Министерство образования и науки Украины
Национальный аэрокосмический университет им. М.Е. Жуковского
Кафедра компьютерных систем и сетей

Системи защиты информации с детальной разработкой блока оценки рисков

Подготовил студент групи 545-и Гончаров М.С.
Дипломный руководитель ст.пр.к.503 Цуранов М.В.

Цели и задачи

Цель
- разработать блок оценки рисков

Задачи:
- проанализировать методики оценки рисков;
- проанализировать программные реализации оценки рисков;
- разработать блок оценки и выбора ПО для оценки рисков

Оценка рисков

Риски - возможность (вероятность) нанесения ущерба информационным ресурсам, снижения уровня их защищенности.

Оценка информационных рисков

$$R=D \times P(V)$$

где R - информационный риск;
D - критичность актива (убыток)
P (V) - вероятность реализации уязвимости

Критичность - степень влияния информации на эффективность функционирования процессов компании.

Вероятность реализации - возможность осуществления угрозы по направлению к любой системы.

Стандарт ISO/IEC 27001

- Подготовлен для реализации требований по созданию, внедрению, поддержке и постоянному улучшению системы менеджмента информационной безопасности.
- Определяет информационную безопасность как сохранение конфиденциальности, целостности и доступности информации.
- Менеджмент рисков происходит по классической схеме: поиск, классификация, ранжирование, оценка, план по снижению рисков, принятия остаточных рисков и регулярный просмотр рисков.

Стандарт ISO / IEC 27005

- Стандарт обеспечивает рекомендации для менеджмента риском информационной безопасности в организации.
- Стандарт не обеспечивает определенной методологии для менеджмента рисков информационной безопасности.
- Стандарт предназначен для определения в организации подхода к менеджменту рисков.

Классификация методов оценки рисков

Методики оценки рисков	Показатели сравнений												
	характеристика применимости					атрибуты							
		анализ риска			оценка	Подход		анализ		усиление анализа			
	идентификации риска	следствие	вероятностные хар	уровень риска	сравнительная риска	дедуктивный	индуктивный	качественный	количественный	качественный	количественный	экстертная реализация	программная реализации
Мозговой штурм	SA	NA	NA	NA	NA	C	NC	(NC)	C	high	high	+	+
метод Делфи	SA	NA	NA	NA	NA	NC	C	(NC)	C	Low	High	+	-
контрольные листы	SA	NA	NA	NA	NA	(NC)	C	NC	C	high	medium	+	+
метод SWIFT	SA	SA	SA	SA	SA	(NC)	NC	C	C	low	Medium	+	-
Марковский анализ	A	SA	NA	NA	NA	(NC)	C	C	C	high	Medium	+	+

SA – строго применяется. NC – метод не применяется. + – реализуется

NA – не применяется. C – метод применяется. - – не реализуется

A – применяется. () – метод применяется с ограничениями

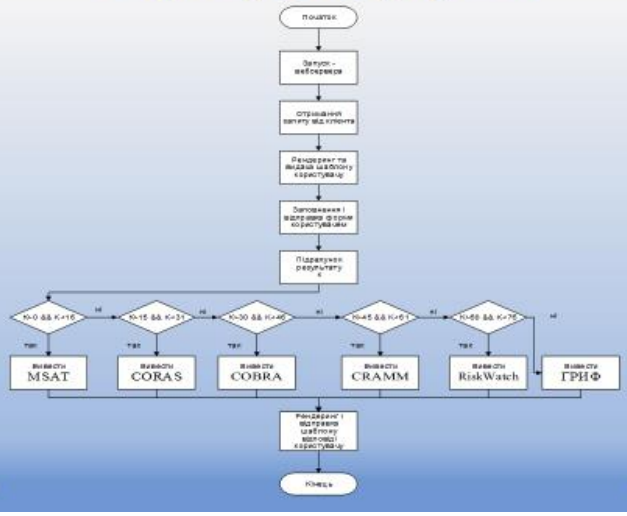
Характеристика программных методик оценки рисков

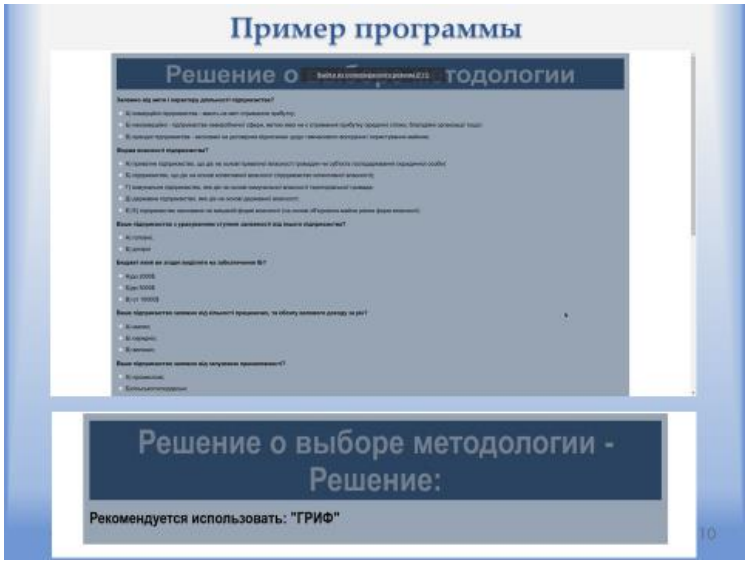
Показатели сравнения	CRAMM	ГРИФ	RiskWatch	COBRA
Риски				
Использование категорий рисков	+	+	+	+
Использование понятия максимально допустимого риска	+	+	+	+
Подготовка плана мероприятий по снижению рисков	+	+	+	-
Управление				
информирование руководителя	+	+	+	+
План работ по снижению рисков	-	+	+	-
Включает проведение тренингов, семинаров, собраний	-	+	+	-
Оценка бизнес-рисков / операционных рисков / ИТ-рисков	-	+	+	+
Оценка рисков на организационном уровне	+	+	-	+
Оценка рисков на техническом уровне	+	+	+	+
Рассматриваемые типы рисков				
Бизнес-риски	-	+	+	+
Риски, связанные с нарушением законодательных актов	-	+	-	-
Риски, связанные с использованием технологий	-	+	-	+
коммерческие риски	+	+	+	+
Риски, связанные с привлечением третьих лиц	+	+	+	+
Риски, связанные с привлечением персонала	+	+	-	+

Характеристика программных методик оценки рисков

Показатели сравнения	CRAMM	ГРИФ	RiskWatch	COBRA
Риски				
Расчет оптимального баланса между различными типами мер безопасности, такими как:				
меры предосторожности	-	+	+	-
мероприятия по выявлению	-	+	+	-
Меры по исправлению	-	+	+	-
Мероприятия по восстановлению	-	+	+	-
Интеграция способов управления	-	+	-	-
Описание назначения способов управления	-	+	+	+
Процедура принятия окончательных рисков	+	+	-	-
Управление остаточными рисками	-	+	-	-
мониторинг рисков	-	+	+	+
Применение мониторинга эффективности мер ИБ	-	+	+	-
Проведение мероприятий по снижению рисков	-	-	+	+
Использование процесса реагирования на инциденты в области ИБ	-	+	-	-
Структурированное документирование результатов оценок рисков	-	+	+	-

Алгоритм роботы программы





Вывод

В результате дипломной работы было проведено:

- анализ методик оценки рисков;
- анализ программной реализации методик оценки рисков;
- разборку блока оценки риска.

11