На правах рукописи

ПОЛИТОВ Михаил Сергеевич

ЭКСПЕРИМЕНТАЛЬНО-АНАЛИТИЧЕСКИЙ МЕТОД ОЦЕНКИ И ПРОГНОЗИРОВАНИЯ УРОВНЯ ЗАЩИЩЁННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ МОДЕЛИ ВРЕМЕННЫХ РЯДОВ

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени кандидата технических наук

Уфа - 2010

Работа выполнена в ГОУ ВПО
«Челябинский государственный университет»
на кафедре вычислительной механики и информационных технологий

Научный руководитель	д-р техн. наук, проф. **МЕЛЬНИКОВ** Андрей Витальевич
Официальные оппоненты	д-р техн. наук, проф. **МИРОНОВ** Валерий Викторович, проф. каф. автоматизированных систем управления Уфимского государственного авиационного технического университета
	канд. техн. наук, **КРУШНЫЙ** Валерий Васильевич, зав. каф. автоматизированных информационных и вычислительных систем Снежинской государственной физико-технической академии
Ведущая организация	ОАО «Государственный ракетный центр имени академика В.П. Макеева»

Защита состоится «26» марта 2010 г. в 10:00 часов

на заседании диссертационного совета Д-212.288.07

при Уфимском государственном авиационном техническом университете

по адресу: 450000, г. Уфа, ул. К. Маркса, 12

С диссертацией можно ознакомиться в библиотеке университета

Автореферат разослан 19 февраля 2010 г.

Ученый секретарь
диссертационного совета
д-р техн. наук, проф. С. С. Валеев

ОБЩАЯ ХАРАКТЕРИСТИКА

Актуальность темы

Современная информационная система (ИС), находящаяся в производственной эксплуатации, включает в себе функции защиты обрабатываемой в ней информации и предотвращения к ней несанкционированного доступа. Однако динамика изменения нарушений защищенности информационных систем свидетельствует о наличии ряда нерешённых задач в области защиты информации ИС, в том числе, при проектировании и эксплуатации средств защиты.

На этапе проектирования системы информационной безопасности ИС необходимо определить требуемый уровень защищённости системы, а на этапе тестирования оценить параметры безопасности аудируемой системы и сопоставить их с начальным заданием по безопасности. Для оценки защищённости системы на этапе тестирования необходимо применение эффективного алгоритме анализа, но на сегодня не существует каких-либо стандартизированных методик объективного анализа защищенности ИС. В каждом конкретном случае алгоритмы действий аудиторов могут существенно различаться, что, в свою очередь, может привести к существенным расхождениям в результатах оценки и неадекватному реагированию на сложившиеся угрозы.

Практикуемые в настоящее время методы исследования защищенности предполагают использование как активного, так и пассивного тестирования системы защиты. Активное тестирование системы защиты заключается в эмуляции действий потенциального злоумышленника по преодолению механизмов защиты. Пассивное тестирование предполагает анализ конфигурации операционной системы и приложений по шаблонам с использованием списков проверки. Тестирование может производиться непосредственно экспертом, либо с использованием специализированных программных средств. При этом возникает проблема выбора и полноты алгоритма анализа, а также сравнения полученных результатов оценки. Для оценки и анализа результатов тестирования различных конфигураций ИС необходима некоторая, абстрагированная от конкретных свойств ИС, единица измерения, с помощью которой можно измерить общий уровень защищённости этих ИС.

Анализ современных методов решения рассматриваемых задач показал, что используются ряд различных подходов. Можно выделить работы С. Као, Л.Ф. Кранор, П. Мела, К. Скарфоне и А. Романовского по проблеме оценки уровня защищённости, С.А. Петренко, С.В. Симонова по построению экономически обоснованных систем обеспечения информационной безопасности, А.В. Мельникова по проблемам анализа защищенности информационных систем, И.В. Котенко по разработке интеллектуальных методов анализа уязвимостей корпоративной вычислительной сети, В.И. Васильева, В.И. Городецкого, О.Б. Макаревича, И.Д. Медведовского, Ю.С. Соломонова, А.А. Шелупанова и др. по проектированию интеллектуальных систем защиты информации. Однако вопросы объективного анализа уровня защищённости ИС и его прогнозирования в этих работах рассмотрены недостаточно глубоко.

