БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Данилюк С.Г.* Вероятностно-лингвистический метод диагностирования: Учебное пособие. – Серпухов: МО РФ, 1998. – 96 с.
2. Классификация и кластер / Под ред. Дж.Райзина. – М.: Мир, 1980.
3. Нечеткие множества в моделях управления и искусственного интеллекта / Под ред. Д.А. Поспелова. – М.: Наука, 1986. – 312 с.

УДК 681.354

М.Е. Путивцев

АНАЛИЗ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ ПРОЦЕССНОГО ПОДХОДА*

Обеспечение информационной безопасности (ИБ) компьютерных систем различного назначения продолжает оставаться чрезвычайно острой проблемой. Можно констатировать тот факт, несмотря на усилия многочисленных организаций, занимающихся решением этой проблемы, общая тенденция остается негативной. Основных причин этому две:

– возрастающая роль информационных технологий в поддержке бизнес-процессов, как следствие возрастающие требования к ИБ автоматизированных систем. Цена ошибок и сбоев информационных систем возрастает;

– возрастающая сложность информационных процессов. Это предъявляет повышенные требования к квалификации персонала, ответственного за обеспечение ИБ. Выбор адекватных решений, обеспечивающих приемлемый уровень ИБ при допустимом уровне затрат, становится все более сложной задачей.

Аудит информационной безопасности является одним из наиболее актуальных и динамично развивающихся направлений менеджмента в области информационной безопасности (ИБ). Его основной задачей является объективная оценка текущего состояния информационной безопасности организации, а также ее адекватность поставленным целям и задачам бизнеса с целью увеличения эффективности и рентабельности экономической деятельности предприятия [1]. Результаты качественно выполненного аудита позволяют построить оптимальную по эффективности и затратам корпоративную систему защиты, адекватную ее текущим задачам и целям бизнеса.

Основные задачи проведения аудита безопасности включают в себя:

- контроль эффективности затрат на системы информационной безопасности;
- проверка плановых этапов развития СУИБ;
- контроль соблюдения интеллектуальной собственности;
- инвентаризация и детализация информационных ресурсов (финансовые отчеты, планы);
- определения законности и эффективности использования информационных ресурсов;
- выявление недостатков с точки зрения информационной безопасности;
- устранение недостатков и внесение необходимых рекомендация;
- выявление нарушений в АСУ.

В настоящее время существует довольно большое количество как отечественных, так и зарубежных методик и подходов по проведению аудита информаци-

* Работа выполнена при поддержке гранта РФФИ №07-07-00138а.

онной безопасности. Все существующие методики во многом зависят от знаний и компетентности аудитора [2].

Именно поэтому существует проблема получения объективных результатов в области оценки информационной безопасности.

Для решения данной проблемы возникает необходимость в разработке формальных средств (моделей и алгоритмов), позволяющих осуществлять анализ системных процессов по обеспечению информационной безопасности предприятия. С их помощью можно эффективно отображать и анализировать модели деятельности широкого спектра сложных систем в различных разрезах. При этом широта и глубина обследования процессов в системе определяется самим оценщиком, что позволяет не перегружать создаваемую модель излишними данными.

В связи с этим встает вопрос об использовании процессного подхода при исследовании деятельности как ИТ-служб, так и служб информационной безопасности, в основе которого лежат модели процессов управления ИТ-поддержкой и систем ИБ.

Для разработки процессной системы управления в первую очередь необходимо построение динамической модели информационной безопасности предприятия. При разработке модели проектировщики определяют роли участников и функции процессов, реализацией которых занимаются конкретные службы исследуемого предприятия. Формирование служб ИБ на предприятиях происходит путем распределения функций процессов и ролей участников по конкретным сотрудникам штатных подразделений и включения описания процессов в нормативно-регламентные документы предприятий, а функций – в должностные инструкции сотрудников.

На первом этапе под руководством группы компетентных лиц, силами штатных сотрудников исследуемого предприятия, строится модель системных процессов по принципу “как есть”, где дается максимально объективная оценка состояния системных процессов [3]. Такая модель представляет предприятие с позиции сотрудников, которые в нем работают и досконально знают все нюансы, в том числе и неформальные, позволяющее учитывать вопросы по аппаратно-техническому оснащению фирмы. По сути, моделирование системных процессов “как есть” представляет собой регистрацию фактического состояния имеющихся системных процессов, позволяющих обнаружить несоответствия требованиям стандарта по проведению аудита. Моделировать системные процессы должны только те лица, которые потенциально могут быть ответственны за их выполнение и имеют закрепленные за ними роли.

