ИНФОРМАТИКА

2008 **октябрь-декабрь** **№ 4**

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 681.324.067

В.В. Анищенко, Е.А. Цынкевич

ФОРМАЛИЗАЦИЯ ОЦЕНКИ РИСКОВ В ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ

Рассматривается формальный подход к оценке рисков в информационных технологиях, связанных с их основными особенностями. Вводятся формализованные определения риска, угрозы и ее составляющих, компонентов информационной технологии, факторов, влияющих на наличие и проявление угроз. Наряду с определениями данных понятий вводятся элементы их классификации. На простом примере показывается невозможность гарантированной минимизации риска проявления угрозы класса $P_w^i(P_d^i)$ *для компонентов, относящихся к классу* C_3^∞, *и как следствие формулируется основная теорема риска, обобщающая полученный результат для классов* C_y^∞ *и* C_∞^∞. *Демонстрируется возможность построения формальных моделей оценки рисков, основанных на использовании в качестве элементной базы предложенных определений.*

Введение

Развитие и распространение информационных технологий сопровождается ростом правонарушений, связанных со злоупотреблением, модификацией и неправомочным доступом к данным и обрабатываемым их программам и как следствие возрастанием риска их использования. Поэтому с учетом неизбежности перехода цивилизации к информационному обществу требуется проведение комплекса мероприятий, включающих разработку специальных средств защиты и методические исследования в области проведения сертификационных испытаний средств защиты, которые используются в автоматизированных системах обработки информации [1]. В свою очередь, это предполагает наличие формальных моделей оценки рисков, обеспечивающих максимальную объективность их практического применения в процессе определения эффективности проводимых мероприятий.

Сложность создания приемлемых для практического применения моделей оценки рисков объясняется тем, что один из основных источников риска, связанный с компьютерными преступлениями, характеризуется высокой скрытностью, сложностью сбора улик по установленным фактам их совершения, сложностью доказательств в суде подобных дел, а также вполне определенным контингентом совершающих их лиц, к которым относятся: высококвалифицированные системные и прикладные программисты, специалисты в области телекоммуникационных систем, системные аналитики [2].

Проблема оценки риска существовала с третьего тысячелетия до нашей эры [3]. Однако несмотря на сравнительно большое число публикаций по оценке рисков в области информационных технологий, предлагаемые в них подходы, как правило, основаны либо на использовании моделей определения показателей уязвимости с привлечением экспертных оценок [4], носящих наиболее субъективный характер, либо на использовании моделей определения количественных показателей надежности [5]. К последним относятся модели Шумана, La Padula, Джелинского – Моранды, Шика – Волверта и т. п. Однако исходные утверждения, на основании которых разрабатывались указанные модели, не предполагают их использование для угроз, отнесенных к классу умышленных.

Все это обосновывает актуальность создания формальных моделей оценки риска в информационных технологиях, более приемлемых для практического применения.

Целью данной статьи является изложение комплексного подхода к решению указанной проблемы, основанного:

1) на определении и классификации основных понятий;

2) введении условных обозначений, отражающих принадлежность понятия к определенному классу;

3) применении математических методов при построении формальных моделей оценки риска и проведении анализа получаемых результатов.

При этом учитывалась возможность наличия как случайных, так и умышленных угроз, а также использовались положения технических нормативных правовых актов [6–12], содержащие определение риска и требования к механизмам, направленным на его минимизацию.

Предложенные подходы учитывают наличие в составе информационных технологий программно управляемых компонентов, реализующих по определенным алгоритмам обработку поступающей информации и предоставление получаемых результатов конечным пользователям, другим компонентам или другим информационным технологиям. С учетом данной особенности, носящей, как легко заметить из ее описания, рекурсивный характер, предлагается не делать принципиальных различий между информационными технологиями и их компонентами.

1. Обозначение и классификация компонентов информационных технологий

Компоненты информационных технологий (далее – компоненты), как правило, обладают достаточно высоким уровнем защиты от проведения исследований их конструктивных особенностей, определяющих реализуемые компонентом алгоритмы. Использование таких компонентов осуществляется в соответствии с эксплуатационной документацией, что предполагает потенциальную возможность отличия их реальных функциональных возможностей от функциональных возможностей, продекларированных в эксплуатационной документации.

В связи с этим при классификации компонентов будем учитывать:

– наличие доступа к любой информации о конструктивных особенностях компонента, реально определяющих алгоритмы его функционирования;

– количество допустимых (корректных) состояний, в которых может находиться компонент в процессе функционирования;

– количество допустимых элементарных воздействий на компонент, инициирующих переход компонента из одного состояния в другое.

Для классификации компонентов будем использовать прописной символ латинского алфавита C_y^z, верхний индекс которого указывает на количество допустимых состояний, а нижний – на количество допустимых элементарных воздействий. При отсутствии доступа к информации о тех или иных конструктивных особенностях компонента предполагаемые количества допустимых состояний и/или воздействий на компонент принимаются равными ∞.