Объект исследования

Безопасность и защищённость данных, обрабатываемых в компьютерных информационных системах.

Предмет исследования

Методы и модели оценки уровня защищённости компьютерных информационных систем.

Цель работы

Повышение достоверности оценки уровня защищённости информационных систем на основе накопленных баз данных их уязвимостей и модели временных рядов.

Задачи исследования

Исходя из поставленной цели работы, определен следующий перечень решаемых задач:

1. Выполнить анализ существующих подходов и методов оценки уровня защищённости информационных систем.
2. Разработать модель оценивания уровня защищённости сложных информационных систем относительно заданной точки входа.
3. Разработать метод прогнозирования уровня защищённости информационных систем на основе достоверных знаний о системе.
4. Разработать структурно-функциональную модель уязвимости информационной системы для создания унифицированной базы уязвимостей.
5. Разработать программный прототип системы динамического анализа защищенности корпоративной вычислительной сети с применением техник эвристического анализа уязвимостей.

Методы исследования

При работе над диссертацией использовались методология защиты информации, методы системного анализа, теория множеств, методы теории нечёткой логики, теория вероятностей, теория временных рядов - для разработки концепции построения информационных систем с заранее заданным уровнем защищенности.

Основные научные результаты, выносимые на защиту

1. Модель оценивания уровня защищённости сложных информационных систем относительно заданной точки входа.
2. Метод прогнозирования уровня защищённости информационных систем на основе достоверных знаний о системе и модели временных рядов.
3. Структурно-функциональная и теоретико-множественная модель уязвимости ИС.
4. Реализация программного прототипа системы динамического анализа защищенности корпоративной вычислительной сети с применением техник эвристического анализа уязвимостей.

Научная новизна результатов

1. Предложена модель оценивания защищенности сложных информационных систем на основе разбиения всей системы на подсистемы - блоки со своими характеристиками уровня уязвимости. В рамках предложенной концепции становится возможным создание систем с заранее определёнными характеристиками защищённости, что, в свою очередь, увеличивает надёжность системы в долгосрочной перспективе.

2. Предложен метод оценки уровня защищённости ИС, который в отличие от существующих экспертных оценок, позволяет на основе накопленных мировым сообществом баз данных уязвимостей информационных систем спрогнозировать с использованием модели временных рядов более достоверные результаты.

3. Предложена структурно - функциональная модель уязвимости с использованием теоретико-множественного подхода, позволяющая параметрически описать каждую уязвимость, систематизировать и структурировать имеющиеся данные по уязвимостям с целью создания соответствующих баз для автоматизированных систем аудита.

Обоснованность и достоверность результатов диссертации

Обоснованность результатов, полученных в диссертационной работе, обусловлена корректным применением математического аппарата, апробированных научных положений и методов исследования, согласованием новых результатов с известными теоретическими положениями.

Достоверность полученных результатов и выводов подтверждается численными методами и экспериментальным путем, результатами апробации разработанного программного прототипа для проведения анализа защищенности корпоративной вычислительной сети.

Практическая значимость результатов

Практическая ценность результатов, полученных в диссертации, заключается в разработке:

– формализованной процедуры анализа защищенности сложных систем на основе логического разбиения всей информационной системы на подсистемы-блоки со своими характеристиками уровня защищённости;

– структурно-функциональной (СФМУ/VSFM) и теоретико-множественной модели уязвимости, позволяющих в параметрически описать каждую уязвимость, что, в свою очередь, даёт возможность систематизировать и структурировать имеющиеся данные по всем уязвимостям;

– методов и алгоритмов (в том числе и эвристических) функционирования автоматизированной системы анализа защищенности корпоративной вычислительной сети, подтвердивших высокую эффективность при апробации разработанного программного комплекса в реальных условиях;

Результаты диссертационной работы в виде методов, алгоритмов, методик и программного обеспечения внедрены в корпоративной вычислительной сети Челябинского государственного университета и ООО «ИТ Энигма».

