Разработка программного комплекса оценки информационной безопасности распределенной информационной системы

Выполнил:
студент группы ИБС-141
Шапкин Илья

Научный руководитель:
к.т.н., доцент, зав каф ИБ
Максимова Е.А.

Цель: Повышение уровня информационной безопасности распределенной информационной системы

Задачи:

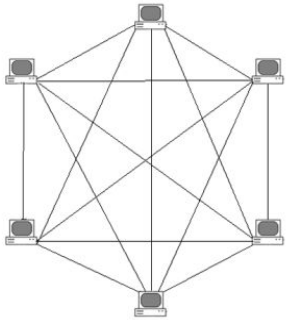
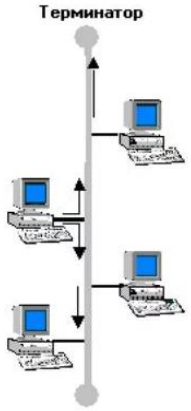
1) Анализ видов информационных систем.
2) Анализ нормативно-правовой базы для оценки информационной безопасности распределенной информационной системы.
3) Анализ оценки информационной безопасности распределенной информационной системы.
4) Анализ методов оценки информационной безопасности распределенной информационной системы.
5) Анализ программных комплексов оценки информационной безопасности распределенной информационной системы.
6) Анализ процедуры оценки информационной безопасности распределенной информационной системы.
7) Разработка формализованной модели оценки информационной безопасности распределенной информационной системы.
8) Разработка архитектуры программного комплекса для оценки информационной безопасности распределенной информационной системы.
9) Разработка пользовательского интерфейса программного комплекса оценки информационной безопасности распределенной системы.
10) Разработка блок-схем алгоритмов программного комплекса для оценки информационной безопасности распределенной информационной системы.
11) Составление плана проведения экспериментального исследования программного комплекса.
12) Экспериментальное исследование программного комплекса.
13) Анализ результатов экспериментальных исследований

Анализ видов информационных систем

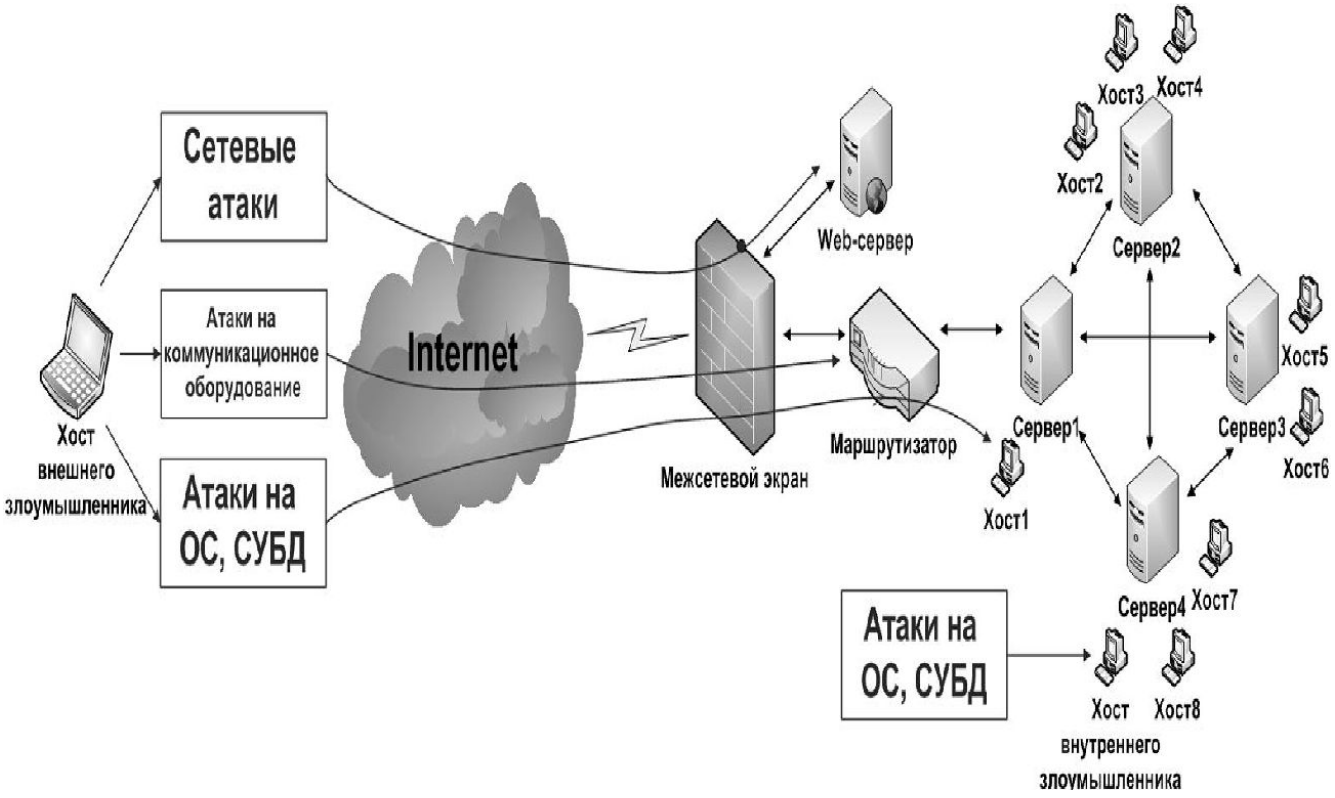
Виды топологий распределенных информационных систем

