DOI: 10.25728/mlsd.2022.1068

ОЦЕНКА СТОИМОСТИ УЩЕРБА СЛОЖНОЙ СИСТЕМЫ

Калашников А.О., Аникина Е.В., Бугайский К.А.
Институт проблем управления им. В.А. Трапезникова РАН,
Россия, г. Москва, ул. Профсоюзная д.65
aokalash@ipu.ru, ajanet@ipu.ru, kabuga@ipu.ru

Аннотация: в настоящей работе рассматривается подход к оценке стоимости ущерба при определении рисков информационной безопасности сложной системы в условиях, когда известны распределения отдельных элементов бизнес-процессов по программно-аппаратным комплексам системы и их стоимостные характеристики.

Ключевые слова: информационный ресурс, бизнес-процесс, локальный ущерб, бинарная свертка.

Введение

Современный этап развития социально-экономической сферы в России характеризуется активным внедрением информационных технологий как для решения конкретных прикладных задач, так и для решения задач управления сложными объектами: от отдельных предприятий до систем национального масштаба, например, таких, как информационные системы, реализуемые в рамках национальных проектов «Цифровая экономика», «Наука», «Образование», «Здравоохранение», «Жильё и городская среда», «Экология». Это создает предпосылки для разработки и внедрения большого количества крупномасштабных и, как правило, распределенных систем. В основе данных систем лежат сложные компьютерные и телекоммуникационные сети, безопасность которых является ключевым элементом обеспечения соответствия целевым показателям систем в целом. Данное обстоятельство определяет и реакцию государства, выражающуюся, в частности, в развитии нормативной и правовой базы критической информационной инфраструктуры РФ. Которая, в соответствии с Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» включает в себя и объекты повышенной опасности, например, относящиеся к области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности. Действующая нормативно-правовая база и передовой международный опыт предполагают решение вопросов обеспечения безопасности сложных и ответственных систем на основе риск-ориентированного подхода.

В самом общем виде риск-ориентированный подход предполагает оценку вероятности нанесения того или иного ущерба в процессе функционирования системы. Что может быть описано как решение двух задач: оценка вероятности реализации угроз и оценка потенциального ущерба в случае их реализации

Задача оценки рисков с точки зрения вероятности реализации угроз достаточно хорошо разработана и остается в центре внимания исследователей [1-3]. Обзоры (см., например [4-7]) наиболее известных методик оценки рисков информационной безопасности показывают, что с одной стороны, для эффективной оценки информационных рисков требуется количественная, желательно финансовая, оценка ущерба от реализации возможных угроз, а с другой стороны, наиболее распространённым методом оценки ущерба от реализации возможных угроз является экспертная оценка на качественном уровне.

Таким образом, существует объективная проблема представления качественных характеристик ущерба в количественном виде. Как правило данная проблема решается назначением каждой из качественных характеристик определенных числовых значений с последующей их интеграцией. Одним из таких подходов является, например, предложенный в работах [2, 3, 8] метод оценки информационных рисков с использованием механизмов комплексного оценивания.

Из работ [1-8] также следует вывод о важности определения не только оцениваемых параметров ущерба, но и размерности шкалы качественной оценки. Которая должна представлять качественные характеристики потенциального ущерба от реализации возможных угроз, виде понятном прежде всего руководству компаний и организаций, то есть в денежном эквиваленте.

1 Общая модель оценки ущерба для сложной системы

Согласно сложившейся отечественной и международной практике [9, см. литературу там же] определение уровня защищенности информационной системы базируется на оценке уровня значимости (критичности) обрабатываемой в ней информации. При этом уровень значимости

полностью задается степенью ущерба возникающем при нарушении конфиденциальности, целостности и доступности обрабатываемой информации.

То есть имеется иерархия понятий:

уровень защищенности → уровень значимости → ущерб.

Однако, необходимо учесть, что:

- перечень видов ущерба динамичен, он постоянно расширяется и уточняется (например, в статьях посвященных анализу информационных рисков все чаще выделяется экологический ущерб);
- на учитываемые виды ущерба и их оценку могут влиять ограничения различного характера, в том числе этического;
- существуют случаи (например, оценка информации личного характера, военной или политической информации), когда нет необходимости или возможности прямого определения ценности информации в денежных единицах.

