# РАЗДЕЛ VII. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

**УДК 658.52.011.56**

## СРАВНИТЕЛЬНЫЙ АНАЛИЗ СУЩЕСТВУЮЩИХ МЕТОДОВ ОПРЕДЕЛЕНИЯ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

П.В. Плетнёв, В.М. Белов

Статья посвящена анализу различных подходов к оценке рисков информационной безопасности (ИБ), описанных в научных и учебных изданиях и руководящих документах.

**Ключевые слова:** анализ уязвимостей ИБ, подходы к оценке рисков ИБ.

**Введение:** Вопросам анализа рисков ИБ посвящено большое количество научных трудов, большинство из которых либо изобилуют наличием математических формул и моделей; либо не содержат вообще никаких математических изысков; либо в них существует перевес в сторону какой-либо из двух выше приведенных групп подходов. Проанализируем содержательные аспекты каждой группы подходов.

Подходы первой группы, как правило, используют различные разделы высшей математики: теорию множеств, теорию вероятностей, дискретную математику и т.д. В качестве ядра подходов выбирают принципы, основанные на теории шансов или полезности (надежности), или нечетких множеств, а также непрерывные или дискретные распределения и т.д. Работы, относящиеся к первой группе подходов, зачастую не учитывают реальные требования организаций, занимающихся анализом рисков; требуют от экспертов в области ИБ достаточной математической подготовки; что часто отрицательно сказывается на практике применения данных подходов.

Вторая группа подходов в большей степени развита зарубежными авторами. Статьи авторов из США, Англии носят прежде всего рекомендательный характер для модернизации, пересмотра некоторых вещей уже работающих, зарекомендовавших себя стандартов ИБ: ISO, BS, не требующих глубокого знания высшей математики.

Третья группа подходов во многих случаях сочетает в себе экспертные оценки и оценки рисков, базирующиеся на определении их вероятности по имеющимся статистическим данным. Подобные подходы можно успешно применять в практической деятельности (не смотря на ряд минусов), так как использование базы статистики позволяет свести к минимуму субъективную точку зрения эксперта на решаемую задачу и проводить работу по оценке рисков ИБ специалистам без большого опыта, квалификации.

Далее в настоящей статье будут более подробно проанализированы первая и вторая, с учетом стандартов ИБ России, группы подходов к оценке рисков ИБ.

В некоторых работах осуществлены подходы, использующие теории графов, нечеткой логики. Это позволяет более наглядно представить причинно-следственные связи между объектами, потоками информационной системы, что, в свою очередь, способствует наиболее точному анализу системы на этапе ее проектирования, облегчает работу экспертов по определению оценок рисков ИБ. Кроме того, анализ рисков осуществляют более формализовано, с более простой программной реализацией.

Для подходов второй группы естественно использовать прописи стандартов ИБ, федеральных нормативных документов, рекомендаций. Хотя им не стоит слепо доверять, но такое решение задач ИБ экономит время работы специалистов по защите информации.

Отметим, что очевидные плюсы применения стандартов безопасности не отражены в большинстве проанализированных подходов. Как будет показано ниже, лишь небольшое количество из них основано, или хотя бы использует, некоторые рекомендации стандартов ИБ.

Многие организации до сих пор придерживаются старых способов точечного управления уязвимостями, вместо управления рисками. Такой выбор затрудняет возможную сертификацию организации, требует от спе-

циалистов по безопасности освоения, повышения опыта в новых для них системах анализа рисков. Кроме того, работа в рамках способов управления уязвимостями затрудняет эксплуатацию обязательных в настоящий момент рекомендаций, нормативных документов ФСТЭК и ФСБ РФ.

Отсюда использовать указанные выше способы лучше не полностью, а выбирать некоторые рекомендации, которые не нарушают работу по анализу рисков, но могут повысить точность итоговых результатов, сократить время работы экспертов.

Процесс анализа рисков является составной частью общей системы управления организацией, поэтому для более качественной работы с рисками информационных систем выбирают общую процессную модель. Модель отражает работу стандартного цикла управления Деминга, определяет: Планирование – Выполнение – Проверку – Корректировку. В стандартах ISO и BS присутствует проекция данного процесса на работу по анализу и управлению рисками ИБ.

В большинстве рассмотренных нами подходов осуществляют работу чаще всего только по пункту оценки рисков, то есть непосредственно по разделу «Выполнение». Таким образом, подсчет рисков, выполненная на его основе закупка новых средств и разработка подходов по повышению безопасности, ненамного отличается по качеству от применяемого в аварийных ситуациях так называемого «заплаточного» метода. Только полностью осуществленный цикл управления, последующее его циклическое повторение с корректировкой, пересмотром рисков, позволяет обеспечить ИБ с помощью анализа рисков.

Нельзя не заметить отсутствие для ряда обсуждаемых подходов экономической составляющей анализа. В результате получают, что управление рисками – это только закупка средств защиты, без учета возможностей данной организации.

**Сравнительный анализ:** Сравнение подходов проводили по следующим параметрам: субъективные оценки сложности вычисления и программной реализации; способ ввода входных данных в систему анализа; вид итогового результата анализа – вид выходных данных; использование стандартов ИБ.

Оценка сложности вычислений представляет собой субъективную характеристику сложности использования рассматриваемых подходов, может принимать значения: «Высокая», «Средняя», «Низкая» сложность. На результат «высокой» оценки наибольшее влияние оказывает применение специальных математических теорий, тогда как решения на основе таблиц, экспертных оценок можно характеризовать низкой сложностью вычислений.