2. Обозначение и классификация угроз

Обычно под угрозой понимают потенциально возможное действие или событие, приводящее к нарушению свойства безопасности некоторого объекта (компонента). Предположив, что в эксплуатационной документации все свойства компонента, определяющие его безопасность, сформулированы корректно, на самом верхнем уровне абстракции в данной статье предлагается рассматривать только две угрозы. Одна из них определяется как потенциальная возможность наличия в составе компонентов неспецифицированных возможностей, влияющих на свойства безопасности, а вторая – как потенциальная возможность их проявления в процессе функционирования компонента. В рамках дальнейшей конкретизации обсуждаемых вопросов для обозначения и классификации угроз будем использовать символы, ассоциируемые с вероятностями, определяющими наличие указанных потенциальных возможностей. При этом для непосредственного обозначения вероятности, определяющей наличие данных потенциальных возможностей, будем использовать квадратные скобки, в которых указывается обозначение соответствующей угрозы.

Для классификации угроз предлагается использовать прописной символ латинского алфавита P_y^z, верхний индекс которого указывает причину, вызвавшую наличие данной угрозы, а нижний – этап жизненного цикла компонента, на котором существует вероятность ее реализации (проявления).

С применением этих обозначений угрозы, которые реализуются на этапе разработки и связанные с ошибочными, умышленными или любыми действиями субъектов, участвовавшими в процессе разработки компонента, независимо от того, являлись они ошибочными или умышленными, обозначаются соответственно как P_d^e, P_d^i и P_d^s. Очевидно, что

$$[P_d^s] = [P_d^e] + [P_d^i] - [P_d^e] \cdot [P_d^i].$$

Для условного обозначения угроз, определяемых как потенциальная возможность проявления неспецифицированных возможностей на этапе эксплуатации компонента, также предлагается использовать аналогичное обозначение, снабженное функциональными скобками, в которых указывается ранее принятое обозначение потенциальной возможности наличия проявляемой угрозы. С применением этих обозначений предлагаемая классификация представляется следующим образом:

$P_w^a(P_d^s)$ – угроза потенциальной возможности отклонения, вызванного наличием неспецифицированных возможностей и связанного с некоторыми неумышленными действиями субъектов, которые имеют доступ к компоненту в процессе эксплуатации;

$P_w^i(P_d^i)$ – угроза потенциальной возможности отклонения, вызванного наличием неспецифицированных возможностей и связанного с умышленными действиями субъектов, участвовавших в процессе разработки компонента, а также с умышленными действиями субъектов, имеющих доступ к компоненту в процессе эксплуатации;

$P_w^s(P_d^s)$ – суммарная угроза потенциальной возможности отклонения, вызванного наличием неспецифицированных возможностей. Очевидно, что

$$[P_w^s(P_d^s)] = [P_w^a(P_d^s)] + [P_w^i(P_d^i)] - [P_w^a(P_d^s)] \cdot [P_w^i(P_d^i)]. \quad (1)$$

3. Обозначение, классификация и общая модель оценки рисков

Для обозначения риска предлагается использовать прописной символ латинского алфавита R, а классификацию проводить на основе связанных с ним угроз, указываемых в функциональных скобках. Таким образом, риски, связанные с угрозами $P_w^a(P_d^s)$, $P_w^i(P_d^i)$ и $P_w^s(P_d^s)$, будут соответственно обозначаться как $R\ (P_w^a(P_d^s))$, $R\ (P_w^i(P_d^i))$ и $R\ (P_w^s(P_d^s))$.

Определив риск в соответствии с [7] и используя в качестве условного обозначения величины ущерба, который может быть получен в результате проявления угрозы, прописной символ латинского алфавита D, получим следующую общую модель оценки риска:

$$R\ (P_w^*(P_d^*)) = k \cdot D_{\max} \cdot [P_w^*(P_d^*)],$$

где $P_w^*(P_d^*)$ определяет класс соответствующей угрозы; k – связующий коэффициент, равный $0{,}5$ для угрозы $R\ (P_w^a(P_d^s))$ и 1 для угрозы $R\ (P_w^i(P_d^i))$; $D_{\max}$ определяет величину максимального ущерба проявления угрозы. Таким образом:

$$R\ (P_w^a(P_d^s)) = 0{,}5 \cdot D_{\max} \cdot [P_w^a(P_d^s)]; \quad (2)$$

$$R\ (P_w^i(P_d^i)) = D_{\max} \cdot [P_w^i(P_d^i)]. \quad (3)$$

Значение $R\ (P_w^s(P_d^s))$ вычисляется на основании (1)–(3):

$$R\ (P_w^s(P_d^s)) = D_{\max} \cdot (0{,}5 \cdot [P_w^a(P_d^s)] + [P_w^i(P_i^i)] - 0{,}5 \cdot [P_w^a(P_d^s)] \cdot [P_w^i(P_i^i)]\ ). \quad (4)$$

4. Оценка значений составляющих угроз

Не уходя от сути обсуждаемой проблемы, максимально упростим рассматриваемый компонент, на примере которого будем проводить оценку значений составляющих угроз.

Итак, пусть исследуемый нами компонент имеет:

– один переключатель, который может находиться в двух положениях: «Вкл.» и «Выкл.» и предназначен для включения и выключения компонента, связанного с подачей электропитания;

– две клавиши для ввода информации с нанесенными на них символами 0 и 1;

– одноразрядный экран, предназначенный для отображения символа, который нанесен на нажатую клавишу.

В руководстве по эксплуатации указано, что данный компонент предназначен для вывода на экран символа, который нанесен на клавишу, нажатую первой в промежутке между его включением и выключением.