Тип	Схема	Описание
Звезда		При использовании топологии «звезда», информации между компонентами РИС передается через единый центральный узел. Центральным узлом может быть сервер или специальное устройство - концентратор(Hub)
Кольцо		С кольцевой топологией все компьютеры подключены к замкнутой кольцевой линии. Информация передается по кольцу в одном направлении и должна пройти через каждый компьютер.Передача информации в такой сети происходит следующим образом. Маркер (Специальный сигнал) передается последовательно, с одного компьютера на другой, до тех пор, пока не будет получен тем, на который вы хотите перенести данные. После получения символа, компьютер создает так называемый 'пакет', в который это помещает адрес получателя и данные, и затем посылает эту пачку по кольцу

Виды топологий распределенных информационных систем

Тип	Схема	Описание
Полносвязная		Топология РИС, в которой каждая рабочая станция подключена ко всем остальным. Этот вариант громоздок и неэффективен, несмотря на свою логическую простоту. Для каждой пары должна быть выделена независимая линия, каждый компьютер должен иметь столько портов связи, сколько компьютеров в сети.
Шина		Общая топология типа шины - это общий кабель (называемый шиной или магистралью), к которому подключены все рабочие станции. На концах кабеля находятся терминаторы, для предотвращения отражения сигнала.

Модель распределенной информационной системы



Анализ злоумышленных воздействий на распределенные информационные системы

Компонент РИС	Угрозы	Последствия (риск)
Web-сервер	− возможность перехвата и модификации трафика − эксплуатация уязвимостей шифрования или аутентификации; − эксплуатация уязвимостей сетевых протоколов; − сканирование сети; − DDos и Dos-атаки; − подмена трафика;	Потеря данных Нарушение доступности сервисов Нарушение целостности данных Прерывание бизнес процесса Утечка информации Финансовые потери Проблемы с регуляторами Потеря репутации
СУБД, БД	− format string; − угрозы выявления паролей; − переполнение буфера; − повышение привилегий внутри СУБД; − PL/SQL инъекции; − несанкционированный доступ к данным и журналам транзакций; − уничтожение и нарушение целостности данных и журналов транзакций;	Нарушение доступности Нарушение целостности Утечка данных Прерывание бизнес-процесса Потеря репутации

Анализ злоумышленных воздействий на распределенные информационные системы

Компонент РИС	Угрозы	Последствия (риск)
ОС	– программные уязвимости ОС; – слабые пароли ОС; – небезопасные настройки и ошибки в конфигурации ОС; – вредоносное ПО; – недокументированные возможности; – переполнение буфера; – повышение привилегий и получение административного доступа;	Нарушение доступности Нарушение целостности Прерывание бизнес процесса
Компоненты представлений и приложений	– эксплуатация уязвимостей веб-приложений (XSS, XSRF, SQL Injection, Response Splitting, Code Execution); – переполнения буфера и format string в веб-серверах и application-серверах (к примеру, SAP IGS, SAP Netweaver, Oracle BEA Weblogic); – небезопасные привилегии на доступ (SAP Netweaver, SAP CRM, Oracle E-Business Suite);	Нарушение доступности Нарушение целостности Утечка данных Финансовые потери Проблемы с регуляторами Потеря репутации

Анализ нормативно-правовой базы для оценки информационной безопасности распределенных информационных систем