Сложность программной реализации также оценивали на основе субъективного мнения. Поэтому, на наш взгляд, можно отметить следующее, что использование математической логики, теории графов облегчает задачу программиста.

Далее, входные данные в систему анализа рисков могут поступать несколькими способами. Основные из них: статистические данные, экспертные оценки. Оба вида данных имеют свои плюсы и минусы, могут быть предназначены для работы в различных ситуациях. На Рисунке 1 представлена статистика по использованию того или иного типа ввода данных в рассматриваемых подходах.

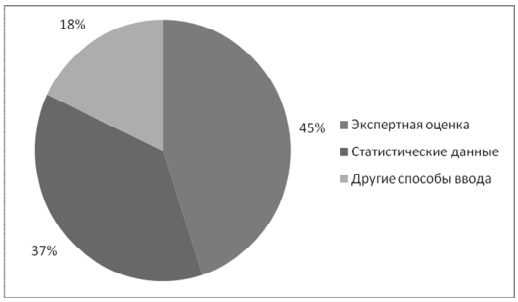


*Рисунок 1 - Соотношение типов входных данных рассматриваемых подходов*

Аналогично входным данным, анализировали типы итоговых результатов. Чаще всего выходные данные представляют в виде количественной или качественной оценки. Хотя количественная оценка является, в большинстве своем, вероятностью риска (точечной оценкой), качественная характеристика более наглядна, дает возможность более простого ранжирования рисков. Статистика типов выходных данных анализируемых подходов представлена на Рисунке 2.

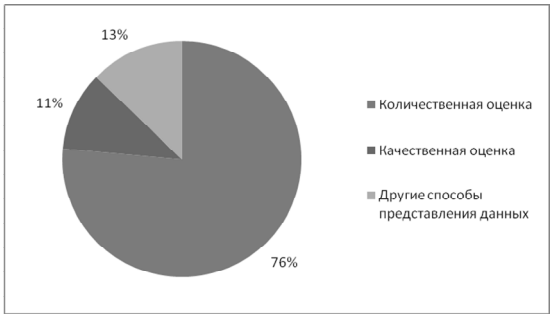


*Рисунок 2 - Соотношение типов выходных данных рассматриваемых подходов*

Как видно из соотношения, количественная оценка преобладает в подходах, представленных в научных статьях, хотя большинство стандартов безопасности используют качественную шкалу оценки.

Последней исследуемой характеристикой сравнения подходов является применение стандартов безопасности, нормативных документов. На Рисунке 3 представлена статистика их использования.

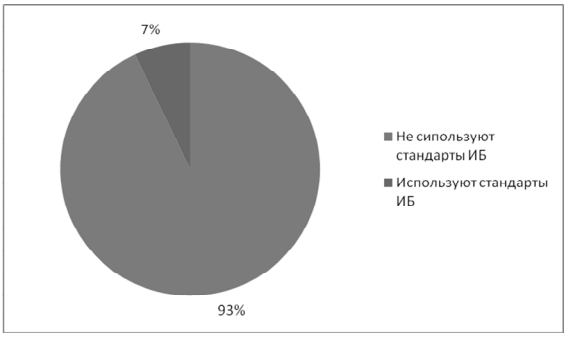


*Рисунок 3 - Соотношение использования стандартов ИБ и нормативных документов в рассматриваемых подходах*

**Заключение:** По результатам работы сделаны следующие выводы: большинство подходов не учитывают концепции, требования различных стандартов ИБ, что может вызвать недоверие к применяемым подходам у экспертов, проводящих анализ рисков ИБ, затрудняет возможную сертификацию организации. Многие подходы, в основе которых лежит цель получить количественную оценку рисков с использованием математических формул, моделей, углубляясь в математические теории, теряют связь с практической оценкой рисков, реальными бизнес требованиями. Ряд подходов не обеспечивают полного процесса по оценке, управлению рисками ИБ, реализуя лишь некоторые его компоненты.

Анализ показывает, что большое количество рассматриваемых подходов содержат свежие идеи, концепции по проведению оценки рисков.

Учитывая сильные и слабые стороны существующих подходов, можно сделать попытку проектирования и реализации более совершенного подхода к оценке рисков ИБ.

**СПИСОК ЛИТЕРАТУРЫ**

1. Кудрявцева, Р. Т. Управление информационными рисками с использованием технологий когнитивного моделирования [Текст] : автореферат дис. … канд. тех. наук : 05.13.19 / Кудрявцева Рима Тимиршаиховна. – Уфа, 2008. – 17 с. – 9 08-5/1180.
2. Кустов, Г. А. Управление информационными рисками организации на основе логико-вероятностного метода [Текст] : автореферат дис. ... канд. тех. наук : 05.13.19 / Кустов Георгий Алексеевич. – Уфа, 2008. – 18 с. – 61 09-5/1099.
3. Лысов, А.С. Задача анализа информационных рисков в государственных учреждениях [Текст] / А.С. Лысов // Безопасность информационных технологий. – 2008. – №1. – С. 39-44.

*Полный перечень литературы не публикуется по причине объёмности более 100 источников.*

*Аспирант кафедры «Безопасность и управление в телекоммуникациях»* ***П.В. Плетнев*** *Новосибирск СибГУТИ, 89236550300 , e-mail: pavelpletnev@rambler.ru, д.т.н., профессор кафедры «Безопасность и управление в телекоммуникациях»* ***В.М. Белов*** *Новосибирск СибГУТИ, р. тел (383) 269-8308, e-mail: vmbelov@mail.ru*