На втором этапе выстроенная модель передается на анализ и обработку аудиторам, которые будут заниматься поискам несоответствий с моделью системных процессов “как должно быть”. Сама модель “как должно быть” является эталонным шаблоном в области управления ИБ и должна представлять собой детализацию всех системных процессов и под-процессов, задействованных в системе информационной безопасности, с определенными ролями и задачами сотрудников предприятия и объектами, которыми оперируют сотрудники при реализации управления ИБ.

Далее вносятся соответствующие изменения, и делается итоговое заключение, которое содержит в себе рекомендации по реорганизации системы управления ИБ в соответствии с сертификацией.

Предложенная методология позволяет получить максимально объективную оценку состояния системы ИБ предприятия.

В данной статье на этапе анализа методологий оценки уровня информационной безопасности, ввиду доступности и достаточно широкой распространенности было решено использовать международный стандарт ИСО\МЭК 17799, регламентирующий принципы управления службами ИБ. Планируемая модель должна представлять собой отображение инфраструктуры конкретно исследуемого предприятия с точки зрения информационной безопасности и характеризует состояние инфраструктуры предприятия с позиции «как есть». То есть данная модель должна давать ответы на следующие вопросы:

1. Какие процедуры (функции, работы) необходимо выполнить для получения объективной оценки уровня ИБ?
2. В какой последовательности выполняются эти процедуры?
3. Какие механизмы контроля и управления существуют в рамках рассматриваемого системного процесса?
4. Кто ответственный за выполнение процесса?
5. Какие входящие документы/информацию использует каждый подпроцесс?
6. Какие исходящие документы/информацию генерирует выполненный подпроцесс?
7. Какие ресурсы необходимы для выполнения процесса/под-процесс?
8. Какая документация/условия регламентирует выполнение процессов?
9. Какие параметры характеризуют выполнение процедур и процесса в целом?

Для моделирования процессов используется несколько различных методов, основой которых являются как структурный, так и объектно-ориентированный подходы к моделированию. Однако деление самих методов на структурные и объектные является достаточно условным, поскольку наиболее развитые методы используют элементы обоих подходов.

При рассмотрении международного стандарта ISO\IEC 17799, отечественным аналогом которого является ГОСТ Р ИСО\МЭК 17799 [4], в соответствии с которым проводится аудит ИБ [5], было отмечено, что объективность результата оценки на соответствия требования стандарта оставляет желать лучшего. Ввиду этого предлагается новая методология проведения сертификации по ГОСТ Р ИСО \МЭК 17799, которая базируется на использовании модели системных процессов по управлению информационной безопасности предприятия.

Технология проведения аудита на соответствие подобным стандартам существенно отличается от технологий, применяемых для предыдущих поколений стандартов, к которым, в частности, относятся Руководящие документы (РД) Гостехкомиссии России 1992–1993 гг. Основное отличие заключается в гораздо большей степени формализации некоторых этапов, использовании поддающихся проверке показателей и критериев, то есть в большей детализации.

Однако при рассмотрении стандарта ISO\IEC 17799 необходимо отметить, что при проведении сертификации на соответствие степень формализации оценочных работ явно недостаточна. Для решения данной проблемы было решено провести подробную детализацию стандарта с определением ролей, задач и объектов, задействованных в проведении сертификации.

В результате проведения детализации режимов международного стандарта на процедуры, процессы и подпроцессы было дано представление содержания структуры ISO 17799 в виде нормальной формы Бэкуса – Наура, исходя из процессной схемы детализации режимов, представленной на рис. 1.

Необходимо отметить, что детализированные подпроцессы должны представлять собой *тривиальную функцию* с входными параметрами. Под тривиальной функцией понимается такая функция, которая не требует никаких пояснений. Результатом работы выполнения тривиальной функции должен являться исходящий документ или информация.

На основе вышеизложенного принципа строится динамическая модель системных процессов. Построение такой модели служит базовым средством для формального описания требований стандарта.