Таким образом, предполагается, что компонент в процессе его эксплуатации может находиться в следующих состояниях:

1) выключен – переключатель находится в положении «Выкл.», экран погашен;

2) только включен – переключатель находится в положении «Вкл.», экран монотонно освещен;

3) включен и первой была нажата клавиша 0 – переключатель находится в положении «Вкл.», на экране отображен символ 0;

4) включен и первой была нажата клавиша 1 – переключатель находится в положении «Вкл.», на экране отображен символ 1.

Все возможные действия, которые могут быть выполнены в процессе эксплуатации, обозначим следующим образом:

а) изменить положение переключателя;

б) нажать клавишу 0;

в) нажать клавишу 1.

Функциональная спецификация изменений состояния компонента (табл. 1) отражает для каждого исходного состояния компонента, указанного в левом столбце таблицы, его последующее состояние, в которое он переходит после выполнения определенного действия, указанного в верхней строке таблицы. Если для состояний 2, 3 и 4 ввести новые обозначения с использованием только обозначения последовательно выполняемых действий, переводящих компонент из начального состояния в одно из этих состояний, то данная функциональная спецификация представляется в виде варианта 2.

Таблица 1
Функциональная спецификация изменений состояния компонента

Вариант 1					Вариант 2			
	а	**б**	**в**			**а**	**б**	**в**
1	2	1	1		**1**	а	1	1
2	1	3	4		**а**	1	аб	ав
3	1	3	3		**аб**	1	аб	аб
4	1	4	4		**ав**	1	ав	ав

Предположим, что реализация исследуемого компонента выполнялась в полном соответствии с его функциональной спецификацией. Тогда полный набор тестов для тестирования данной реализации может быть следующим:

Тест 1: 1а → 2а → 1 (аа);
Тест 2: 1а → 2б → 3а → 1 (аба);
Тест 3: 1а → 2в → 4а → 1 (ава);
Тест 4: 1а → 2б → 3б → 3а → 1 (абба);
Тест 5: 1а → 2б → 3в → 3а → 1 (абва);

Тест 6: 1а → 2в → 4б → 4а → 1 (авба);
Тест 7: 1а → 2в → 4в → 4а → 1 (авва).

Отметим, что в процессе тестирования не предусматривалось выполнение действий, связанных с нажатием клавиш в выключенном состоянии компонента, так как при отсутствии электропитания они не имеют смысла.

При наличии доступа к информации, гарантирующей, что рассматриваемый компонент конструктивно выполнен таким образом, что в выключенном состоянии он не может обрабатывать действий по нажатию клавиш, а после включения эти действия обрабатываются в полном соответствии с его функциональной спецификацией, данный компонент относится к классу C_3^4 и на основании результатов формального тестирования с использованием полного набора тестов может быть доказано его полное соответствие функциональной спецификации, т. е.:

$$[P_w^a(P_d^s)]=0; \tag{5}$$

$$[P_w^i(P_d^i)]=0, \tag{6}$$

а из (1)–(4) следует, что и

$$R\ (P_w^a(P_d^s))=0; \tag{7}$$

$$R\ (P_w^i(P_d^i))=0. \tag{8}$$

Теперь предположим, что реализация компонента могла быть выполнена не в полном соответствии с приведенной выше функциональной спецификацией, а конструктивные особенности компонента позволяют ему сохранять и обрабатывать информацию практически о всех действиях, производимых в процессе его эксплуатации, т. е. компонент фактически может быть отнесен к классу C_3^∞. В этом случае реальная функциональная спецификация изменений состояния компонента по результатам выполняемых действий может самым существенным образом отличаться от спецификации, представленной в табл. 1. Например, реальная функциональная спецификация такого компонента для самого общего случая может быть представлена в следующем виде (табл. 2).

Таблица 2

Функциональная спецификация компонента для класса C_3^∞

	а	**б**	**в**
1	а	б	в
а	аа	аб	ав
аа	ааа	ааб	аав
.	.	.	.
аб	аба	абб	абв
аба	абаа	абаб	абав
абаа	абааа	абааб	абаав
.	.	.	.
.	.	.	.
б	ба	бб	бв
ба	баа	баб	бав
баа	бааа	бааб	баав
.	.	.	.
.	.	.	.

С учетом последнего предположения каждое конкретное состояние компонента характеризуется последовательностью всех действий, выполненных с того момента, когда он находился в начальном состоянии 1, поэтому легко заметить, что общее количество конечных состояний, в которых может находиться компонент после выполнения n действий, составит 3^n.

Компонент, реализация которого соответствует высказанным предположениям, обеспечивает:

– сохранение информации о выполнении очередного действия;

– обработку хранимой информации о выполненных действиях;

– переход в следующее состояние в соответствии с результатом обработки хранимой информации о выполненных действиях.

Если предположить, что компонент может хранить информацию не более чем об l действиях, непосредственно предшествовавших процессу обработки хранимой информации, то в этом случае общее количество состояний, в которых может находиться компонент, не превышает значения y^l, а функционально полный набор тестов должен предусматривать выполнение всех возможных последовательностей действий, длина которых не превышает l. Для рассматриваемого случая $y = 3$, а предельное значение z составляет 3^l, и естественно предположить, что при их выполнении не все получаемые конечные состояния могут удовлетворять функциональной спецификации состояний компонента, приведенной в табл. 1.