Документ	Название	Описание
ГОСТ Р ИСО/МЭК ТО 13335-3-2007	Информационная технология. Методы и средства обеспечения безопасности. Методы менеджмента безопасности информационных технологи	Настоящий стандарт устанавливает методы оценки информационной безопасности информационных технологий. В основе этих методов лежат общие принципы, установленные в ИСО/МЭК 13335-1.
ГОСТ Р ИСО/МЭК 15408-1-2008	Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Введение и общая модель	Настоящий стандарт предназначен для использования в качестве основы при оценке характеристик безопасности систем информационных технологий (ИТ). Устанавливая общую базу критериев, стандарт позволяет сделать результаты оценки информационной безопасности значимыми для более широкой аудитории.
СТО БР ИББС–1.1–2007	Практические правила управления ИБ	В данном ГОСТе были проанализированы и изучены меры безопасности при проведении аудита ИБ (п12.3).
ГОСТ Р ИСО/МЭК 27007–2014	ИТ. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента ИБ	Настоящий стандарт предоставляет руководство по менеджменту программы аудита (СМИБ) и проведению внутренних или внешних аудитов.
ГОСТ Р ИСО 19011–2012	Руководящие указания по аудиту систем менеджмента	Настоящий стандарт предназначен для широкого круга потенциальных пользователей, включающих в себя аудиторов ИБ, и т.д. При этом пользователи настоящего стандарта могут применять настоящие руководящие указания при разработке своих собственных требований, относящихся к аудиту.

Анализ оценки информационной безопасности распределенных информационных систем

Анализ методов оценки информационной безопасности распределенной информационной системы

Критерии / Метод	Метод оценки по эталону	Риск–ориентированный метод оценки	Метод оценки по экономическим показателям
Учет механизмов защиты	0	1	0
Учет угроз	0	1	0
Учет капитала предприятия	1	1	1
Учет ценности активов ИС	0	1	1
Рекомендации по повышению оценки	1	1	0
Учет затрат на информационную безопасность	0	0	1
Учет текущего уровня ИБ	0	1	0
Управление рисками ИБ	0	1	0

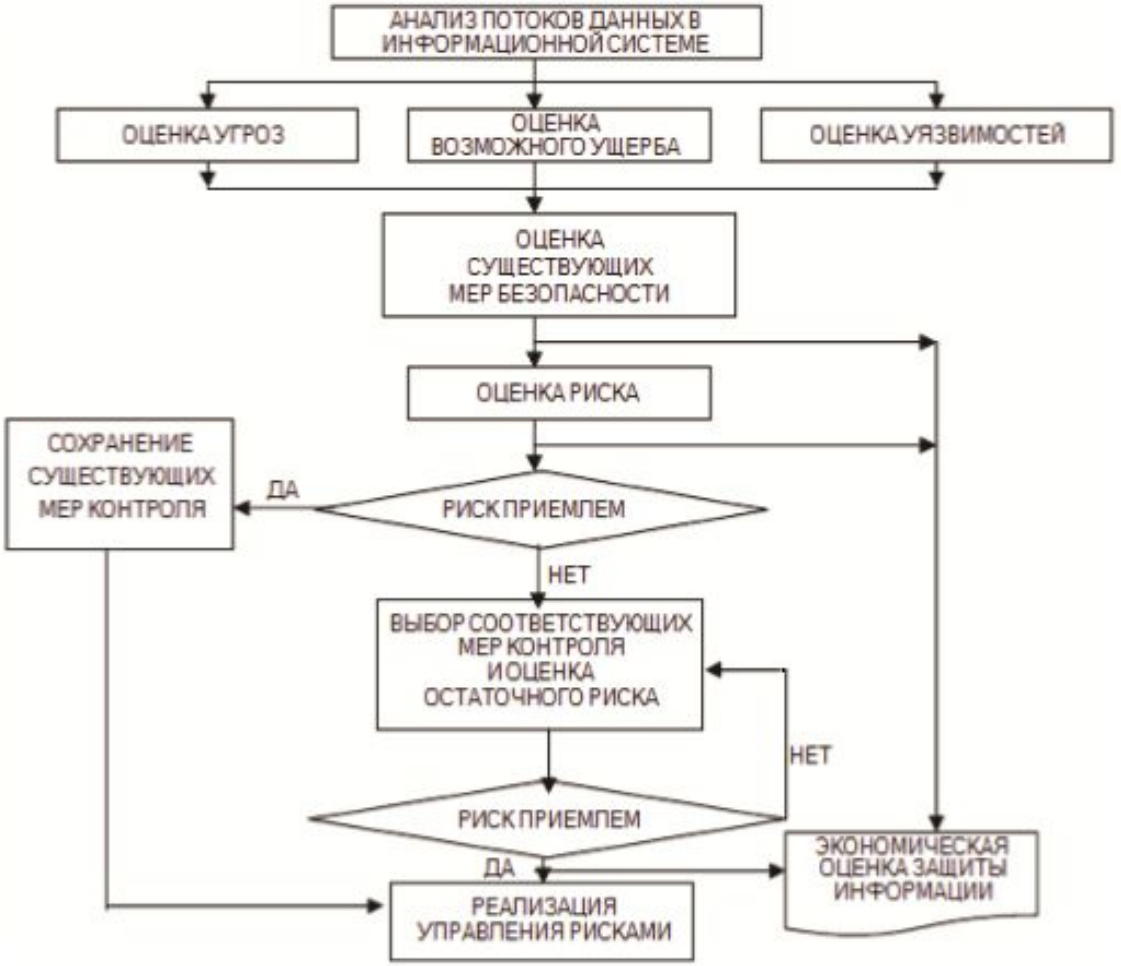
Анализ программных комплексов по ценке информационной безопасности распределенных информационных систем