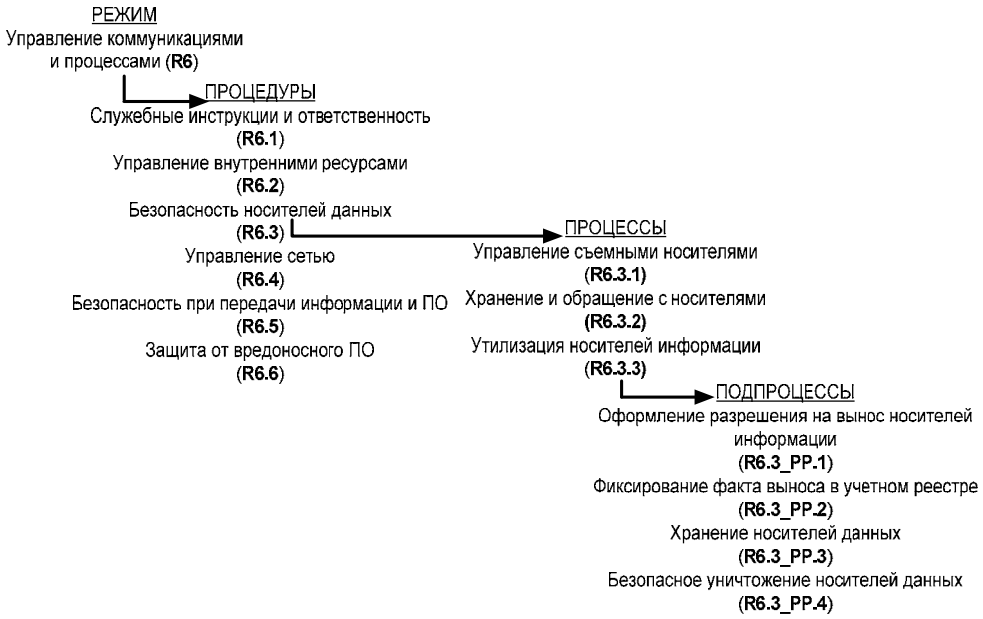

Рис. 1. Процессная схема детализации режимов стандарта ИСО\МЭК 17799

Разработка динамической модели службы информационной безопасности подразумевает собой четкое определение последовательности выполнения всех системных процедур, основанных на международном стандарте безопасности ИСО\МЭК 17799, а также дальнейшая детализация этих процедур на системные процессы и подпроцессы [6]. Для этого была проведена детализация режимов международного стандарта на процедуры, процессы и подпроцессы (рис. 2).

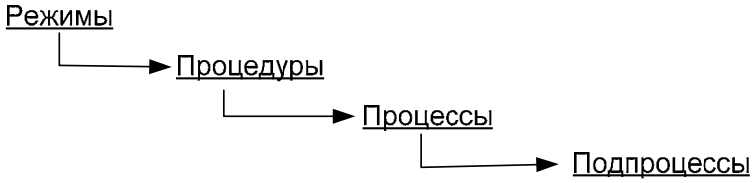

Рис. 2. Структурная детализация

Также в модели должно присутствовать четкое разграничение ответственностей и ролей участников системных процедур и процессов с использованием модели RACI [7].

Изначально при проведении детализации режимов стандарта стал вопрос определения порядка выполнения процедур и составления алгоритмов выполнения процессов в соответствии с международным стандартом.

Необходимо отметить, что уровень детализации должен удовлетворять ожидаемой модели системных процессов. В нашем случае детализированный подпроцесс должен представлять собой тривиальную функцию с входными параметрами. Где под тривиальной функцией понимается такая функция, которая не требует никаких пояснений. Результатом работы выполнения тривиальной функции должен являться исходящий документ или информация.

Итак, при рассмотрении режима «Управление коммуникациями и процессами» была определена последовательность всех процедур для данного режима и составлены алгоритмы выполнения процессов с закрепленными ролями участников процессной системы управления ИБ. Ниже для примера представлен алгоритм «Процедуры разделения ресурсов» (рис. 3.).

Как видно из рис. 3 алгоритм состоит из последовательно выполняемых подпроцессов, входных и результирующих параметров (документы, дополнительные подпроцессы), участников алгоритма и их ролей. Результатом работы данного алгоритма является утвержденный документ с регламентированными правилами переноса программного обеспечения в бизнес среду.

