АНАЛИЗ СУЩЕСТВУЮЩИХ МОДЕЛЕЙ ОЦЕНКИ РИСКОВ ИБ ДЛЯ ЧАСТНЫХ ОБЛАЧНЫХ СРЕД

Ермошкин Григорий Николаевич,
аспирант, Всероссийская государственная налоговая академия Минфина РФ
ermoshkin_nn@mail.ru

Аннотация. *Представлен анализ существующих моделей оценки риска на предмет возможности их использования для информационных систем, функционирующих на основе облачных вычислений.*

Ключевые слова: *информационная безопасность, облачная архитектура, частное облако, оценка рисков.*

THE ANALYSIS OF RISK ASSESSMENT MODELS IN SYSTEMS OF PRIVATE CLOUD ARCHITECTURE

Ermoshkin Grigoriy,
Postgraduate student, Russian State Tax Academy Ministry of Finance RF

Abstract. *This article will analyze current models of risk assessment and highlight their problems and advantages, an attempt to use them for resolving some of the issues in area of cloud computing.*

Keywords: *information security, cloud computing, private cloud, risk assessment.*

Введение

В современном мире нельзя представить себе человека, который смог бы обойтись без использования плодов информационных технологий. На всех управленческих уровнях имеется желание расширить свои коммуникационные и информационные возможности за счет внедрения современных информационных технологий.

Общеизвестно, что традиционные центры обработки данных находятся под угрозой вымирания. А преимущества, которыми обладают облачные вычисления огромны, но только, если удастся верно, рассчитать риски. Если погнаться за быстрой прибылью и снижением расходов, о которых говорят, когда речь заходит о переходе к облачным вычислениям и вовремя не осознать какими рисками они грозят обернуться организация может понести серьезные убытки.

Сегодня все больше руководителей ИТ выбирают облачные вычисления. Потребители облачных вычислений могут значительно уменьшить расходы на инфраструктуру информационных технологий (в краткосрочном и среднесрочном планах) и гибко реагировать на изменения вычислительных потребностей, используя свойства вычислительной эластичности (англ. *Elastic computing*) облачных услуг.

С точки зрения поставщика, благодаря объединению ресурсов и непостоянному характеру потребления со стороны потребителей, облачные вычисления позволяют экономить на масштабах, используя меньшие аппаратные ресурсы, чем требовались бы при выделенных аппаратных мощностях для каждого потребителя, а за счёт автоматизации процедур модификации выделения ресурсов существенно снижаются затраты на абонентское обслуживание.

С точки зрения потребителя, эти характеристики позволяют получить услуги с высоким уровнем доступности (англ. *high availability*) и низкими рисками неработоспособности, обеспечить быстрое масштабирование вычислительной системы благодаря *эластичности* без необходимости создания, обслуживания и модернизации собственной аппаратной инфраструктуры.

Удобство и универсальность доступа обеспечивается широкой доступностью услуг и поддержкой различного класса терминальных устройств.

Суть облачных вычислений в переходе к высоко стандартизированным наборам удобных сервисов и программного обеспечения, которые вместе составляют основу высокоэффективного использования ресурсов.

Отсутствие достаточного количества серьезных исследований вопросов риска облачных вычислений, мешает многим организациям совершить переход к облачной модели. В данной работе будет произведен анализ моделей рисков, который частично удовлетворит эту потребность.

1. Частные облачные среды

Частное облако (англ. *private cloud*) — инфраструктура, предназначенная для использования одной организацией, включающей несколько потребителей (например, подразделений одной организации), возможно также клиентами и подрядчиками данной организации.

Частное облако может находиться в собственности, управлении и эксплуатации, как самой организации, так и третьей стороны (или какой-либо их комбинации), и оно может физически существовать как внутри, так и вне юрисдикции владельца.

Если частное облако находится в собственности организации и физически существует внутри ее юрисдикции, то возможно абстрагироваться от идеи облака и считать что фирма его не использует. При использовании частного облака, можно считать клиентом работников организации, а ее саму провайдером услуг.

