СРАВНИТЕЛЬНЫЙ АНАЛИЗ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Б. Е. Кубеев

Узбекистан, Ташкент

Одной из актуальных проблем информатизации общества является защита информации, а также возможность анализа и прогнозирования рисков и угроз, которые могут повлиять на целостность информации в корпоративных системах.

Для помощи в организации защитных мер и были созданы интеллектуальные системы защиты информации (ИСЗИ), Эти системы позволяют с высокой степенью вероятности прогнозировать возможные риски и угрозы.

Разработанные на сегодняшний день такие системы как CRAMM (Великобритания), RiskWatch (США),

ГРИФ (Россия) - это инструменты, позволяющие помимо анализа рисков, решать также и ряд других аудиторских задач, включая:

- проведение обследования ИС и выпуск сопроводительной документации на всех этапах его проведения;

- разработка политики безопасности и плана обеспечения непрерывности бизнеса.

В основе метода *CRAMM* лежит комплексный подход к оценке рисков, сочетая количественные и качественные методы анализа. Метод является универсальным и подходит как для больших, так и для мелких организаций, как правительственного, так и коммерческого сектора.

CRAMM разделяет всю процедуру на три последовательных этапа:

Задачей первого этапа является ответ на вопрос: «Достаточно ли для защиты системы применения средств базового уровня, реализующих традиционные функции безопасности, или необходимо проведение более детального анализа?»

На втором этапе производится идентификация рисков и оценивается их величина. На третьем этапе решается вопрос о выборе адекватных контрмер.

К недостаткам метода CRAMM можно отнести следующие:

- использование метода CRAMM требует специальной подготовки и высокой квалификации аудитора;

- CRAMM в гораздо большей степени подходит для аудита уже существующих ИС, находящихся на стадии эксплуатации, нежели чем для ИС, находящихся на стадии разработки;

- аудит по методу CRAMM - процесс достаточно трудоемкий и может потребовать месяцев непрерывной работы аудитора;

- программный инструментарий CRAMM генерирует большое количество бумажной документации, которая не всегда оказывается полезной на практике.

В методе *RiskWatch* в качестве критериев для оценки и управления рисками используются предсказание годовых потерь (Annual Loss Expectancy, ALE) и оценка возврата от инвестиций (Return on Investment, ROI).

RiskWatch помогает провести анализ рисков и сделать обоснованный выбор мер и средств защиты. В отличие от CRAMM, программа RiskWatch более ориентирована на точную количественную оценку соотношения потерь от угроз безопасности и затрат на создание системы защиты.

Используемая в программе методика включает в себя 4 фазы:

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 подробно описываются ресурсы, потери и классы инцидентов. Классы инцидентов получаются путем сопоставления категории потерь и категории ресурсов.

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

Четвертый этап - генерация отчетов.

Некоторые недостатки RiskWatch:

- этот 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 исчерпывает понимание риска с системных позиций - метод не учитывает комплексный подход к информационной безопасности.

ГРИФ - комплексная система анализа и управления рисками информационной системы компании. Данная система решает следующие задачи:

- анализирует уровень защищенности всех ценных ресурсов компании;

- оценивает возможный ущерб, который понесет компания в результате реализации угроз информационной безопасности;

- позволяет эффективно управлять рисками при помощи выбора контрмер, наиболее оптимальных по соотношению цена/качество.

Система ГРИФ предоставляет возможность проводить анализ рисков информационной системы при помощи анализа модели информационных потоков, а также, анализируя модель угроз и уязвимостей - в зависимости от того, какими исходными данными располагает пользователь, а также от того, какие данные интересуют пользователя на выходе.

Вся работа делиться на следующие этапы:

На первом этапе метода ГРИФ проводится опрос ИТ-менеджера с целью определения полного списка информационных ресурсов, представляющих ценность для компании.

На втором этапе проводится опрос ИТ-менеджера с целью ввода в систему ГРИФ всех видов информации, представляющей ценность для компании. Введенные группы ценной информации должны быть размещены пользователем на указанных в предыдущем этапе объектах хранения информации (серверах, рабочих станциях и т.д.). Заключительная фаза – указание ущерба по каждой группе ценной информации, расположенной на соответствующих ресурсах, по всем видам угроз.

На третьем этапе вначале проходит определение всех видов пользовательских групп (и число пользователей в каждой группе). Затем определяется, к каким группам информации на ресурсах имеет доступ каждая из групп пользователей. В заключение определяются виды (локальный и/или удаленный) и права (чтение, запись, удаление) доступа пользователей ко всем ресурсам, содержащих ценную информацию.

На четвертом этапе проводится опрос ИТ-менеджера для определения средств защиты информации, которыми защищена ценная информация на ресурсах. Кроме того, в систему вводится информация о разовых затратах на приобретение всех применяющихся средств защиты информации и ежегодные затраты на их техническую поддержку, а также - ежегодные затраты на сопровождение системы информационной безопасности компании

На завершающем этапе пользователь должен ответить на список вопросов по политике безопасности, реализованной в системе, что позволяет оценить реальный уровень защищенности системы и детализировать оценки рисков.

Отчет представляет собой подробный, дающий полную картину возможного ущерба от инцидентов документ, готовый для представления руководству компании.

Исходя из вышеизложенного можно сделать вывод, что каждая из существующих ИСЗО имеет существенные недостатки и не является универсальной системой защиты информации. Одним из способов повышения качества ИСЗО является применение

методик, в основе которых лежит теория нечетких множеств, а также использование данных систем в совокупности с комплексом всех мер по защите информации.