УДК 004.942

АВТОМАТИЗИРОВАННАЯ СИСТЕМА УЧЕТА И АНАЛИЗА РИСКОВ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Заболотникова А.Е.,
научные руководители ст. преподаватель каф. ИСТМ Лапина Е.В., доц. каф. ИСТМ Лапина Л.А.
Сибирский федеральный университет

Представлены результаты, обобщающие процедуру анализа рисков системы электронного документооборота. Основой подхода является разработка автоматизированной системы, позволяющей анализироватьвозможные риски и оценивать эффективность внедренных мер по защите информации.

Ключевые слова: *система электронного документооборота, модель композитного документооборота, анализ риска, информационный риск.*

В связи с глобальной информатизацией современного общества широкое распространение получили системы электронного документооборота (СЭД). Задача оценки эффективности проектирования, разработки и внедрения СЭД является одной из самых востребованных и актуальных задач. Обеспечение минимального уровня защиты документооборота достигается с помощью выполнения требований и рекомендаций нормативно-методических документов. Системы анализа угроз и рисков позволяют оценить возможные угрозы системы и выбрать наиболее подходящие меры по их снижению или устранению, что обеспечивает стабильность функционирования СЭД.

Целью работы является создание автоматизированной системы, производящей анализ рисков и получение адекватных оценок защищенности СЭД.

Для достижения цели работы необходимо решить ряд задач:

- определить концепцию построения модели СЭД;
- определить методику оценки ценности ресурсов;
- сформировать базу данных списка угроз и уязвимостей, оценить их характеристики;
- сформировать базу данныхперечня контрмер;
- определить методикуанализа эффективности внедренных контрмер.

Результатом работы автоматизированной системыявляется отчет, в котором отражены анализрисков информационной безопасности СЭД и показателиэффективности внедрения комплекса мероприятий контрмер.

Описание модели СЭД.Анализ рисков информационной безопасности осуществляется с помощью построения модели СЭД. Авторами предлагается использовать концепцию модели на основе композитного документооборота представленную в работе. Главным преимуществом такой модели являются: простота реализации, возможность адаптации к любому типу организации и возможность модификации модели в процессе ее построения.

Для построения критериев эффективности в модели композитного документооборота, информационная система отображается взаимодействием компонентов трех множеств:

- множество участников;
- множество действий участников;
- множество состояний документов.

Для описания множества участников необходимо составить список всех сотрудников, пользователей системы электронного документооборота. Для описания множества состояний необходимо составить подробный список документов и список производимых действий с документами участниками системы документооборота. Все документы разделяются на категории ценности информации, и составляются в соответствующий список по убыванию ценности информации, содержащейся в документе. Основным критерием при определении особой ценности документа является содержание документа. Категория ценности информации выражается многоуровневой шкалой ценности (по убыванию). Благодаря разделению документов на категории ценности модель может быть применена для последующего анализа рисков системы документооборота.

Таким образом, входными данными для автоматизированной системы является следующая информация о СЭД:

- перечень ресурсов с ценной информацией;
- физические связи ресурсов друг с другом;
- отделы, к которым относятся ресурсы;
- виды ценной информации;
- ущерб для каждого вида ценной информации;
- группы пользователей, имеющих доступ к ценной информации и их права доступа;
- средства защиты информации.

Исходя из введенных данных, строится модель СЭД, на основе которой будет проведен анализ защищенности каждого вида информации на ресурсе.

Расчет рисков для угроз информационной безопасности СЭД.Риск реализации угрозы информационной безопасности для каждого вида информации рассчитывается по трем основным угрозам: конфиденциальность, целостность и доступность. Информационные риски системы документооборота рассчитывается по формуле 1:

$$R = P*C, \qquad (1)$$

где R – информационный риск; P – вероятность реализации угрозы; C – ценность документа (ущерб от реализации угрозы).

Ценность информации рассчитывается согласно формуле (2) В.И. Корогодина:

$$V = (P-p) / (1-p), \qquad (2)$$

где V – мера ценности информации; p – вероятность достижения цели до получения информации; P – вероятность достижения цели после получения информации.

Для подсчета ценности документа в денежных единицах, необходимо, ценность V умножить на коэффициент J, который рассчитывается экспериментальным путем по формуле 3:

$$C = V \cdot J, \qquad (3)$$

Задание контрмер. Выбор защитных мер для понижения риска осуществляется в соответствии с ГОСТ Р ИСО/МЭК ТО 13335-4-2007 и ГОСТ Р ИСО 15489-1-2007.

Получение оценки снижения рисков основывается на предположении, что вероятность успешной атаки на укрепленную систему задается соотношением 4:

$$Pnew = Pold*(«Старое\_время» / «Новое\_время»), \quad (4)$$

где Pold – вероятность успешной атаки в базовой (старой) конфигурации; «Старое_время» – ожидаемое время успешной атаки с минимальной длительностью в базовой (старой) конфигурации; «Новое_время» – ожидаемое время успешной атаки с минимальной длительностью в укрепленной (новой) конфигурации.

Алгоритм работы автоматизированной системы. На первом этапе осуществляется ввод исходных данных в систему:

- список ценных информационных ресурсов с указанием ущерба по каждой группе ценной информации, расположенной на соответствующих ресурсах, по трем видам угроз.
- список пользователей информационных ресурсов с указанием прав их доступа.
- перечень средств защиты информации на ресурсах.

На втором этапе формируется модель СЭД с точки зрения информационной безопасности. Далее пользователь имеет возможность задавать контрмеры из перечня имеющихся.

В результате работы алгоритма программа представляет отчет, содержащий данные о:

- инвентаризации и значениях риска для каждого ценного ресурса;
- остаточных рисках;
- эффективности выбранных контрмер.

Автоматизированная система предусматривает возможность отслеживания изменений возможных рисков СЭД во времени и отображение динамики в наглядной форме. Так же предусмотрена возможность пополнения баз данных угроз и защитных контрмер, что усиливает эффективность работы данной системы.