С учетом того что количество последовательностей длины l, входящих в состав функционально полного набора последовательностей данной длины, находится в экспоненциальной зависимости по отношению к y, а само значение l может принимать сколь угодно большие значения и, как правило, неизвестно, оценим вероятность получения ошибочных результатов в процессе обычного функционирования испытываемой реализации:

$$\begin{cases} z = \infty; \\ p = [P_w^a (P_d^s)]. \end{cases} \tag{9}$$

Указанную оценку можно получить, обработав результаты выполнения n различных последовательностей действий, осуществляемых случайным образом.

Для случая (9) получение данной оценки сводится к решению задачи, описанной ниже.

На отрезке $[0, 1]$ расположена точка p, определяющая сечение данного отрезка на две части и задающая отображение всех точек данного отрезка в элементы множества $\{+,-\}$ следующим образом:

– каждая точка, лежащая на отрезке $[0, p]$, отображается в –;

– каждая точка, лежащая на отрезке $(p, 0]$, отображается в +.

Далее из отрезка $[0, 1]$ по равномерному закону распределения выбираются n точек, которые сразу же отображаются в элементы множества $\{+,-\}$, т. е. конечные результаты произведенной выборки содержат лишь образы выбранных точек, а не числовые значения, соответствующие их расположению на отрезке $[0, 1]$.

На основании конечных результатов произведенной выборки требуется определить такое значение p, чтобы точка, задающая сечение, располагалась на отрезке $[0, p]$ с заданной вероятностью P.

С использованием схемы испытаний Бернулли решение данной задачи при общем количестве выборок, равном n, среди которых m результатов принимает значение минус, следующее:

$$P = \frac{\int_0^p x^m (1-x)^{n-m} dx}{\int_0^1 x^m (1-x)^{n-m} dx}. \tag{10}$$

Очевидно, что если исследуемый компонент относится к компонентам, критичным к отказам, то нас будут интересовать только серии испытаний с нулевым количеством отрицательных результатов, т. е. когда $m = 0$. В этом случае

$$P = \frac{\int_0^p (1-x)^n dx}{\int_0^1 (1-x)^n dx} = 1-(1-p)^{n+1}, \tag{11}$$

откуда

$$p = 1 - \sqrt[n+1]{1-P}\,. \tag{12}$$

Таким образом, если для функциональной спецификации, представленной в табл. 2, необходимо будет с вероятностью $0{,}95$ узнать значение p после семи удачно завершенных тестов (ааабаавааббаабваавбаавва), соответствующих функционально полному набору тестов для функциональной спецификации, представленной в табл. 1, то оно окажется равным $\approx 0{,}45$. С учетом того, что в данной интерпретации именно значение p определяет оценку вероятности получения отрицательного результата при выполнении очередного действия в процессе эксплуатации компонента, нас также будет интересовать и обратная задача, т. е. определение минимального количества тестов, при выполнении которых с вероятностью, равной P, можно утверждать, что вероятностная оценка получения в процессе эксплуатации отрицательного результата не превышает некоторого критического значения p:

$$p = 1 - \sqrt[n+1]{1-P}\,, \tag{13}$$

откуда

$$n = \frac{\ln(1-P)}{\ln(1-p)} - 1\,. \tag{14}$$

В критичных к отказам системах значение p составляет $10^{-6} - 10^{-8}$, а требуемая достоверность – 0,95. Используя (14), рассчитаем значение n для $P = 0{,}95$ и $p = 10^{-6}$:

$$n \approx 2995730\,.$$

При наличии средств автоматизации процесса тестирования подготовка и выполнение такого количества действий вполне реальны.

Итак, в случае C_3^∞ после $2\,995\,730$ удачно завершенных действий с вероятностью $0{,}95$ можно утверждать, что вероятность отклонения, вызванного наличием неспецифицированных возможностей, не превышает 10^{-6}:

$$[P_w^a(P_d^s)] \le 10^{-6}\,.$$

Отметим, что данные о наличии в компоненте неспецифицированных и труднонаходимых возможностей, связанных с ошибками проектирования, неизвестны как самим разработчикам, так и потенциальным пользователям. Из этого следует, что предложенные выше вероятностные оценки наличия и проявления таких угроз являются весьма приемлемыми.

Далее предположим, что кому-то из персонала, имеющего доступ к исследуемому компоненту, известна такая последовательность действий, выполнение которой переводит компо-

нент в ошибочное состояние. Естественно, что длина такой последовательности должна гарантировать практически нулевую вероятность ее вхождения в состав последовательностей, используемых в процессе тестирования, и в то же время должна позволять ее безошибочное выполнение в весьма ограниченный промежуток времени. Рассмотрим данный случай для C_y^∞ более подробно, считая, что суммарное количество всех действий, выполняемых в процессе тестирования, не превышает некоторого значения L.

Предполагая, что порядок осуществления действий был определен наиболее оптимальным образом, т. е. любая последовательность, состоящая не менее чем из l действий, выполняется в процессе тестирования только один раз, если соблюдается условие

$$L \le (y^l + l - 1), \tag{15}$$

найдем длину l, для которой вероятность вхождения некоторой случайной последовательности данной длины в состав тестов не превышает значения p_l.