Исходя из особенностей природы частного облака, можно сказать, что оценка риска для данной модели не имеет сильных отличий от стандартной модели размещения данных. Т.о., возможно использовать существующие модели оценки рисков.

Оценка рисков на качественном уровне не позволяет однозначно сравнить затраты на обеспечение ИБ и получаемую от них отдачу (в виде снижения суммарного риска). Поэтому более предпочтительными представляются количественные методики. Но они требуют наличия оценок вероятности возникновения для каждой из рассматриваемых угроз безопасности. Кроме того, использование интегральных показателей, таких как ALE, опасно тем, что неправильная оценка вероятности угрозы в отношении очень дорогостоящего актива может кардинально изменить оцениваемое значение суммарной стоимости рисков.

2. Риск-модель OCTAVE

Особенность данной модели заключается в том, что весь процесс анализа производится силами сотрудников организации, без привлечения внешних консультантов. Для этого создается смешанная группа, включающая как технических специалистов, так и руководителей разного уровня, что позволяет всесторонне оценить последствия для бизнеса возможных инцидентов в области безопасности и разработать контрмеры.

OCTAVE предполагает три фазы анализа:

1. Разработка профиля угроз, связанных с активом.
2. Идентификация инфраструктурных уязвимостей.
3. Разработка стратегии и планов безопасности.

Методика OCTAVE предлагает при описании профиля использовать “деревья вариантов”, пример подобного дерева для угроз класса 1 приведен на рисунке 1.

Главная задача первой стадии - стандартизованным образом описать сочетание угрозы и ресурса.

Предположим, что на предприятии имеется информационный ресурс (актив) - база данных (БД) отдела кадров (HR Database). Профиль, соответствующий угрозе кражи информации сотрудником предприятия представлен в таблице 1.

Вторая фаза исследования системы в соответствии с методикой - идентификация инфраструктурных уязвимостей. В ходе этой фазы определяется инфраструктура, поддерживающая существование выделенного ранее актива и то окружение, которое может позволить получить к ней доступ.

Рассматриваются компоненты следующих классов: серверы; сетевое оборудование; СЗИ; персональные компьютеры; домашние персональные компьютеры “надомных” пользователей, работающих удаленно, но имеющих доступ в сеть организации; мобильные компьютеры; системы хранения; беспроводные устройства; прочее.

Группа, проводящая анализ для каждого сегмента сети, отмечает, какие компоненты в нем проверяются на наличие уязвимостей. Уязвимости проверяются сканерами безопасности уровня операционной системы, сетевыми сканерами безопасности, специализированными сканерами, с помощью списков уязвимостей (checklists), тестовых скриптов.

Для каждого компонента определяется:

- список уязвимостей, которые надо устранить немедленно (high-severity vulnerabilities);

