нулевым. Если не выполнено — то риск будет 100-процентным и пользователь все потеряет.

Усложним задачу. Предположим, что оценка выполнения требования безопасности определяется по шкале от 0 до 100 процентов и возможна некоторая интегральная оценка возможного ущерба, учитывающая как размер ущерба в случае невыполнения требования, так и вероятность его нанесения. Назовем эту оценку ожидаемым процентом потерь собственности, зависящей от АИС. Тогда процент выполнения требования будет определять ожидаемый процент потерь собственности, зависящей от АИС.

Обозначим через q процент выполнения требования.

Ожидаемый процент потерь собственности, зависящей от АИС, по сути представляющий собой риск доверия (r) пользователя, в этом случае определяется по формуле:

$$r = 100 - q\,. \qquad (1)$$

Далее положим, что количество требований безопасности системы более чем одно. Обозначим количество таких требований через I. Тогда, если предположить что значимость выполнения каждого требования одинакова, а степень q_i выполнения каждого требования можно оценить в диапазоне от 0 до 100 процентов, то риск доверия к безопасности такой

системы будет оцениваться как среднее арифметическое значение степени невыполнения указанных требований:

$$r = \frac{\sum_{i=1}^{I}(100 - q_i)}{100 \times I}. \quad (2)$$

Далее предположим, что с каждым требованием связан такой интегральный показатель, как вес требования (w_i), учитывающий как относительную вероятность нанесения ущерба из-за невыполнения требования, так и относительную величину этого ущерба. Пусть значение w_i также определяется по шкале от 0 до 100.

Таким образом, задавая вес w_i, можно определить, в какой степени при оценке риска доверия к безопасности должно учитываться выполнение этого требования. Тогда формула расчета риска доверия принимает следующий вид:

$$r = \sum_{i=1}^{I} \frac{w_i}{\sum_{i=1}^{I} w_i} \times (100 - q_i). \quad (3)$$

Будем называть значимостью требования величину z_i, рассчитываемую по формуле:

$$z_i = \frac{w_i}{\sum_{i=1}^{I} w_i}. \quad (4)$$

Тогда формулу (3) расчета риска доверия можно переписать в виде:

$$r = \sum_{i=1}^{I} z_i \times (100 - q_i). \quad (5)$$

Предположим теперь, что риск доверия к безопасности системы зависит не от одного объекта, а от J объектов, для каждого из которых риск доверия был рассчитан по формуле (5). Тогда, если значимость объектов одинакова, то риск доверия к безопасности системы R рассчитывается по формуле:

$$R = \frac{\sum_{j=1}^{J} r_j}{100 \times J}. \quad (6)$$

Если по объектам были определены значимости, задающие степень влияния оценок рисков по составляющим на степень риска по системе в целом, то формула (6) должна принять следующий вид:

$$R = \sum_{j=1}^{J} r_j \times z_j . \qquad (7)$$

Приведенную логику рассуждений можно обобщить на случай многоуровневой иерархической системы. Тогда, пользуясь формулой (7), можно рассчитать оценку риска доверия к каждому следующему иерархического уровню, исходя из знания оценок рисков доверия к безопасности всех его структурных составляющих.

Таким образом, определив требования безопасности ко всем объектам, составляющим систему, оценив их выполнение, а так же определив значимости влияния оценок выполнения отдельных требований и оценок рисков по отдельным структурным составляющим, можно оценивать уровни доверия к безопасности системы любой иерархической сложности.