Учитывая, что максимальное количество различных последовательностей длины l, которые могут входить в состав последовательности длины L, не превышает

$$L - l + 1, \tag{16}$$

а общее количество всех различных последовательностей данной длины равно y^l, получаем, что

$$\frac{L - l + 1}{y^l} \le p_l. \tag{17}$$

Считая, что значение l несоизмеримо меньше значения L, можно упростить (17). В итоге получаем

$$\frac{L}{y^l} \le p_l. \tag{18}$$

Из (18) следует

$$l \ge \frac{\ln L - \ln p_l}{\ln y}. \tag{19}$$

Предположив, что $L = 3 \cdot 10^6$, рассчитаем, используя (19), значения l для C_3^∞ и $p_l = 10^{-6}$. В результате получаем $l \approx 27$.

Таким образом, для C_3^∞ установлено, что если существует одна единственная последовательность, состоящая из 27 действий, при выполнении которой компонент переходит в ошибочное состояние, то вероятность ее обнаружения составляет менее 10^{-6}, если тестирование проводилось с общим количеством действий $3 \cdot 10^6$.

В то же время, если кому-то из персонала, имеющего доступ к компоненту, известна данная последовательность действий, то во время очередного доступа он может практически с вероятностью, равной единице, выполнить ее безошибочно и инициировать переход компонента в ошибочное состояние. Фактически значение $[P_w^i(P_d^i)]$ определяется вероятностью безошибочного выполнения субъектом, имеющим доступ к компоненту, известной ему последовательности действий, длина которой для C_3^∞, как было определено ранее, составляет $l \approx 27$, и, следовательно:

$$[P_w^i(P_d^i)] \approx 1.$$

Отметим, что даже для весьма простого компонента C_3^∞ полученные результаты по оценке риска не позволяют делать каких-либо утверждений о безопасности его использования. Кроме того, при добавлении к компоненту клавиш {2,3,4,5,6,7,8,9}, в результате чего компонент станет относиться к классу C_{11}^∞, получим аналогичную оценку значения $l \approx 12$.

При следующем расширении возможностей по вводу прописных букв {А, Б, В, …, Я} с отнесением компонента к классу C_{44}^∞ значение $l \approx 8$, т. е. вероятность безошибочного выполнения субъектом, имеющим доступ к компоненту, известной ему последовательности действий еще больше возрастает и вполне может быть принята за единицу:

$$[P_w^i(P_d^i)] = 1. \tag{20}$$

Логарифмическая зависимость l от L показывает, что даже многократное увеличение ресурсов на проведение тестирования не может существенным образом повлиять на получаемые результаты.

Приведенные рассуждения позволяют сформулировать следующую терему:

Основная теорема риска. *Для любого C_y^∞, а следовательно, и для любого C_∞^∞, функциональная спецификация которого соответствует классу C_y^z, всегда существует реализация, содержащая неспецифицированную возможность, вероятность обнаружения которой будет сколь угодно малой при сколь угодно большом фиксированном количестве выполняемых в процессе испытаний действий.* Доказывается как следствие (19).

Из всего вышеизложенного следует, что при оценке риска, связанного с использованием компонента, тестирование которого проводилось по принципу «черного ящика», основной риск связан с потенциальной угрозой наличия в компоненте неспецифицированных возможностей. Проявление данной угрозы может быть инициировано выполнением сравнительно небольшой последовательности действий, переводящих компонент в ошибочное состояние и связанных с возможностью доступа к нему субъектов, которым известна данная последовательность действий, т. е. особое внимание в данном случае необходимо обращать на угрозу $P_w^i(P_d^i)$.

Кому-то может показаться, что рассмотренные выше компоненты представляют чисто теоретический интерес и не имеют практического значения. Однако если предположить, что на клавишах компонента C_3^∞ вместо символа 0 (ноль) и символа 1 (единица) написано соответственно «за» и «против» и данный компонент входит в состав информационной технологии, обеспечивающей процесс голосования при принятии решений государственной важности, то мнение о практической значимости приведенных примеров должно существенно измениться. Кроме того, при замене в рассмотренных выше компонентах переключателя на клавишу ввода компоненты классов C_{11}^∞ и C_{44}^∞ вполне могут использоваться для ввода цифровой и символьной информации практически во всех банковских системах.

Следовательно, для компонентов, относящихся к классам C_y^∞ и C_∞^∞, без принятия каких-либо мер вероятность проявления угрозы $P_w^i(P_d^i)$ практически равна единице. Использование таких компонентов в составе критичных к отказам информационных технологий либо должно быть запрещено, либо должно выполняться при условии обязательного проведения комплекса мероприятий, учитывающих факторы, которые влияют на вероятность наличия и проявления данных угроз.

Рассмотрим множество основных факторов, оказывающих наиболее существенное влияние на наличие и проявление угроз $P_w^i(P_d^i)$.

5. Определение основных факторов, влияющих на вероятность наличия и проявления умышленных угроз

Естественно предположить, что любой субъект (далее – S^i), имеющий соответствующий мотив для совершения некоторых противоправных действий (далее – A^i) в отношении кого-либо субъекта (далее – S^u), перед тем как их совершить, также оценивает риск, которому он себя подвергает. При этом происходит поиск ответов на следующие вопросы:

1. Существует ли у S^u потенциальная возможность установления в течение определенного времени T_1 факта, что по отношению к нему были совершены A^i? И если на данный вопрос получен положительный ответ, то какова вероятность реализации данной возможности?

2. Существует ли у S^u потенциальная возможность установления в течение определенного времени T_2 факта, что совершенное по отношению к нему A^i было выполнено именно S^i? И если на данный вопрос получен положительный ответ, то какова вероятность реализации данной возможности?