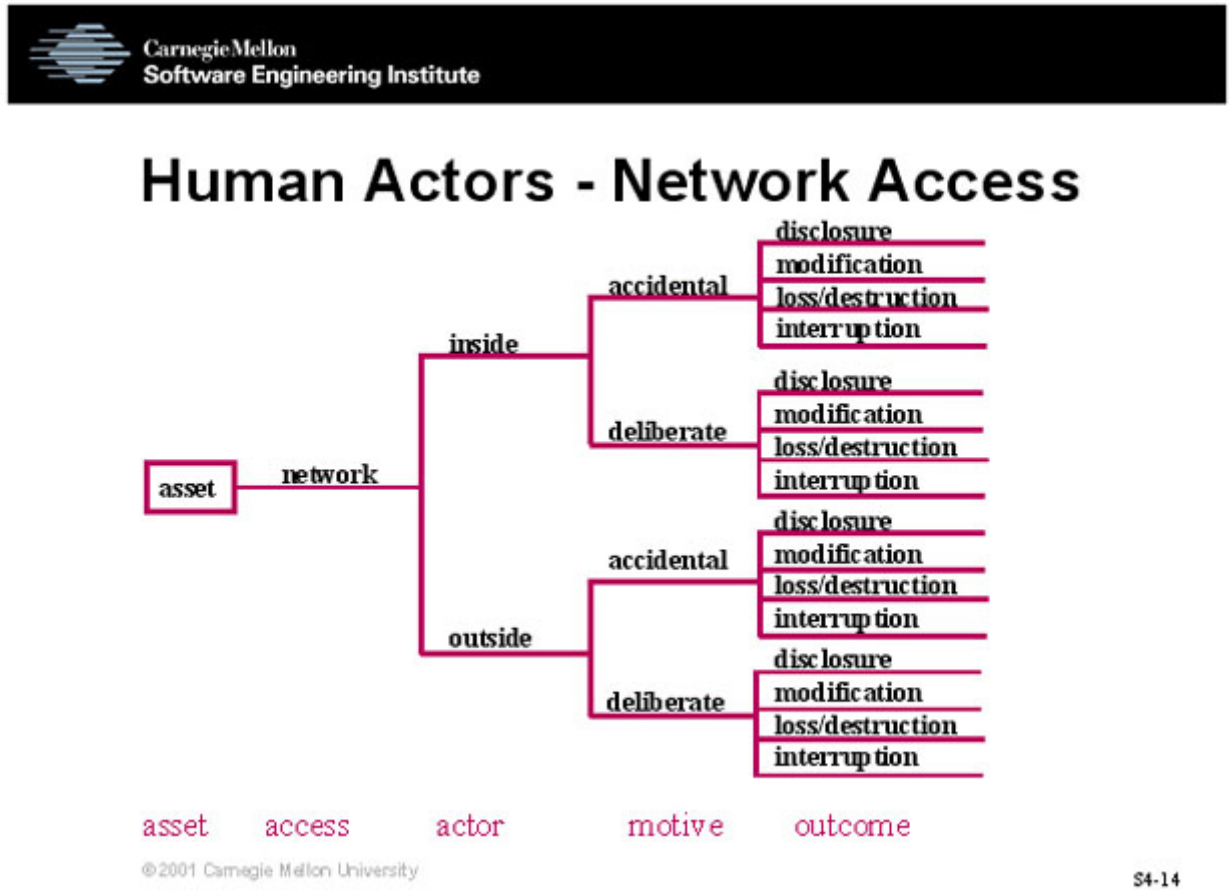

Рис. 1. Дерево вариантов, использующееся при описании профиля

- список уязвимостей, которые надо устранить в ближайшее время (middle-severity vulnerabilities);
- список уязвимостей, в отношении которых не требуется немедленных действий (low-severity vulnerabilities).

По результатам стадии готовится отчет, в котором указывается, какие уязвимости обнаружены, какое влияние они могут оказать на выделенные ранее активы, какие меры надо предпринять для устранения уязвимостей.

Разработка стратегии и планов безопасности - третья стадия исследования системы. Она начинается с оценки рисков, которая проводится на базе отчетов по двум предыдущим этапам. В OCTAVE при оценке риска дается только оценка ожидаемого ущерба, без оценки вероятности. Шкала: высокий (high), средний (middle), низкий (low). Оценивается финансовый ущерб, ущерб репутации компании, жизни и здоровью клиентов и сотрудников, ущерб, который может вызвать судебное преследование в результате того или иного инцидента. Описываются значения, соответствующие каждой градации шкалы.

Далее, разрабатывают планы снижения рисков нескольких типов:

- долговременные;
- на среднюю перспективу;
- списки задач на ближайшее время.

Для определения мер противодействия угрозам в методике предлагаются каталоги средств.