При распределении ролей участников выполнения алгоритма использовалась модель RACI. Данная модель является вспомогательным инструментом при распределении ролей и обязанностей при выполнении системного процесса. Смысл аббревиатур модели RACI изложен ниже:

- **R** – ответственный. Лицо ответственное за проблему/задачу;
- **A** – перед кем ответственен “**R**”. Лицо которое должно подписать или одобрить работу.
- **S** – может быть поддерживающим. Может обеспечить ресурсы или может сыграть поддерживающую роль в выполнении системного процесса.
- **C** – следует проконсультироваться. Имеет ли информацию и способность, необходимую для выполнения работы;
- **I** – следует проинформировать. Необходимо уведомить о результатах, но нет необходимости в консультациях.

Одной из особенностей используемой модели распределения ролей является то, что у каждого системного подпроцесса предпочтительно должно быть только одно «**R**». Расхождение происходит, когда у процесса нет ни одного «**R**». В случае множественных «**R**», необходимо далее детализировать субпроцессы для разделения индивидуальных обязанностей.

Все вышеизложенное представляет собой основы процессной системы управления информационной безопасности.

Результаты работы процессной системы передаются на обработку аналитику по ИБ, который будет заниматься поиском “уязвимых мест” в управлении системой безопасности компании и оптимизацией основных процессов, трансформируя динамическую модель «как есть» в соответствующее представление «как должно быть». На основании этих изменений будет выноситься итоговое заключение, которое должно содержать в себе рекомендации по реорганизации системы управления безопасности.

Полученная динамическая модель менеджмента ИБ позволяет как оценить уровень управления информационной безопасности, так и координировать внедрение новой системы управления ИБ.