3. Существует ли у S^u потенциальная возможность привлечения в течение определенного времени T_3 к ответственности S^i? И если на данный вопрос получен положительный ответ, то какова вероятность реализации данной возможности?

4. Какова адекватность ответственности, которая угрожает S^i, по отношению к мотиву, инициирующему выполнение A^i?

Также естественно предположить, что при получении хотя бы одного отрицательного ответа на вопросы 1–3 S^i с единичной вероятностью примет решение о выполнении A^i.

Очевидно, что если умышленные действия по встраиванию в компоненты неспецифицированных возможностей и их последующей инициации рассматривать как противоправные по отношению к пользователям информационных технологий, то приведенные выше утверждения можно применить и при определении множества основных факторов, оказывающих наиболее существенное влияние на наличие и проявление угроз $P_w^i(P_d^i)$.

Для условного обозначения факторов, влияющих на вероятность наличия в составе компонентов неспецифицированных возможностей и их проявлений, предлагается использовать прописной символ латинского алфавита F_y^z, верхний индекс которого указывает на принадлежность фактора к классу сдерживающих или способствующих наличию и (или) проявлению угроз, а нижний – на их смысловые отличия.

К основным сдерживающим факторам, оказывающим понижающее влияние на вероятность наличия и (или) проявления угроз $P_w^i(P_d^i)$, относятся:

F_c^d – *наличие независимого от исполнителя контроля за соответствием разрабатываемых компонентов формальным спецификациям.* Определяет вероятность $P(C_y^z(F_c^p))$ обнаружения в составе C_y^z неспецифицированных возможностей в процессе его разработки. Данная вероятность для C_∞^∞

$$P(C_\infty^\infty(F_c^p))=0. \tag{21}$$

F_{du}^d – *возможность обнаружения в составе компонента неспецифицированной возможности до момента ее проявления в процессе эксплуатации компонента.* Определяет вероятность $P(C_y^z(F_{du}^d))$ обнаружения в составе C_y^z неспецифицированной возможности в течение определенного промежутка времени после его разработки. Данная вероятность для C_∞^∞

$$P(C_{\infty}^{\infty}(F_{du}^{d}))=0\,. \tag{22}$$

F_{da}^{d} – *возможность обнаружения отклонений после их возникновения в процессе эксплуатации компонента.* Определяет вероятность $P(C_{y}^{z}(F_{da}^{d}))$ своевременного обнаружения отклонений в процессе эксплуатации C_{y}^{z}. Данная вероятность для C_{∞}^{∞}

$$P(C_{\infty}^{\infty}(F_{da}^{d}))=P(C_{y'}^{z'}(F_{da}^{d}))\,, \tag{23}$$

где $C_{y'}^{z'}$ – исследуемый компонент, для которого количество допустимых состояний и воздействий в соответствии с его эксплуатационной документацией составляет z и y.

F_{ri}^{d} – *возможность определения причины, инициировавшей возникновение обнаруженного отклонения.* Определяет вероятность $P(C_{y}^{z}(F_{ri}^{d}))$ своевременного определения указанной причины для C_{y}^{z}. Данная вероятность для C_{∞}^{∞}

$$P(C_{\infty}^{\infty}(F_{ri}^{d}))=0\,. \tag{24}$$

F_{rp}^{d} – *возможность определения причины, приведшей к наличию в составе компонента неспецифицированной возможности, позволившей инициировать обнаруженное отклонение.* Определяет вероятность $P(C_{y}^{z}(F_{rp}^{d}))$ своевременного определения указанной причины для C_{y}^{z}. Данная вероятность для C_{∞}^{∞}

$$P(C_{\infty}^{\infty}(F_{rp}^{d}))=0\,. \tag{25}$$

F_{ii}^{d} – *возможность идентификации субъектов, инициировавших возникновение отклонения в процессе эксплуатации компонента.* Определяет вероятность $P(C_{y}^{z}(F_{ii}^{d}))$ своевременной идентификации указанных субъектов для C_{y}^{z}. Данная вероятность для C_{∞}^{∞}

$$P(C_{\infty}^{\infty}(F_{ii}^{d}))=P(C_{y'}^{z'}(F_{ii}^{d}))\,. \tag{26}$$

F_{ip}^{d} – *возможность идентификации субъектов, ответственных за наличие в составе компонента неспецифицированной возможности.* Определяет вероятность $P(C_{y}^{z}(F_{ip}^{d}))$ своевременной идентификации указанных субъектов для C_{y}^{z}. Данная вероятность для C_{∞}^{∞}

$$P(C_{\infty}^{\infty}(F_{ip}^{d}))=P(C_{y'}^{z'}(F_{ip}^{d}))\,. \tag{27}$$

F_{ari}^{d} – *возможность привлечения к ответственности субъектов, инициировавших возникновение отклонения.* Определяет вероятность $P(C_{y}^{z}(F_{ari}^{d}))$ своевременного привлечения к ответственности указанных субъектов для C_{y}^{z}. Данная вероятность для C_{∞}^{∞}

$$P(C_{\infty}^{\infty}(F_{ari}^{d}))=P(C_{k'}^{z'}(F_{ari}^{d}))\,. \tag{28}$$

F^d_{arp} – *возможность привлечения к ответственности субъектов, ответственных за наличие в составе компонента неспецифицированной возможности.* Определяет вероятность $P(C^z_y(F^d_{arp}))$ своевременного привлечения к ответственности указанных субъектов для C^z_y. Данная вероятность для C^∞_∞