В случаи использования организацией частного облака данная модель может быть использована для проведения оценки риска. Т.к. организация сохраняет контроль над данными и оборудованием она может использовать данную модель без внесения в нее поправок. Если же физически оно находится вне юрисдикции организации и ее работники не

Таблица 1

Пример профиля угрозы

Ресурс (Asset)	БД отдела кадров (HR Database)
Тип доступа (Access)	Через сеть передачи данных (Network)
Источник угрозы (Actor)	Внутренний (Inside)
Тип нарушения (Motive)	Преднамеренное (Deliberate)
Уязвимость (Vulnerability)	-
Результат (Outcome)	Раскрытие данных (Disclosure)
Ссылка на каталог уязвимостей (Catalog reference)	-

имеют к доступа к оборудованию данная методика не может быть использована, т.к. нет возможности произвести полный учет всех инфраструктурных уязвимостей.

Хотелось бы еще раз подчеркнуть, что в отличие от прочих методик, OCTAVE не предполагает привлечения для исследования безопасности ИС сторонних экспертов, а вся документация по OCTAVE общедоступна и бесплатна, что делает методику особенно привлекательной для предприятий с жестко ограниченным бюджетом, выделяемым на цели обеспечения ИБ.

Мониторинг рисков не является сильной стороной OCTAVE, несмотря на то, что так же, как и другие методики, полностью отвечает критериям категории «Риски». OCTAVE предусматривает регулярное проведение оценки ИТ-рисков и обновление их величин как части процесса оценки рисков. В случаи, когда стратегия управления рисками определена, OCTAVE предполагает использование в качестве способов снижения рисков только его снижение и принятие. Такой способ управления рисками, как обход (исключение) или передача не используется.

OCTAVE подразумевает адаптацию к конкретным условиям применения, например к размеру компании, виду бизнеса, требованиям законодательства и тех или иных стандартов и пр.

OCTAVE не дает количественной оценки рисков, однако качественная оценка может быть использована в определении количественной шкалы их ранжирования. В оценку могут включаться различные области рисков, которые, за исключением технических рисков и рисков нарушения законодательства, напрямую не включены в методику. Таковые учитываются косвенно, в ходе проведения интервью с владельцами информационных активов, во время которых выясняется, какие последствия могут наступить в случае реализации угроз.

Данная модель не формирует четких инструкций по организации мониторинга состояния рисков, но подчеркивает важность его наличия.

3. Риск-модель CRAMM

В основе модели CRAMM лежит комплексный подход к оценке рисков, сочетающий количественные и качественные методы анализа. Модель является универсальной и подходит как для крупных, так и для малых организаций, как правительственного, так и коммерческого сектора. Версии программного обеспечения CRAMM, ориентированные на разные типы организаций, отличаются друг от друга своими базами знаний (profiles).

Исследование ИБ системы с помощью риск-модели CRAMM проводится в три стадии.

На первой стадии анализируется все, что касается идентификации и определения ценности ресурсов системы. Она начинается с решения задачи определения границ исследуемой системы: собираются сведения о конфигурации системы и о том, кто отвечает за физические и программные ресурсы, кто входит в число пользователей системы, как они ее применяют, или будут применять.

Проводится идентификация ресурсов: физических, программных и информационных, содержащихся внутри границ системы. Каждый ресурс необходимо отнести к одному из предопределенных

классов. Затем строится модель информационной системы с позиции ИБ. Для каждого информационного процесса, имеющего, по мнению пользователя, самостоятельное значение и называемого пользовательским сервисом, строится дерево связей используемых ресурсов. Построенная модель позволяет выделить критичные элементы.

Ценность физических ресурсов в CRAMM определяется стоимостью их восстановления в случае разрушения.

Ценность данных и программного обеспечения определяется в следующих ситуациях:

- недоступность ресурса в течение определенного периода времени;
- разрушение ресурса - потеря информации, полученной со времени последнего резервного копирования, или ее полное разрушение;
- нарушение конфиденциальности в случаях несанкционированного доступа штатных сотрудников или посторонних лиц;
- модификация - рассматривается для случаев мелких ошибок персонала (ошибки ввода), программных ошибок, преднамеренных ошибок;
- ошибки, связанные с передачей информации: отказ от доставки, недоставка информации, доставка по неверному адресу.