В качестве комментариев к применению данной методики можно дать следующие замечания:

1. Очевидно, что требования по доверию к безопасности могут быть отнесены не только к самому нижнему уровню объектов, но и к любой структурной составляющей более высокого иерархического уровня. В таких случаях при применении этой методики следует определить виртуальные иерархические структуры и виртуальные объекты, которые позволят отразить и учесть требования к безопасности структурных составляющих более высокого, чем объекты уровня.
2. В методике нет разделения требований на функциональные требования к безопасности и на требования обеспечения доказательств полноты и выполнения функциональных требований. Но при оценке уровня доверия к безопасности наличие таких требований обязательно и это должно учитываться пользователями этой методики при построении систем требований и при их оценке. Поэтому при построении системы требований для использования этой методики рекомендуется ориентироваться на подход обеспечения доверия, заложенный в [5].
3. Методика не содержит учета возможных субъективных ошибок и вероятной «размытости» оценок, которые могут иметь место:
   а) при определении перечня объектов, от которых зависит безопасность системы;
   б) при составлении наборов требований, обеспечивающих доверие к безопасности каждого из объектов;

в) при оценках выполнения требований;
г) при учете степени доказанности выполнения требований.

Поэтому указанную методику рекомендуется применять только вместе с методом дельфийских групп, возможно в его распределенном варианте, когда изначально тем или иным образом построенные системы объектов и требований к их безопасности представляются в виде ясных и понятных форм, по которым привлеченные к работе специалисты и эксперты вносят свои замечания и предложения. В ходе итеративных процедур учета этих предложений и замечаний формируется некоторое консолидированное мнение по всем вопросам.

В то же время, можно отметить, хотя предложенная комбинация этой методики с концепцией дельфийских групп на сегодня является наименее затратной при ее использовании и, как правило, полностью удовлетворяет пользователей этой методики, в то же время, указанные в этом пункте ограничения, определяют и возможные дальнейшие пути развития этой методики на пути использования теории нечетких множеств.

4. Одним из важнейших недостатков, который имеет место в указанной методике, является то, что в ней полностью игнорируются взаимосвязи между требованиями. Самое главное, что при этом может быть не учтено, что некоторые сочетания невыполненных требований могут фактически означать полную незащищенность объектов АИС, от какого-либо класса угроз.

   Решение этой проблемы возможно при автоматизации использования этой методики. Она должна быть в обязательном порядке дополнена системой идентификации опасных сочетаний невыполненных требований, факт обнаружения которых будет означать полную незащищенность системы от каких-либо угроз.

5. Предлагаемый индекс не позволяет учесть масштаб проблем безопасности. Он дает возможность получить качественную оценку по обеспечению выполнения требований по безопасности без учета сложности обеспечения этой безопасности в каждом конкретном случае. Так, если к примеру существуют две структуры одного иерархического уровня — одна, состоящая из одного объекта, другая, скажем, из 100 объектов, и для всех объектов как первой, так и второй структур будет не выполнено одно и то же требование, то оценка риска по обеим структурам будет одной и той же.

В то же время при всех перечисленных недостатках следует отметить, что расчет предлагаемого индекса дает возможность решать такие задачи контроля выполнения требований, как выявление «узких» мест, отслеживание динамики изменения ситуации с выполнением требований, выявление

наиболее проблематичных с точки зрения выполнения требований классов объектов, точек технологических процессов и отдельных требований.

Более того, при решении указанных задач в инфраструктурах большого (национального и транснационального масштаба), это практически единственный существующий на сегодняшний день метод, который позволяет контролировать состояние их кибербезопасности во всем диапазоне огромного числа требований безопасности, разнесенным по неограниченному множеству объектов и процессов.

Литература

1. *Кононов А. А.*, *Поликарпов А. К.* Обеспечение безопасности информации: задачи и решения // Информационная безопасность. 2005. № 5.
2. *Кононов А. А.*, *Поликарпов А. К.* Обеспечение гарантированной защиты информации в компьютерных системах // Науч.-техн. информ. Сер. 1. 2006. № 4. С. 42–43.
3. BS ISO/IEC 27001:2005 RU. Информационные технологии — Методы обеспечения безопасности — Системы управления информационной безопасностью — Требования. Британский стандарт. М.: ООО «GlobalTrust Solutions», 2006.
4. *Edgeworth F. Y.* The plurality of index numbers. Economic Journal, 1925, Vol. 35. P. 379.
5. ГОСТ Р ИСО/МЭК 15408. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 3. Требования доверия к безопасности. М.: Госстандарт России, 2002.