Анализ существующих подходов к управлению рисками [2, 3, 8 см. литературу там же] позволяет сделать вывод о том, что характеристики потенциального ущерба существенно зависят от характера деятельности компании или организации. Которая в достаточной для данной работы мере описывается бизнес-процессами. Функционирование бизнес-процессов в современных условиях практически невозможно без применения информационных технологий. Тогда иерархия понятий может быть расширена следующим образом:

уровень защищенности → уровень значимости → ущерб →
бизнес-процессы → информационные технологии.

Таким образом, при проведении оценки потенциального ущерба целесообразно сосредоточиться на оценке вклада компонент информационных технологий в нарушения бизнес-процессов. Что позволяет абстрагироваться от вида и степени потенциального ущерба, но дает возможность формирования исходных данных для риск-ориентированного подхода при обеспечении безопасности сложных систем.

Для определения вклада компонент информационных технологий в оценку потенциального ущерба рассмотрим следующую модель компании или организации. Будем считать, что:

1) деятельность компании или организации может быть описана перечнем взаимосвязанных бизнес-процессов;

2) сами бизнес-процессы с точки зрения информационных технологий – это движение документов и данных;

3) понятия «ценность информации» и «ущерб (от нарушения конфиденциальности, целостности или доступности информации)» возникают в процессе «потребления» (сбора, обработки и хранения) информации при реализации бизнес-процессов;

4) сбор, обработка и хранение информации в интересах бизнес-процессов осуществляется с помощью программных, аппаратных и программно-аппаратных средств;

5) нарушения конфиденциальности, целостности или доступности информации могут быть осуществлены в процессе работы данных средств.

Можно считать, что «ценность информации» определяется:

- ценностью или стоимостью бизнес-процесса, в котором используется информация;
- влиянием информации на достижение конечных целей бизнес-процесса.

Для объектов критической информационной инфраструктуры выполнение указанных двух условий является обязательным при проведении категорирования объектов. Следовательно, есть все основания считать, что руководство компании или организации может определить стоимость/ценность бизнес-процесса в денежном выражении (например, как часть прибыли).

Для конкретизации дальнейшего изложения введем понятие «информационный ресурс» (далее – ИР), под которым будем понимать данные и/или документ(ы) и средства их обработки, необходимые для решения задач обеспечения функционирования бизнес-процесса.

Обозначим: p – бизнес-процесс, s – стоимость бизнес-процесса, r – информационный ресурс, q – ущерб.

На основании приведенных выше рассуждений можно построить следующие морфизмы:

$s = f(p), q = g(s), r = h(p), q = k(r)$.

Которые в свою очередь дают возможность построить морфизм: $r = \sigma(s)$, что позволяет говорить о ценности ИР, выраженной в денежном эквиваленте, то есть, как доли стоимости бизнес-процесса.

Отметим, что отношение $(g^{\circ}\sigma^{\circ}h)$ позволяет рассматривать стоимость ИР как эквивалент потенциального ущерба бизнес-процессу в случае нарушений функционирования ИР.

Каждый бизнес-процесс состоит, как правило, из нескольких шагов. Можно положить, что конкретный ИР на каждом шаге оказывает непосредственное или опосредованное влияние на достижение целей данного шага. Для учета этого фактора воспользуемся продукционной моделью и представим шаг бизнес-процесса в следующем виде:

Если {*имеем набор входных данных Д и параметров условий У*},
то {*применяем правило П и выбираем решение Р по операции с данными Д*}.

Данная модель позволяет самом общем виде классифицировать ИР по степени влияния на бизнес-процесс следующим образом:

- ИР необходим и достаточен по Д и отвечает необходимым и достаточным условиям У;
- ИР необходим, но недостаточен по Д и отвечает необходимым и достаточным условиям У;
- ИР необходим и достаточен по Д и не отвечает необходимым и достаточным условиям У;
- ИР необходим, но недостаточен по Д и не отвечает необходимым и достаточным условиям У;
- ИР несет уточняющий или вспомогательный характер по У или Д.

Таким образом, можно рассматривать стоимость конкретного ИР или вызываемый им потенциальный ущерб для бизнес-процесса в виде:

стоимость ИР = <стоимость бизнес-процесса, данные, условия>.

2 Определение стоимости ИР

Условия У могут трактоваться по-разному, в зависимости от характера бизнес-процессов. Например, это может быть соблюдение таких качеств ИР как достоверность и актуальность. Для абстрагирования от особенностей отдельных бизнес-процессов представляется целесообразным в качестве условий У рассматривать традиционную триаду информационной безопасности – конфиденциальность, целостность, доступность. Такой подход дает возможность определить [9] следующие качественные характеристики для оценивания влияния ИР на бизнес-процесс.