Для оценки возможного ущерба CRAMM рекомендует использовать следующие параметры:

- ущерб репутации организации;
- нарушение действующего законодательства;
- ущерб для здоровья персонала;
- ущерб, связанный с разглашением персональных данных отдельных лиц;
- финансовые потери от разглашения информации;
- финансовые потери, связанные с восстановлением ресурсов;
- потери, связанные с невозможностью выполнения обязательств;
- дезорганизация деятельности.

Для данных и программного обеспечения выбираются применимые к данной ИС критерии, дается оценка ущерба по шкале со значениями от 1 до 10.

При низкой оценке по всем используемым критериям (3 балла и ниже) считается, что рассматриваемая система требует базового уровня защиты, и вторая стадия исследования пропускается.

На второй стадии рассматривается все, что относится к идентификации и оценке уровней угроз для групп ресурсов и их уязвимостей. В конце стадии заказчик получает идентифицированные и оцененные уровни рисков для своей системы. На этой стадии оцениваются зависимость пользовательских сервисов от определенных групп ресурсов и существующий уровень угроз и уязвимостей, вычисляются уровни рисков и анализируются результаты.

Ресурсы группируются по типам угроз и уязвимостей. Оценка уровней угроз и уязвимостей производится на основе исследования косвенных факторов.

CRAMM объединяет угрозы и уязвимости в матрице риска. Основной подход, для решения этой проблемы состоит в рассмотрении:

- уровня угрозы;
- уровня уязвимости;
- размера ожидаемых финансовых потерь.

Исходя из оценок стоимости ресурсов защищаемой ИС, оценок угроз и уязвимостей, определяются "ожидаемые годовые потери". На рисунке 2 приведен пример матрицы оценки ожидаемых потерь. В ней второй столбец слева содержит значения стоимости ресурса, верхняя строка заголовка таблицы - оценку частоты возникновения угрозы в течение года (уровня угрозы), нижняя строка заголовка - оценку вероятности успеха реализации угрозы (уровня уязвимости).

Значения ожидаемых годовых потерь (англ. Annual Loss of Expectancy) переводятся в CRAMM в баллы, показывающие уровень риска.

В соответствии с приведенной ниже матрицей, выводится оценка риска (рисунок 3.).

Третья стадия исследования заключается в поиске адекватных контрмер. По существу, это поиск варианта системы безопасности, наилучшим образом удовлетворяющей требованиям заказчика.

На этой стадии CRAMM генерирует несколько вариантов мер противодействия, адекватных выявленным рискам и их уровням. Контрмеры можно объединить в три категории: около 300 рекомендаций общего плана; более 1000 конкретных рекомендаций; около 900 примеров того, как можно организовать защиту в данной ситуации.

Таким образом, CRAMM - пример модели, в которой первоначальные оценки даются на качественном уровне, и потом производится переход к количественной оценке (в баллах).

При использовании частного облака, если организация сохраняет контроль над данными и