Критерии / програм.комп	CRAMM	RiskWatch	ГРИФ	CONDOR +
Легкая деятельность для потребителя	Необходима высокая специализированность	Необходима высокая специализированность	Высокая специализированность не требуется	Необходима высокая специализированность
Цена на лицензию, руб	От 60 000	От 300 000	От 30 000	От 12 000
system requirements	ОС Windows 98/Me/NT/2000/XP Свободное дисковое пространство 50 Мбайт Минимальные требования: частота процессора 800 МГц, 64 Мбайт памяти Рекомендуемые требования: частота процессора 1000 МГц, 128 Мбайт памяти	ОС Windows 2000/XP Свободное дисковое пространство для инсталляции 30 Мбайт Процессор Intel Pentium или совместимый, 256 Мбайт памяти	ОС Windows 2000/XP Минимальные требования: свободное дисковое пространство (для диска с данными пользователя) 300 Мбайт, 256 Мбайт памяти Рекомендуемые требования: свободное дисковое пространство (для диска с данными пользователя) 1 Гбайт, 512 Мбайт памяти	ОС Windows 2000/XP Минимальные требования: свободное дисковое пространство (для диска с данными пользователя) 400 Мбайт, 256 Мбайт памяти Рекомендуемые требования: свободное дисковое пространство (для диска с данными пользователя) 1 Гбайт, 512 Мбайт памяти
Support	Присутствует	Присутствует	Присутствует	Присутствует
Количественный/качественный метод	Качественная оценка	Количественная оценка	Качественная и количественная оценки	Качественная и количественная оценки
Сетевое решение	Отсутствует	Отсутствует	Digital Security Office	Digital Security

Анализ программных комплексов по ценке информационной безопасности распределенных информационных систем

Критерии / програм.комп	CRAMM	RiskWatch	ГРИФ	CONDOR +
Набор функций	Вводимые данные: ресурсы; стоимость ресурсов; угрозы; Уязвимость системы; выбор адекватных контрмер. Варианты отчетов: отчет по анализу рисков; общий отчет по анализу рисков; подробный отчет по анализу рисков.	Ввод: Тип информационной системы; основные требования безопасности; ресурсы; потери; угрозы; Уязвимость; меры защиты; стоимость ресурсов; частота возникновения угроз; выбор контрмер. Вариантов отчетов: сводные результаты; отчет о стоимости защищаемых ресурсов и ожидаемых потерь от реализации угроз; отчет об угрозах и мерах противодействия; отчет о рентабельности; отчет о результатах аудита безопасности.	Ввод: ресурсы; сетевое оборудование; типы информации; группа пользователей; средства защиты; угрозы; Уязвимость; выбор контрмер. Состав отчета: инвентаризация ресурсов; риски по видам информации; ресурсные риски; соотношение ущерба и риска информации и ресурсов; отдельные контрмеры; рекомендации экспертов.	Входные данные: объект; пользователь; позиция; разделы; виды информации; группа пользователей; средства защиты; угрозы; Уязвимость; выбор контрмер. Состав отчета: инвентаризация ресурсов; риски по видам информации; ресурсные риски; соотношение ущерба и риска информации и ресурсов; отдельные контрмеры; рекомендации экспертов.

Анализ процедуры оценки информационной безопасности распределенной информационной системы



Разработка формализованной модели оценки информационной безопасности распределенной информационной системы

Риск от k угрозы ИБ в распределенной информационной системе

$$R_k(TR_k, A) = v_k p_k d_k u(TR_k)$$

где A – множество используемых активов, TRk- k угроза из множества угроз TR, v – частота возникновения данной угрозы за фиксированный промежуток времени, p – вероятность успешной реализации угрозы, d – коэффициент разрушительности угрозы.