Доступность:

- это единственный ИР используемый на данном шаге бизнес-процесса и время его поступления критично для успешного завершения шага;
- это один из необходимых ИР для данного шага бизнес-процесса и время его поступления критично для успешного завершения шага;
- это единственный ИР используемый на данном шаге бизнес-процесса и время его поступления не критично для успешного завершения шага;
- это один из необходимых ИР для данного шага бизнес-процесса и время его поступления не критично для успешного завершения шага;
- это один из используемых на данном шаге бизнес-процесса ИР и его отсутствие увеличивает время или затраты необходимые для успешного завершения шага.

Целостность:

- это единственный ИР используемый на данном шаге бизнес-процесса и нарушение его целостности критично для успешного завершения шага;
- это единственный ИР используемый на данном шаге бизнес-процесса и нарушение его целостности не критично для успешного завершения шага;
- это один из необходимых ИР для данного шага бизнес-процесса и нарушение его целостности критично для успешного завершения шага;
- это один из необходимых ИР для данного шага бизнес-процесса и нарушение его целостности не критично для успешного завершения шага;
- это один из используемых на данном шаге бизнес-процесса ИР и нарушение его целостности увеличивает время или затраты необходимые для успешного завершения шага.

Конфиденциальность:

- это единственный ИР используемый на данном шаге бизнес-процесса и нарушение его конфиденциальности критично для успешного завершения шага;
- это единственный ИР используемый на данном шаге бизнес-процесса и нарушение его конфиденциальности не критично для успешного завершения шага;

- это один из необходимых ИР для данного шага бизнес-процесса и нарушение его конфиденциальности критично для успешного завершения шага;
- это один из необходимых ИР для данного шага бизнес-процесса и нарушение его конфиденциальности не критично для успешного завершения шага;
- это один из используемых на данном шаге бизнес-процесса ИР и нарушение его конфиденциальности увеличивает время или затраты необходимые для успешного завершения шага.

Для перевода приведенных качественных характеристик оценки степени влияния ИР на бизнес-процесс воспользуемся функцией желательности Харрингтона. В результате получаем шкалу коэффициента влияния ИР на отдельном шаге бизнес-процесса – $V^a \in [0,1]$

Каждый шаг бизнес-процесса имеет определенный вес (влияние) с точки зрения успешности реализации данного бизнес-процесса. Вес шага также может быть выражен через шкалу Харрингтона, что дает коэффициент участия ИР в бизнес-процессе – $V^c \in [0,1]$.

Обозначим:

M^u – стоимость ИР по влиянию условий У для бизнес-процесса;

C – стоимость бизнес-процесса;

N – общее число шагов бизнес-процесса;

K – число шагов бизнес-процесса, в которых задействован данный ИР;

V_i^β – значение коэффициента влияния ИР на -том шаге бизнес-процесса;

V_i^γ – значение коэффициента участия ИР на -том шаге бизнес-процесса;

R – общее число ИР, участвующих в бизнес-процессе;

$A_j = \sum_{i=1}^{K} V_i^\gamma$ – доля -го ИР в стоимости бизнес-процесса по коэффициенту участия;

$B_j = \sum_{j=1}^{K} V_j^\beta$ – доля -го ИР в стоимости бизнес-процесса по коэффициенту влияния.

Соответственно, $D = \sum_{j=1}^{R} A_j$ и C может рассматриваться как величина эквивалентная D.

В результате получаем:

$$M^u = \frac{B}{D} C = \frac{\sum_{i=1}^{K} V_i^\beta}{\sum_{j=1}^{R} \sum_{i=1}^{K} V_i^\gamma} C.$$

Назовем M^u базовой стоимостью ИР.

Предварительно отметим, что в рамках единой информационной системы:

- отдельный ИР может применяться в различных бизнес-процессах в интересах различных пользователей;
- влияние ИР на потенциальный ущерб зависит от характеристик обрабатываемой информации.
- Тогда надо рассмотреть два аспекта влияния данных Д на стоимость ИР для бизнес-процесса, вытекающих из свойств информации:
- чьи интересы затрагивает данный ИР в данном бизнес-процессе;
- для обработки какой информации используется данный ИР.