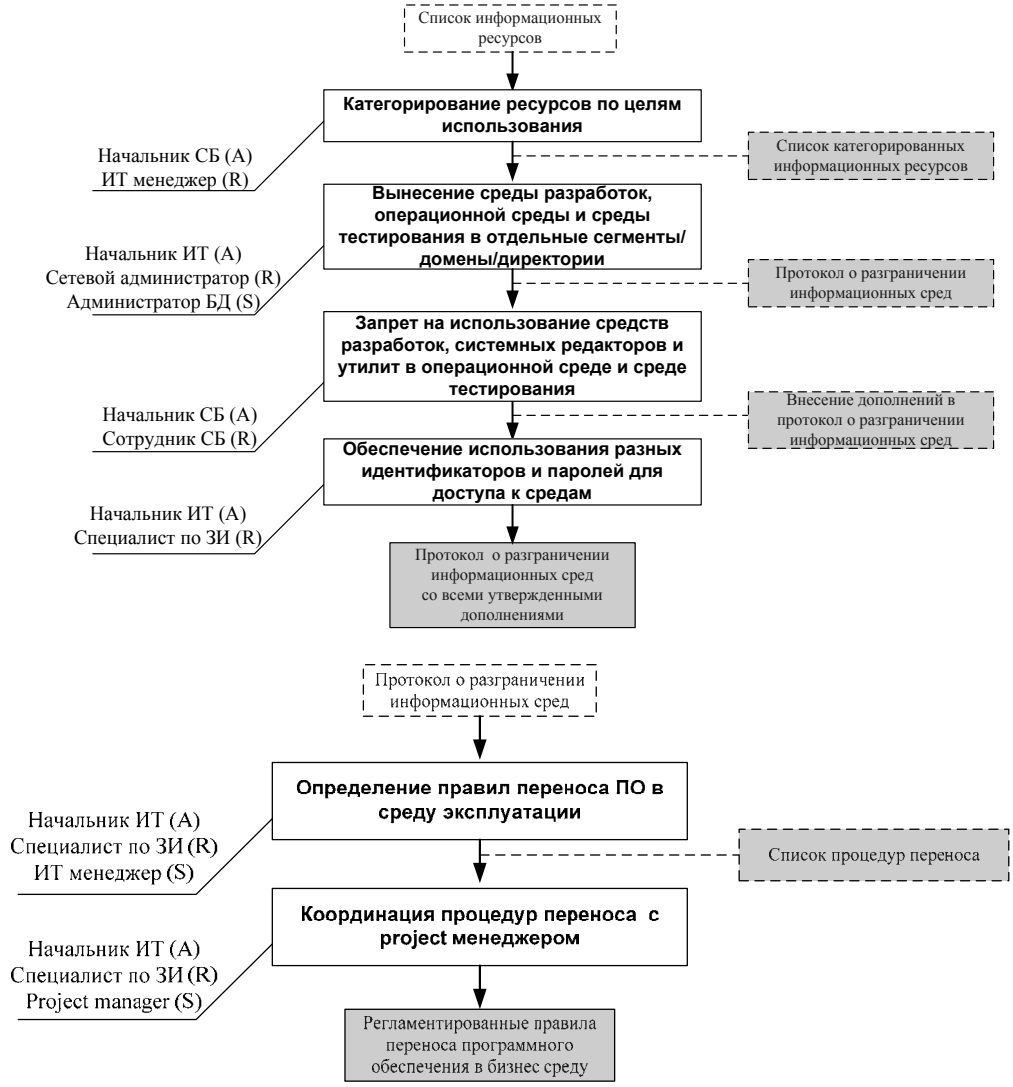

Рис. 3. Процедуры разделения ресурсов

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Петренко С.А., Симонов С.В.* Экономически оправданная безопасность. Управление информационными рисками. – М.: Изд-во ДМК, 2003.

2. *Путивцев М.Е.* Методы комплексной оценки информационной безопасности. – Таганрог: Технологический институт ЮФУ, 2007.

3. *Беккер Й., Вилков Л.* Менеджмент процессов. – М.: Эксмо, 2007. – 358 с.

4. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью. – М.: Стандартинформ, 2006. – 62 с.

5. *Симонов С.В.* Аудит безопасности информационных систем. – М.: Jet Info, 1999. №9.

6. *Путивцев М. Е., Баранник А. А*. Модель проведения сертификации по стандарту ISO\IEC 17799 с использованием процессного подхода. – Таганрог: Технологический институт ЮФУ, 2007.

7. Что такое RACI model? *Источник: http://www.12manage.com/methods_raci_ru.html*

УДК 681.324

И.В. Машкина, С.Н. Алекса

РАЗРАБОТКА МЕТОДА И ФУНКЦИОНАЛЬНОЙ МОДЕЛИ ЧИСЛЕННОЙ ОЦЕНКИ РИСКА НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И УРОВНЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ НА ОСНОВЕ ВЕРОЯТНОСТНО-СТАТИЧЕСКОГО ПОДХОДА*

Адекватный научно-методологический базис должен содержать количественные методы анализа и синтеза систем защиты и управления ими в процессе функционирования. Потому одним из основных положений унифицированной концепции защиты [1] является требование научно обоснованного подхода к оценке, желательно в количественном выражении, требуемого уровня защищенности (риска) на объекте защиты в изменяющихся условиях его функционирования.

Процесс оценивания величины риска нарушения информационной безопасности (ИБ) при проектировании системы защиты информации (СЗИ) включает в себя: определение ценности ресурсов, изучение угроз и уязвимостей, выбор параметров для их описания и получение оценок вероятностей по этим параметрам, оценок теоретической эффективности контрмер и ожидаемого ущерба, определение его приемлемости.

В процессе анализа и оценивания рисков устанавливается степень адекватности используемых или планируемых наборов средств защиты (СрЗ) существующим угрозам. Свойство защищенности информации каждого СрЗ, входящего в СЗИ, в совокупности определяет защищенность информации в СЗИ в целом.

Наличие уязвимости СрЗ может привести к нарушению защищенности, т. е. осуществлению угрозы. При решении задач защиты информации первостепенное значение имеет количественная оценка ее уязвимости. Поскольку воздействие на информацию различных факторов в значительной мере является случайным, то в качестве количественной меры ее уязвимости наиболее целесообразно применить вероятность нарушения защищенности информации $P_{бт}^{н}$.

Неясность способа определения значений вероятностей угроз и уязвимостей является основной проблемой при получении количественной оценки риска нарушения ИБ. Известно, что применение методов классической теории вероятностей допустимо при повторяемости опытов и одинаковости условий. Это требование в сложных системах, какими являются СЗИ, обычно не выполняется.

Значение показателя СрЗ защищенности информации $P_{бт}$ – это *субъективная вероятность* обнаружения и блокирования СрЗ несанкционированных действий, т. е. теоретическая ожидаемая эффективность барьера.

Очевидно, *вероятность нарушения защищенности* $P_{бт}^{н}$ дополняет $P_{бт}$ до единицы т.е.

*Работа выполнена при поддержке гранта РФФИ №08-08-97035.