$$P(C^\infty_\infty(F^d_{arp})) = P(C^{z'}_{y'}(F^d_{arp})). \quad (29)$$

F^d_{adi} – *адекватность степени ответственности субъектов, умышленно инициировавших возникновение отклонения.* Определяет вероятность $P(C^z_y(F^d_{adi}))$ невыполнения субъектами умышленных действий по инициации для C^z_y отклонения при наступлении определенного события, если им известно, что они могут быть привлечены к ответственности с вероятностью

$$p_{ari} = P(C^z_y(F^d_{da})) \cdot P(C^z_y(F^d_{ri})) \cdot P(C^z_y(F^d_{ii})) \cdot P(C^z_y(F^d_{ari})). \quad (30)$$

F^d_{adp} – *адекватность степени ответственности субъектов, умышленно внедривших в состав компонента неспецифицированную возможность.* Определяет вероятность $P(C^z_y(F^d_{adp}))$ отказа от умышленного внедрения субъектами в C^z_y неспецифицированной возможности при наступлении определенного события, если им известно, что они могут быть привлечены к ответственности с вероятностью

$$\begin{aligned} p_{arp} = &\left(P(C^z_y(F^p_c)) + P(C^z_y(F^d_{du}))\right) \cdot P(C^z_y(F^d_{ip})) \cdot P(C^z_y(F^d_{arp})) - \\ &- P(C^z_y(F^p_c)) \cdot P(C^z_y(F^d_{du})) \cdot \left(P(C^z_y(F^d_{ip})) \cdot P(C^z_y(F^d_{arp}))\right)^2. \end{aligned} \quad (31)$$

К основным факторам, оказывающим повышающее влияние на вероятность наличия и (или) проявления потенциальных угроз, относятся:

F^p_{mi} – *наличие мотива у субъектов для умышленного инициирования неспецифицированной возможности.* Определяет вероятность $P(C^z_y(F^p_{mi}))$ выполнения субъектами умышленных действий по инициированию для C^z_y отклонения при наступлении определенного события, если им известно, что они могут быть привлечены к ответственности с вероятностью p_{ari}. Очевидно, что

$$P(C^z_y(F^p_{mi})) = 1 - P(C^z_y(F^d_{adi})). \quad (32)$$

F^p_{ei} – *наличие множества* E_i *определенных событий*, при наступлении которых субъектами, имеющими доступ к информационной технологии, может быть принято решение об умышленном инициировании неспецифицированной возможности для C^z_y. Определяет вероятность $P(C^z_y(F^p_{ei}))$ наступления одного из событий, включенных в множество E_i.

F^p_{mp} – *наличие мотива у субъектов, участвующих в процессе разработки информационной технологии, для умышленного внедрения неспецифицированной возможности.* Определяет вероятность $P(C^z_y(F^p_{mp}))$ умышленного внедрения субъектами неспецифицированной возмож-

ности в C_y^z при наступлении определенного события, если им известно, что они могут быть привлечены к ответственности с вероятностью p_{arp}. Очевидно, что

$$P(C_y^z(F_{mp}^p)) = 1 - P(C_y^z(F_{adp}^d)). \quad (33)$$

F_{ep}^p *– наличие множества* E_p *определенных событий*, при наступлении которых субъектами, участвующими в процессе разработки информационной технологии, может быть внедрена неспецифицированная возможность в C_y^z. Определяет вероятность $P(C_y^z(F_{ep}^p))$ наступления одного из событий, включенных в множество E_p.

F_c^p *– сложность формальных спецификаций компонента*. Определяет вероятность $P(C_y^z(F_c^p))$ наличия в составе C_y^z неспецифицированных возможностей, связанных с ошибками субъектов, которые участвуют в процессе разработки.

На основании приведенных выше обозначений можно разрабатывать формальные модели оценки рисков. Однако для оценки числовых значений приведенных выше основных факторов требуется их дальнейшая конкретизация. При этом необходимо учитывать особенности условий разработки и эксплуатации исследуемых компонентов, а также корреляционные зависимости, существующие между факторами, которые влияют на вероятность наличия и проявления потенциальных угроз.

6. Пример формальной модели оценки риска для угрозы $P_w^i(P_d^i)$

Предположив, что можно получить приемлемые оценки значений для основных факторов, оценим риск причинения ущерба при возникновении отклонения, вызванного наличием угрозы $P_w^i(P_d^i)$.

Из (3) следует, что для этого необходимо найти значение вероятности $P_w^i(P_d^i)$, которое может быть определено следующим образом:

$$[P_w^i(P_d^i)] = P(C_y^z(F_{mp}^p)) \cdot P(C_y^z(F_{ep}^p)) \cdot P(C_y^z(F_{mi}^p)) \cdot P(C_y^z(F_{ei}^p)). \quad (34)$$

Легко заметить, что первые два сомножителя определяют вероятность наличия в составе компонента неспецифицированных возможностей, связанных с умышленными действиями субъектов, участвовавших в процессе его разработки, следующие два – вероятность выполнения умышленных действий субъектами, имеющими доступ к информационной технологии в процессе эксплуатации. Далее из (3) и (34) получаем

$$R(P_w^i(P_d^i)) = D_{\max} \cdot P(C_y^z(F_{mp}^p)) \cdot P(C_y^z(F_{ep}^p)) \cdot P(C_y^z(F_{mi}^p)) \cdot P(C_y^z(F_{ei}^p)). \quad (35)$$