Апробация работы

Основные научные и практические результаты диссертационной работы докладывались и обсуждались на ряде следующих конференций:

– Всероссийской научной конференции «Математика, механика, информатика», Челябинск, 2004, 2006;

– 7-ой и 9-ой Международной научной конференции «Компьютерные науки и информационные технологии» (CSIT), Уфа, 2005, 2007;

– Международной научно-практической конференции студентов, аспирантов и молодых учёных, Екатеринбург, 2006;

– 10-ой Всероссийской научно-практической конференции «Проблемы информационной безопасности государства, общества и личности».

Публикации

Результаты выполненных исследований отражены в 8 публикациях: в 6 научных статьях, в 2 изданиях из списка периодических изданий, рекомендованных ВАК Рособрнадзора, в 2 тезисах докладов в материалах международных и российских конференций.

Структура и объем работы

Диссертация состоит из введения, четырех глав, заключения, библиографического списка из 126 наименований и глоссария, всего на 143 листах.

СОДЕРЖАНИЕ РАБОТЫ

В работе обосновывается актуальность темы диссертационного исследования, сформулированы цель и задачи работы, определены научная новизна и практическая значимость выносимых на защиту результатов.

В работе выполнен анализ состояния проблем автоматизации аудита уровня защищённости информационных систем и повышения объективности самой экспертизы. Определено понятие защищённости информационных систем и проведён анализ основных угроз, влияющих на это свойство. Выявлены ключевые особенности современных информационных систем, оказывающие непосредственное воздействие на такие характеристики, как надёжность и безопасность. Определены основные стандарты и нормативные документы, координирующие действия экспертов в области защиты информации. Дана классификация современных средств защиты, а также их достоинства и недостатки. Проанализированы и обобщены проводимые исследования и международный опыт в области защиты информации. Детально рассмотрена современная реализация процесса анализа защищённости, его этапы, их сильные и слабы стороны, используемые автоматизированные средства аудита с их плюсами и минусами.

Проведённый обзор выявил ряд противоречий и недоработок в обозначенной области исследований. Практически полностью отсутствуют аналитические методы, позволяющие оценить уровень защищённости объекта защиты на этапе проектирования, когда уже понятно из каких блоков будет состоять система. Большинству используемых сегодня методов оценки характерен высокий уровень субъективности, опреде-

ляемый экспертным подходом к оценке уровня защищенности автоматизированной системы. К сожалению динамические алгоритмы анализа текущего состояния уровня защищённости ресурсов вычислительной сети на этапах промышленной эксплуатации не получили пока широкого распространения. Ключевой особенностью данных алгоритмов является то, что они создаются системой «на лету» согласно выявленным свойствам анализируемого объекта, что позволяет обнаруживать неизвестные до сих пор уязвимости и проводить более глубокий аудит компьютерных систем с любой конфигурацией.

В работе проведён анализ трёх основных методик оценки защищённости (модель оценки по Общим Критериям, анализ рисков, модель на основе критериев качества), рассмотрены их ключевые особенности, выявлены преимущества и недостатки предложен новый оригинальный подход к оцениванию уровня защищённости информационных систем.

Недостатками всех этих методик является достаточно высокий уровень абстракции, который в каждом конкретном случае даёт слишком большую свободу в интерпретации предписанных шагов алгоритма анализа и их результатов.

Перечисленные методы исследования предполагают использование как активного, так и пассивного тестирования системы защиты. Тестирование может производиться экспертом самостоятельно, либо с использованием специализированных программных средств. Но здесь возникает проблема выбора и сравнения результатов анализа. Возникает потребность в некоторой, абстрагированной от конкретных свойств системы, шкале, в рамках которой и будет измеряться общий уровень безопасности. Одним из возможных решений этой проблемы является оригинальный метод аналитической оценки и прогнозирования общего уровня защищённости на основе теории временных рядов. Данный метод позволяет оценить уровень защиты отдельных элементов информационной системы.