		0.1	0.1	0.1	0.34	0.34	0.34	1	1	1	3.33	3.33	3.33	10	10	10
		0.1	0.5	1	0.1	0.5	1	0.1	0.5	1	0.1	0.5	1	0.1	0.5	1
1	1000	1.0E+01	5.0E+01	1.0E+02	3.4E+01	1.7E+02	3.4E+02	1.0E+02	5.0E+02	1.0E+03	3.3E+02	1.7E+03	3.3E+03	5.0E+03	5.0E+03	1.0E+04
2	10000	1.0E+02	5.0E+02	1.0E+03	3.4E+02	1.7E+03	3.4E+03	1.0E+03	5.0E+03	1.0E+04	3.3E+03	1.7E+04	3.3E+04	5.0E+04	5.0E+04	1.0E+05
3	30000	3.0E+02	1.5E+03	3.0E+03	1.0E+03	5.1E+03	1.0E+04	3.0E+03	1.5E+04	3.0E+04	1.0E+04	5.0E+04	1.0E+05	1.5E+05	1.5E+05	3.0E+05
4	100000	1.0E+03	5.0E+03	1.0E+04	3.4E+03	1.7E+04	3.4E+04	1.0E+04	5.0E+04	1.0E+05	3.3E+04	1.7E+05	3.3E+05	5.0E+05	5.0E+05	1.0E+06
5	300000	3.0E+03	1.5E+04	3.0E+04	1.0E+04	5.1E+04	1.0E+05	3.0E+04	1.5E+05	3.0E+05	1.0E+05	5.0E+05	1.0E+06	1.5E+06	1.5E+06	3.0E+06
6	1000000	1.0E+04	5.0E+04	1.0E+05	3.4E+04	1.7E+05	3.4E+05	1.0E+05	5.0E+05	1.0E+06	3.3E+05	1.7E+06	3.3E+06	5.0E+06	5.0E+06	1.0E+07
7	3000000	3.0E+04	1.5E+05	3.0E+05	1.0E+05	5.1E+05	1.0E+06	3.0E+05	1.5E+06	3.0E+06	1.0E+06	5.0E+06	1.0E+07	1.5E+07	1.5E+07	3.0E+07
8	1E+07	1.0E+05	5.0E+05	1.0E+06	3.4E+05	1.7E+06	3.4E+06	1.0E+06	5.0E+06	1.0E+07	3.3E+06	1.7E+07	3.3E+07	5.0E+07	5.0E+07	1.0E+08
9	3E+07	3.0E+05	1.5E+06	3.0E+06	1.0E+06	5.1E+06	1.0E+07	3.0E+06	1.5E+07	3.0E+07	1.0E+07	5.0E+07	1.0E+08	1.5E+08	1.5E+08	3.0E+08
10	1E+08	1.0E+06	5.0E+06	1.0E+07	3.4E+06	1.7E+07	3.4E+07	1.0E+07	5.0E+07	1.0E+08	3.3E+07	1.7E+08	3.3E+08	5.0E+08	5.0E+08	1.0E+09

Рис. 2. Матрица оценки ожидаемых потерь

Threat	Very Low	Very Low	Very Low	Low	Low	Low	Medium	Medium	Medium	High	High	High	Very High	Very High	Very High
Vuln.	Low	Medium	High	Low	Medium	High	Low	Medium	High	Low	Medium	High	Low	Medium	High
Asset Value															
1	1	1	1	1	1	1	1	1	2	1	2	2	2	2	3
2	1	1	2	1	2	2	2	3	3	2	3	3	3	3	4
3	1	2	2	2	2	3	2	3	3	3	3	4	3	4	4
4	2	2	3	2	3	3	3	3	4	3	4	4	4	4	5
5	2	3	3	3	3	4	3	4	4	4	4	5	4	5	5
6	3	3	4	3	4	4	4	4	5	4	5	5	5	5	6
7	3	4	4	4	4	5	4	5	5	5	5	6	5	6	6
8	4	4	5	4	5	5	5	5	6	5	6	6	6	6	7
9	4	5	5	5	5	6	5	6	6	6	6	7	7	7	7
10	5	5	6	5	6	6	6	6	6	6	7	7	7	7	7

Рис. 3. Матрица оценки риска

физическими компонентами системы данная модель не нуждается во внесении поправок на облачную природу. Однако следует сказать о некоторых недостатках данной модели. Если организация не имеет контроля над оборудованием, то невозможно использовать ни один из стандартных сценариев данной модели, ни одна из стадий исследования не может быть полностью закончится, т.е., модель не может быть использована без внесения ряда поправок. Однако остается возможность использовать в анализе данные провайдера и использовать модель без корректировок.

Эта модель не учитывает, например, наличие или отсутствие «программ по повышению информированности сотрудников в области информационной безопасности», сопроводительной документации, такой как описание бизнес-процессов или отчетов по проведенным оценкам ИТ-рисков. В отношении стратегии работы с рисками CRAMM предполагает использование только методов их снижения. Такие способы управления рисками, как обход, принятие или передача не рассматриваются.