С точки зрения интересов можно положить, что ИР используется в интересах пользователей системы. Следовательно, необходим коэффициент заинтересованности пользователей V^u. Который определяется как доля пользователей, использующих определенный ИР:

$$V^u = U_i / U,$$

где:

U – общее число пользователей в системе;

U_i – число пользователей использующих ИР.

С точки зрения обрабатываемой информации можно положить, что любой ИР имеет «абсолютную» ценность, выражаемую через принадлежность к одному из видов тайн. Следовательно, необходим коэффициент ценности для пользователей V^V. Который определяется в виде значений следующей шкалы:

- государственная тайна;
- профессиональная тайна;
- коммерческая тайна;
- информация ограниченного распространения;
- публичная информация.

Расчет значений коэффициента ценности V^V также целесообразно вести с помощью функции желательности Харрингтона.

Про эти два коэффициента, – V^u и V^V, – можно сказать следующее:

- они независимы;
- они постоянны для данного ИР и данного бизнес-процесса;
- они влияют на базовую ценность ИР в сторону её увеличения;
- они изменяются в диапазоне от 0 до 1.

Для учета влияния этих коэффициентов на стоимость ИР положим, что они описывают ИР в целом (не зависят от шага бизнес-процесса) и прибегнем к геометрической интерпретации. Представим базовую стоимость ИР M^u в виде площади квадрата со стороной равной 1 в декартовой системе координат. Положим, что коэффициенты V^V и V^u откладываются по осям системы координат, каждый по своей. Точка отсчета каждого из коэффициентов расположена в точке пересечения оси координат и границы квадрата базовой стоимости ИР.

Отсюда следует, что коэффициенты V^V и V^u будут давать приращение к сторонам квадрата базовой стоимости. То есть, $X' = \mathrm{V^a} + \mathrm{V^u}$ и $Y' = \mathrm{V^a} + \mathrm{V^v}$, где: X', Y' – отрезки осей системы координат; $V^a = 1$; $V^u \in [0,1]$; $V^v \in [0,1]$.

Тогда полная стоимость отдельного ИР для конкретного бизнес-процесса будет равна:

$$M = X'Y'M^u.$$

3 Применение метода оценки стоимости ИР при анализе рисков

Современные информационные системы в значительной мере базируются на облачных и граничных вычислениях, а также микросервисах в рамках архитектуры «инфраструктура как код» [10]. Что приводит к включению в состав информационных систем сотен и тысяч средств вычислительной техники в виде виртуальных машин и контейнеров, а также активных сетевых устройств. Данная тенденция в сочетании с бурным ростом «интернета вещей» и «промышленного интернета вещей» вызывает необходимость рассматривать риски информационных систем как сложных сетей. В этом случае не только каждый бизнес-процесс может состоять из нескольких ИР, но и каждый узел сложной сети может обеспечивать функционирование нескольких ИР. Отсюда возникает задача формирования интегральной оценки потенциального ущерба применительно к бизнес-процессам и узлам сложной сети. Как было сказано выше в разделе 1, полную стоимость ИР M можно рассматривать как эквивалент потенциального ущерба бизнес-процессу в случае нарушений функционирования ИР. То есть, нарушения параметров конфиденциальности, целостности или доступности как обрабатываемой в ИР информации, так и средств ее обработки. С учетом требований нормативно-правовой базы и лучших мировых практик по информационной безопасности целесообразно расчет стоимости ИР вести раздельно для этих нарушений (см. раздел 2). Для оценки рисков сложной сети представляется целесообразным использовать интегральные оценки ущерба для ИР, бизнес-процессов и узлов сложной сети.

Введем понятие класса ИР: $I = M/C$. Расчет стоимости ИР раздельно для нарушений конфиденциальности, целостности или доступности можно рассматривать как непересекающиеся подмножества множества I:

I^k – значения класса ИР по условию конфиденциальности;

I^c – значение класса ИР по условию целостности;

I^d – значение класса ИР по условию доступности.

Ранжируем по увеличению значений подмножества I^k, I^c, I^d и соответствующие порядковые номера будем рассматривать в качестве бальных оценок для ИР. Тогда при использовании алгоритма бинарной свертки, изложенного в [8], можно получить интегральную оценку ИР. Целесообразно на нижнем уровне бинарной структуры расположить оценки для I^c и I^d, а на верхнем – для I^k. При этом положим, что матрицы свертки едины для всех ИР анализируемой сложной сети.