Введены следующие определения и допущения:

1. Жизненный путь программно-технического средства оцениваться в количестве выпущенных производителем версий и модификаций;
2. Подсчёт количества версий ведётся не по числу реально используемых версий, а исходя из формальной системы образования порядкового номера версии. При этом не учитывается факт существования/отсутствия каждой отдельной.
3. Виды и типы уязвимостей классифицируются следующим образом:
   – *Low* – уязвимости типа «поднятие локальных привилегий», но не до local system;
   – *Midle* – уязвимости, мешающие нормальному функционированию системы и приводящие к возникновению DoS, уязвимости, приводящие к поднятию локальных привилегий до local system;
   – *High* – уязвимости, позволяющие злоумышленнику получить удалённый контроль над системой.
4. Уровень защищённости информационной системы оценивается по отношению общего количества уязвимостей каждого класса к общему количеству версий системы.

Если система имеет несколько целевых узлов, то совокупная уязвимость рассчитывается следующим образом:

$$CISV^{VC} = K_1 \cdot ISV^{VC}{}_1 + K_2 \cdot ISV^{VC}{}_2 + ... + K_i \cdot ISV^{VC}{}_i ,$$

где i – порядковый номер информационной подсистемы;

$CISV^{VC}$ – совокупная уязвимость информационной системы, рассчитанная уязвимостях конкретного класса уязвимости;

$ISV^{VC}{}_i$ – количество уязвимостей i-ой подсистемы каждого класса уязвимостей;

K_i – коэффициент долевого участия важности каждой конкретной системы в общей значимости всей ИТ – инфраструктуры. Измеряется в процентах.

Для оценки совокупной уязвимости информационной системы воспользуемся логическими схемами, представленными ниже:

I. Модель последовательного соединения звеньев системы (см. Рис.1):

$$CISV^{vc} = MIN(ISV^{vc}{}_1, ISV^{vc}{}_2)$$

Для n звеньев при последовательном соединении:

$$CISV^{vc} = \underset{i=1}{\overset{n}{MIN}}(ISV_i^{VC}),$$

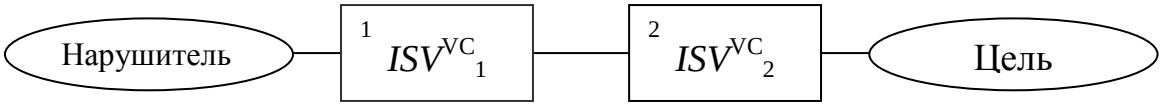

Рисунок 1 – Последовательная логическая схема «Нарушитель-Цель»

II. Модель параллельного соединения звеньев системы (см. Рис.2):

$$CISV^{vc} = MAX(ISV^{vc}{}_1, ISV^{vc}{}_2)$$

Для n звеньев системы при параллельном соединении:

$$CISV^{vc} = \underset{i=1}{\overset{n}{MAX}}(ISV_i^{VC})$$

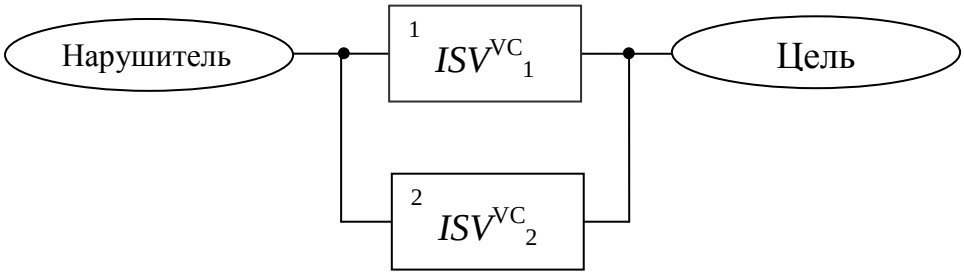

Рисунок 2 – Параллельная логическая схема «Нарушитель-Цель»

Разработанная методика позволяет проектировать системы с заданием по конкретному уровню защищённости, а также сравнить уровни уязвимости объектов защиты между собой. Практическая апробация разработанного метода выполнена на примере web-сервера Apache (см. Рис. 4).