Сильная сторона модели — идентификация элементов риска: материальных и нематериальных активов и их ценности, угроз, мер безопасности, величины потенциального ущерба и вероятности реализации угрозы.

Риск-модель CRAMM использует количественные и качественные способы оценки ИТ-рисков, однако не определяет условий, при которых последние могут быть приняты компанией, и не включает в себя расчет возврата инвестиций на внедрение мер безопасности, несмотря на то, что принятие решения о применении той или иной меры должно базироваться не только на величине риска, но и на стоимости ее реализации и владения.

Модель CRAMM имеет существенные недостатки. В ней отсутствуют: процесс интеграции способов управления и описании назначения того или иного способа; мониторинг эффективности

используемых способов управления и способов управления остаточными рисками; перерасчет максимально допустимых величин рисков; процесс реагирования на инциденты.

Практическое применение CRAMM сопряжено с необходимостью привлечения специалистов высокой квалификации; трудоемкостью и длительностью процесса оценки рисков, который может потребовать многих месяцев непрерывной работы высококвалифицированных специалистов; необходимостью обработки вручную сотен страниц отчетной документации, генерируемых программным инструментарием CRAMM.

4. Риск-модель RiskWatch

Компания RiskWatch разработала собственную модель анализа рисков и семейство программный средств, в которых она в той либо иной мере реализуется.

В семейство RiskWatch входят программные продукты для проведения различных видов аудита безопасности.

В моделе RiskWatch в качестве критериев для оценки и управления рисками используются ожидаемые годовые потери (Annual Loss Expectancy, ALE) и оценка возврата инвестиций (Return on Investment, ROI). RiskWatch ориентирована на точную количественную оценку соотношения потерь от угроз безопасности и затрат на создание системы защиты. В основе продукта RiskWatch находится метод анализа рисков, которая состоит из четырех этапов.

Первый этап - определение предмета исследования. Здесь описываются такие параметры, как тип организации, состав исследуемой системы (в общих чертах), базовые требования в области безопасности.

Второй этап - ввод данных, описывающих конкретные характеристики системы.

На этом этапе, в частности, подробно описываются ресурсы, потери и классы инцидентов. Классы инцидентов получаются путем сопоставления категории потерь и категории ресурсов.

Для выявления возможных уязвимостей используется вопросник, база которого содержит более 600 вопросов. Вопросы связаны с категориями ресурсов.

Также задается частота возникновения каждой из выделенных угроз, степень уязвимости и ценность ресурсов. Если для выбранного класса угроз в системе есть среднегодовые оценки возникновения (LAFE и SAFE), то используются они. Все это используется в дальнейшем для расчета эффекта от внедрения средств защиты.

Третий этап - количественная оценка риска. На этом этапе рассчитывается профиль рисков, и выбираются меры обеспечения безопасности.

На этом этапе рассчитывается профиль рисков, и выбираются меры обеспечения безопасности. Сначала устанавливаются связи между ресурсами, потерями, угрозами и уязвимостями, выделенными на предыдущих шагах исследования. По сути, риск оценивается с помощью математического ожидания потерь за год.

Формулы (1) и (2) показывают варианты расчета показателя ALE:

$$ALE = AssetValue \times ExposureFactor \times Frequency \quad (1)$$

где:

- Asset Value - стоимость рассматриваемого актива (данных, программ, аппаратуры и т.д.);
- Exposure Factor - коэффициент воздействия - показывает, какая часть (в процентах) от стоимости актива, подвергается риску;
- Frequency - частота возникновения нежелательного события;
- ALE - это оценка ожидаемых годовых потерь для одного конкретного актива от реализации одной угрозы.

Когда все активы и воздействия идентифицированы и собраны вместе, то появляется возможность оценить общий риск для ИС, как сумму всех частных значений.