Обозначим: $BS(I)$ – функция бинарной свертки; P – общее число бизнес-процессов, в которых участвует ИР; R – общее число ИР, участвующих в отдельном бизнес-процессе; Q – общее число ИР, работающих на отдельном узле.

Тогда интегральные оценки ущерба в сложной сети можно представить как: $W^P = \sum_{j=1}^{P} BS(I_j)$ – для отдельного ИР; $W^R = \sum_{j=1}^{R} BS(I_j)$ – для отдельного бизнес-процесса; $W^Q = \sum_{j=1}^{Q} BS(I_j)$ – для отдельного узла.

4 Заключение

В настоящей работе рассматривается метод оценки стоимости потенциального ущерба необходимого для организации процесса управления рисками сложной системы. Полученные интегральные оценки ущерба могут использоваться для выработки исходных данных в расчетах эффективного распределения затрат на реализацию мер информационной безопасности в информационных системах на основе механизмов теоретико-игрового и стохастического моделирования. А также могут применяться в алгоритмах и методах количественных оценок эффективности применения средств защиты информации на всех этапах жизненного цикла информационной системы, включая этап её проектирования.

Показана возможность выражать в денежном эквиваленте стоимости ИР и узлов сложной сети обеспечивающих функционирование бизнес-процессов при условии известной их стоимости в организации. Аналогичным образом метод может использоваться для проведения сравнительного анализа ценности различных ИР и узлов сложной сети путем введения оценочной стоимости бизнес-процессов.

Определенная с помощью предлагаемого метода интегральная оценка стоимости ущерба позволяет:

- рассматривать задачу размещения ИР по узлам сложной сети в качестве одной из общесистемных мер защиты информации;
- получать динамику изменения класса ИР по шагам бизнес-процессов;
- обеспечить возможность сегментирования узлов сложной сети с учетом требований обеспечения конфиденциальности, целостности и доступности;
- возможность сегментирования узлов сложной сети по диапазону значений интегральной оценки ИР, что будет отражать категорию обрабатываемой информации.

Кроме того, расчет интегральной оценки ущерба для узлов сложной сети дает возможность определять контуры (группы узлов) в информационной системе и распределять средства защиты информации по критерию стоимости/ущерба.

Литература

1. *Ермилов Е. В., Ермилов Е. В., Остапенко Г. А., Калашников А. О.* Функции ущерба риска при описании отказов информационных систем критически важных объектов // Информация и безопасность. – 2013. – Т. 16. – № 2. – С. 247–248;
2. *Калашников А. О.* Управление информационными рисками организационных систем: механизмы комплексного оценивания // Информация и безопасность. – 2016. – Том 20. – № 3(4). – С. 315–322;
3. *Калашников А. О., Аникина Е. В.* Модели управления информационными рисками сложных систем // Информация и безопасность. – 2020. – Том 23. – № 2(4). – С. 191–202;
4. *Пугин В. В., Губарева О. Ю.* Обзор методик анализа рисков информационной безопасности информационной системы предприятия // T-Comm: Телекоммуникации и транспорт. – 2012. – Т. 6. – № 6. – С. 54–57;
5. *Аникин И. В., Емалетдинова Л. Ю., Кирпичников А. П.* Обеспечение информационной безопасности корпоративных информационных сетей через оценку и управление рисками // Вестник Технологического университета. – 2015. – Т. 18. – № 7. – С. 247–250;
6. *Калашников А. О.* Управление информационными рисками с использованием арбитражных схем // Системы управления и информационные технологии. – 2004. – № 4 (16). – С. 57–61;
7 *Баранова Е. К.* Методики анализа и оценки рисков информационной безопасности // Образовательные ресурсы и технологии. – 2015. – №1 (9) – С. 73–79;
8. *Калашников А. О., Аникина Е. В.* Модель управления информационной безопасностью критической информационной инфраструктуры на основе выявления аномальных состояний (часть1) // Информация и безопасность. – 2018. – Том 21. – № 2(4). – С. 145–154;
9. *Калашников А. О., Бугайский К. А., Аникина Е. В.* Методика оценки стоимости информационного ресурса // Информация и безопасность. – 2020. – Т. 23. – № 1. – С. 7–18;
10. *Калашников А. О., Бугайский К. А.* Инфраструктура как код: формируется новая реальность информационной безопасности // Информация и безопасность. – 2019. – Т. 22. – № 4. – С. 495–506.