Ущерб по каждой k угрозе

$$u(TR_k) = \sum_{i=1}^{m} (C(A_i^j) rma_{TRk,Ai})$$

Матрица бинарных отношений между угрозами и активами

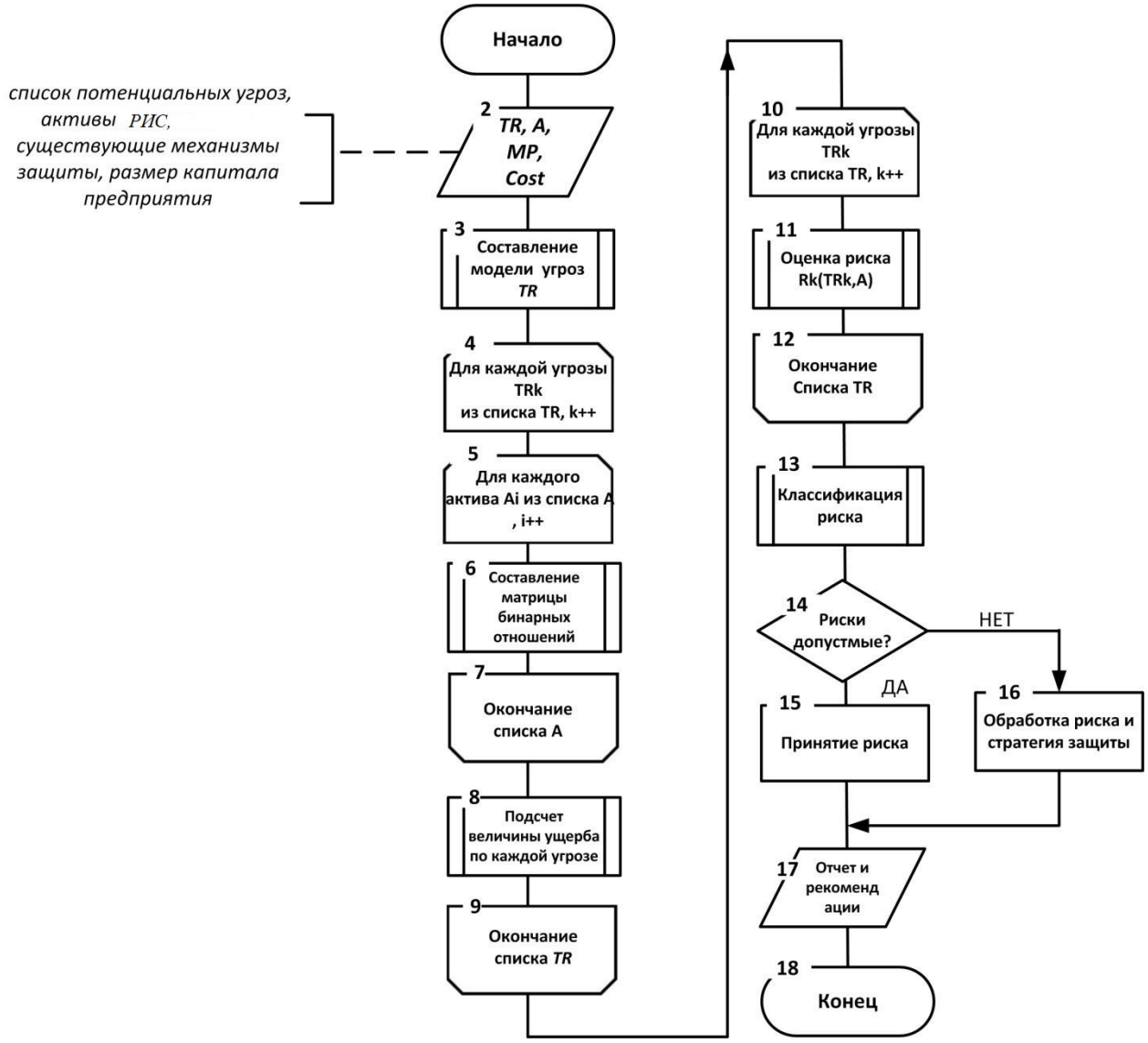
$$\text{RMA} = (\text{rma}_{\text{TR,A}}) = \begin{cases} 1, \text{если для актива A существует угроза TR} \\ 0, \text{если для актива A не существует угроза TR} \end{cases}$$

$C(A_i^j) = \frac{Cost(A_i^j)}{Cost}$ - Ценность актива, где $Cost(A_i^j)$ - стоимость актива

$Cost$ капитал предприятия

Разработка архитектуры программного комплекса оценки информационной безопасности распределенной информационной системы

Блок-схема обобщённого алгоритма оценки ИБ РИС



СПАСИБО ЗА ВНИМАНИЕ!