ВОПРОСЫ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Атаманов Александр Николаевич,
Соискатель, Национальный исследовательский ядерный университет «МИФИ»
05.13.19
silence@rbcmail.ru

Аннотация: *Рассматриваются проблемы оценки рисков информационной безопасности при построении комплексных систем защиты информации. Описываются основные понятия в данной области и делаются выводы о необходимости разработки новых подходов динамической итеративной оценки рисков.*

Ключевые слова: информационная безопасность, анализ рисков, непрерывный аудит, аудит информационной безопасности.

ON SOME ISSUES OF INFORMATION SECURITY RISK ASSESSMENT IN HETEROGENEOUS AUTOMATED SYSTEMS

Atamanov Alexandr Nikolaevich
Applicant, National Research Nuclear University «MEPhI»

Summary: *Some issues of information security risk assessment are considered in the paper. It states basic concepts in the field and draws a conclusion on the neccessarity of dynamic iterative security risk assessment.*

Keywords: risk analysis, information security risk assessment, information security, information security auditing.

Под информационной безопасностью понимается «состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность (т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней), целостность и доступность информации…» [1]. В связи с этим, защита информации представляет собой деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. Иными словами, защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- соблюдение конфиденциальности информации ограниченного доступа;
- реализацию права на доступ к информации [2].

Таким образом, защита информации представляет собой процесс, направленный на достижение состояния информационной безопасности. При этом, учитывая количество и качество задач, решение которых необходимо для достижения требуемого состояния, а так же бурное развитие технологий, задачи управления системой информационной безопасности является весьма сложной. На сегодняшний день сформировано несколько подходов к решению этой задачи. Общей идеей всех из них является комплексность, а так же необходимость процедур анализа угроз и рисков в ходе создания и/или поддержки системы информационной безопасности.

Вопрос анализа рисков информационной безопасности, как составной части комплексного подхода к обеспечению информационной безопасности, достаточно широко освещен в целом ряде международных стандартов. При этом основное внимание уделяется организационным вопросам проведения процедуры.

Ряд отдельных методологий, используемых в практике работы аудиторов и специалистов по безопасности, а так же инструментальных средств позволяют проводить количественную оценку рисков. Создан так же целый ряд программных комплексов, позволяющий автоматизировать отдельные этапы работы специалиста. Тем не менее, средства автоматизации, как правило, ориентированы на поддержку качественного анализа рисков и выполнение организационных требований стандартов, и применение количественного анализа рисков для технических рисков. Общими недостатком всех рассмотренных продуктов являются:

- требуется построение модели автоматизированной системы (в большей или меньшей степени);
- процесс анализа рисков не является итеративным – не обеспечена возможность для уточнения оценок рисков, полученных на предыдущих этапах;
- не предусмотрены средства для агрегации качественных и количественных оценок, что усложняет использование результатов анализа для решения задач управления;
- использование количественных методов оценки рисков не учитывает требований работы с неточными данными или в условиях недостатка данных;
- не предусмотрено возможностей обучения системы.

Таким образом, совершенствование методик проведения анализа рисков информационной безопасности систем является актуальной задачей.

В условиях увеличивающейся сложности автоматизированных систем, вопросы обеспечения информационной безопасности приобретают все большее значение для государства и бизнеса. Особое внимание начинает уделяться анализу рисков информационной безопасности, как необходимой составляющей комплексного подхода к обеспечению информационной безопасности.

Как следствие большого количества стандартов и подходов, основные понятия и определения в этой области характеризуются множественностью. Наиболее подходящим для большинства практических применений определением риска информационной безопасности является данное в стандарте ISO 27005 и стандарте BS7799. Согласно ISO 27005 «риск информационной безопасности – это потенциальная возможность использования уязвимостей актива или группы активов конкретной угрозой для причинения ущерба организации». Из этого определения следует, что риск это комплексная величина, определяемая как функция (или функционал) ряда других величин. Трудности проведения анализа рисков непосредственно вытекают из трудностей и ошибок при анализе составляющих риска. Помимо организационных, можно выделить следующие основные вопросы:

- заведомая неполнота информации о составляющих риска и их неоднозначные свойства;
- создание модели информационной системы;
- длительность процесса и быстрая потеря актуальности результатов оценки;
- агрегация данных из различных источников – в том числе статистик и экспертных оценок;
- необходимость привлечения отдельных специалистов по анализу рисков.

В связи с этим, особую актуальность представляют активно развивающаяся методы непрерывного аудита и анализа рисков информационной безопасности. Совместно с современными моделями управления информационными системами, системами менеджмента информационной безопасности, мониторинга и анализа защищенности, данные методологии позволяют наиболее быстро и эффективно строить и развивать систему защиты информации организации. Система непрерывного

динамического аудита и анализа рисков позволяет специалистам проводить итеративную оценку рисков с учетом имеющихся данных по бизнес-ландшафту, актуальной информации по используемым или предполагаемым к внедрению технологиям, имеющимся или возможным уязвимостям и их вероятностям.

Особую роль в непрерывном анализе рисков при этом должна занимать функция прогнозирования рисков, связанных с планируемыми к внедрению технологиями. Путем автоматизации процесса учета угроз, связанных с появлением новых уязвимостей в типовом ПО, формализации изменений в бизнес-ландшафте и информационной системе, агрегации данных из различных источников можно создать среду, позволяющую специалисту создавать отчеты о состоянии защищенности той или иной информационной системы, основываясь на серии последовательных отчетов, составленных за короткий промежуток времени. Обработка этих данных с использованием методов статистического прогнозирования позволит определить оптимальный набор контрмер с учетом «будущих рисков» и тем самым повысить эффективность внедрения превентивных контрмер и существенно снизить время реакции системы на появление новых уязвимостей [3].

Таким образом, необходимо синтезировать подход к получению количественной оценки и управлению рисками информационной безопасности в автоматизированной системе, учитывая:

- возможность агрегации разнородных данных;
- возможность обучения в процессе работы и уточнения оценок, полученных на предыдущих этапах;
- возможность работы с заведомо неточными данными;
- возможность автоматизации большинства процессов принятия решений.

Для создания такой среды необходимо построение модели автоматизированной системы, что само по себе является сложной задачей, требующей, как правило, существенных упрощений.

В целях решения данных задач необходимо синтезировать автоматическую систему, позволяющую полностью или частично автоматизировать процесс описания среды функционирования и вывода значений рисков. Подход позволяет существенно повысить уровень защищенности автоматизированной системы за счет динамического итеративного анализа рисков информационной безопасности. Показано, что для реализации данного подхода при оценке вероятности реализации угроз информационной безопасности целесообразно применить байесовский подход.

Список литературы

1. «Специальные требования и рекомендации по защите конфиденциальной информации (СТР -К)», Гостехкомиссия России, 2001 г.
2. Федеральный закон от 27.07.2006 №149-ФЗ (ред. От 06.04.2011, с изм. От 21.07.2011) «Об информации, информационных технологиях и о защите информации».
3. Атаманов А. Н., Минаева Е. В. Мониторинг информационных рисков как средство повышения защищенности информационных систем // В сб. материалов российской научной конференции «Методы и средства обеспечения информационной безопасности». СПб., 2008. С. 97.