Можно ввести показатели "ожидаемая годовая частота происшествия" (Annualized Rate of Occurrence - ARO) и "ожидаемый единичный ущерб" (Single Loss Expectancy - SLE), который может рассчитываться как разница первоначальной стоимости актива и его остаточной стоимости после происшествия (хотя подобный способ оценки применим не во всех случаях, например, он не подходит для оценки рисков, связанных с нарушением конфиденциальности информации). Тогда, для отдельно взятого сочетания угроза-ресурс применима формула (2):

$$ALE = ARO \times SLE \quad (2)$$

Дополнительно рассматриваются сценарии "что, если", которые позволяют описать аналогичные

ситуации при условии внедрения средств защиты. Сравнивая ожидаемые потери при условии внедрения защитных мер и без них можно оценить эффект от таких мероприятий.

RiskWatch включает в себя базы с оценками LAFE и SAFE, а также с обобщенным описанием различных типов средств защиты.

Эффект от внедрения средств защиты количественно описывается с помощью показателя ROI (Return on Investment - возврат инвестиций), который показывает отдачу от сделанных инвестиций за определенный период времени. Рассчитывается он по формуле:

$$ROI = \sum_i NVP\left(Benefits_i\right) - \sum_j NVP\left(Costs_j\right) \quad (3)$$

где:

- $Costs_j$ - затраты на внедрение и поддержание j -меры защиты;
- $Benefits_i$ - оценка той пользы (т.е. ожидаемого снижения потерь), которую приносит внедрение данной меры защиты;
- NPV (Net Present Value) - чистая текущая стоимость.

Четвертый этап - генерация отчетов.

Таким образом, рассматриваемое средство позволяет оценить не только те риски, которые сейчас существуют у предприятия, но и ту выгоду, которую может принести внедрение физических, технических, программных и прочих средств и механизмов защиты. Подготовленные отчеты и графики дают материал, достаточный для принятия решений об изменении системы обеспечения безопасности предприятия.

При использовании частного, если организация сохраняет контроль над данными и физическими компонентами системы данная методика не нуждается во внесении поправок на облачную природу.

Если организация не имеет контроля над оборудованием, то невозможно использовать ни один из стандартных сценариев данной модели, ни одна из стадий исследования не может быть правильно проведенна, т.е., модель не может быть использована без внесения ряда поправок.

Однако остается возможность использовать в анализе данные провайдера и использовать модель без корректировок.

Из недостатков следует отметить:

- Такой метод подходит, если требуется провести анализ рисков на программно-техническом уровне защиты, без учета организационных и административных факторов. Полученные оценки рисков (математическое ожидание потерь) далеко не исчерпывают понимание риска с системных позиций — метод не учитывает комплексный подход к информационной безопасности.
- ПО RiskWatch существует только на английском языке.
- Высокая стоимость лицензии.

Заключение

Важно сказать, что ни одна из моделей полностью не подходит для случая облачных вычислений. Т.к. не в одной из них не учитываются специфика модели взаимодействия, присущая облачным средам. В случаи использования частного облака, рассмотренные модели могут быть использованы для управления риском с внесением ряда поправок.

Однако, если частное облако находится в собственности организации и физически существует внутри ее юрисдикции, то возможно абстрагироваться от идеи облака и считать что фирма его не использует. При использовании частного облака, можно считать клиентом работников организации, а ее саму провайдером услуг.

Также они могут служить базисом для создания новой модели, способной удовлетворить возникшую потребность.

Список литературы

1. “Risk Management in Cloud Computing” By Sri Prakash, Technology Risk Management Consultant, E-Com Canada Inc. Fri, April 15, 2011.
2. “The future of IT outsourcing and cloud computing” PwC study, November, 2011.
3. http://csrc.nist.gov/groups/SNS/cloud-computing/
4. Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, Joint Task Force Transformation Initiative, NIST Special Publication 800-37, Revision 1, <URL: http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-l.pdf>.
5. Steve Elky. An Introduction to Information System Risk Management -SANS Institute, 2007.