В предложенной модели наиболее сложным является определение значений сомножителей $P(C_y^z(F_{ep}^p))$ и $P(C_y^z(F_{ei}^p))$, связанных с множествами определенных событий E_p и E_i, при наступлении которых субъектами может быть внедрена, а затем и инициирована неспецифицированная возможность. Анализ полученной модели показывает, что при использовании импортируемых компонентов класса C_∞^∞, для которых значение составляющих $P(C_y^z(F_{mp}^p))$ и $P(C_y^z(F_{ep}^p))$, как правило, принимается равным единице, основные усилия должны быть направлены на минимизацию значений составляющих $P(C_y^z(F_{mi}^p))$ и $P(C_y^z(F_{ei}^p))$.

В то же время для компонентов класса C_y^z при обеспечении в соответствии с [9−11] уровня гарантийных требований не ниже пятого класса значение составляющих $P(C_y^z(F_{mp}^p))$ и $P(C_y^z(F_{ep}^p))$ практически сводится к нулю.

Заключение

Несмотря на то что в вопросе оценки рисков пока нет единых универсальных решений и каждая организация, обладая определенной направленностью деятельности и имея специфические особенности применения информационных технологий, индивидуально предпринимает шаги по их оценке, предлагаемый подход позволяет говорить о наличии некоторой общности в решениях обсуждаемого вопроса. Например, одним из наиболее общих результатов, получаемых из основной теоремы риска, является утверждение, что для компонентов, относящихся к классам C_y^∞ и C_∞^∞, без принятия каких-либо мер по минимизации вероятность проявления угрозы $P_w^i(P_d^i)$ практически равна единице при наступлении события из множества E_i. Другими словами, использование таких компонентов в составе критичных к отказам информационных технологий либо должно быть запрещено, либо должно выполняться при условии обязательного проведения комплекса мероприятий, учитывающих факторы, влияющие на вероятность наличия и проявления угрозы $P_w^i(P_d^i)$.

Предоставляемые возможности по разработке формальных моделей оценки риска и проведению последующего анализа функциональных зависимостей между результирующими величинами и значениями элементов, входящих в состав модели, позволяют оптимизировать затраты, связанные с проведением мероприятий, которые направлены на минимизацию риска, и тем самым существенно повысить их эффективность, т. е. получить приемлемые результаты в условиях ограниченных ресурсов.

Список литературы

1. Осовецкий, Л.Г. Анализ защищенности сетей АТМ / Л.Г. Осовецкий, М.В. Тарасюк, А.Ю. Щеглов // Технология и средства связи. – 1998. – № 4. – С. 103–107.

2. Леонов, А.П. Безопасность автоматизированных банковских и офисных систем/ А.П. Леонов, К.А. Леонов, Г.В. Фролов. – Минск : НКП Беларуси, 1996. – 280 с.

3. Vincent, T. Covello. Risk Analysis and Risk Management: An Historical Perspective / Vincent T. Covello and Jeryl Mumpower // Risk Analysis. – 1985. – Vol. 5, № 2.

4. Герасименко, В.Ф. Защита информации в автоматизированных системах обработки данных. В 2-х кн. : Кн. 1 / В.Ф. Герасименко. – М. : Энергоатомиздат, 1994. – 400 с.

5. Благодатских, В.А. Стандартизация разработки программных средств/ В.А. Благодатских, В.А. Волнин, К.Ф. Поскакалов. – М. : Финансы и статистика, 2005. – 288 с.

6. СТБ П ИСО/МЭК 17799-2000/2004. Информационные технологии и безопасность. Правила управления информационной безопасностью.

7. ГОСТ Р 51897 – 2002. Менеджмент риска. Термины и определения.

8. ГОСТ Р 51898 – 2002. Аспекты безопасности. Правила включения в стандарты.

9. СТБ 34.101.1-2004 (ИСО/МЭК 15408-1-1999). Информационная технология. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

10. СТБ 34.101.2-2004 (ИСО/МЭК 15408-2-1999). Информационная технология. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.

11. СТБ 34.101.3-2004 (ИСО/МЭК 15408-3-1999). Информационная технология. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности.

12. СТБ П 34.101.6. Информационные технологии и безопасность. Задание по обеспечению безопасности. Разработка, обоснование, оценка.

Поступила 21.03.08

Объединенный институт проблем
информатики НАН Беларуси,
Минск, Сурганова, 6
e-mail: y.tsynkevich@gmail.com

U.V. Anishchanka, E.A. Tsynkevich

FORMALIZATION OF THE ESTIMATION OF RISKS IN INFORMATION TECHNOLOGIES

The formalized approach to risks estimation in information technologies is considered. The formalized definitions of risk, threat and its components in the information technologies as well as the factors causing the threats are introduced. Along with definitions of proposed concepts their classification is suggested. On a simple example the impossibility of guaranteed minimization of threat display of risk of class $P_w^i(P_d^i)$ for the components concerning the class C_∞^∞ is shown and the basic theorem of risk is formulated. On an example of threat $P_w^i(P_d^i)$ the possibility of construction of formal models for estimating the risks based on the formalized concepts is shown.