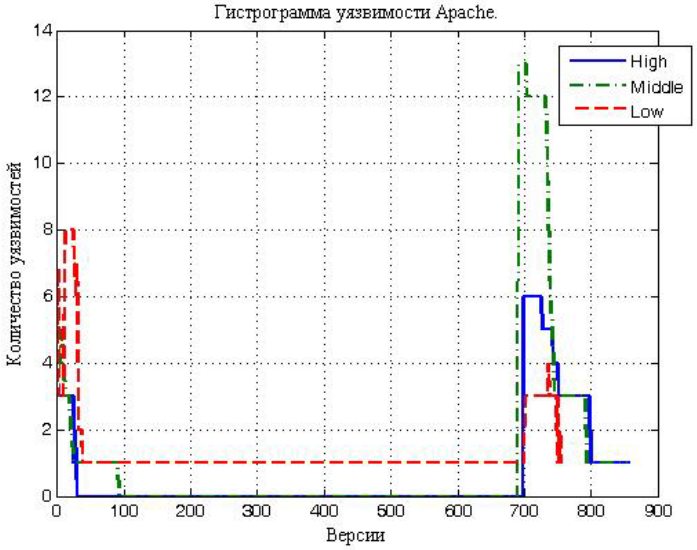

Рисунок 4 – Уровень уязвимости для различных версий web-сервера Apache

Как известно смена основных номеров версий программного продукта связана с существенными изменениями кода и функциональными преобразования. В пределах этих версий идёт доработка уже заложенного функционала и исправление ошибок.

Для прогнозирования числа уязвимостей в будущих версиях web-сервера Apache была применена теория временных рядов и выполнен анализ полученных данных. Как известно, временной ряд есть последовательность измерений выполненных через определенные промежутки времени. В нашем случае шкала версий программного продукта рассматривалась, как шкала времени.

Использовалась, классическая модель временного ряда, состоящая из четырех компонент:

тренда – общей тенденции движения на повышение или понижение;

циклической составляющей – колебания относительно основной тенденции движения;

случайной составляющей – отклонения от хода отклика, определяемого трендовой, циклической и сезонной составляющими. Данная составляющая связана с ошибками измерениями или влияниями случайных величин.

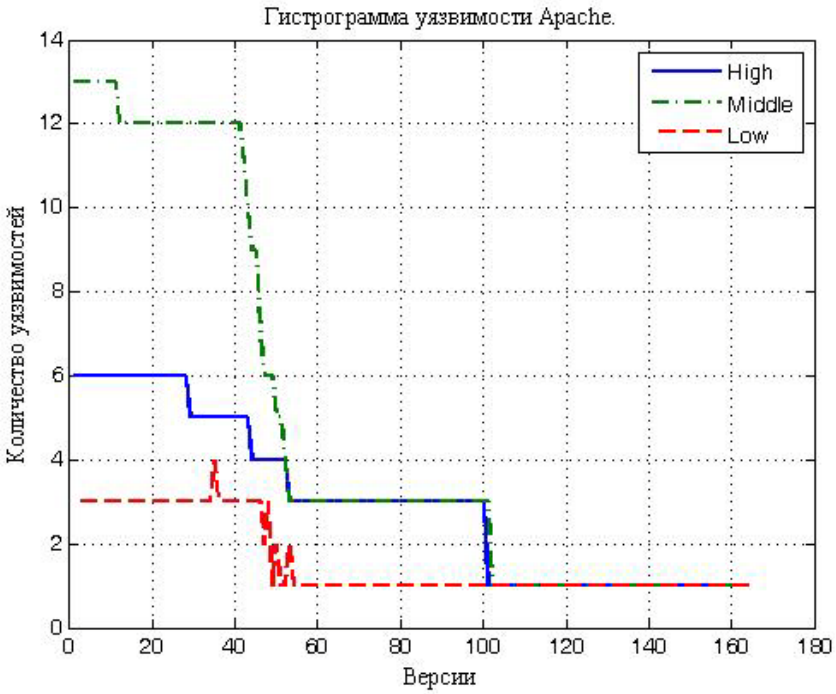

Рисунок 5 – Уязвимость второй версии web-сервера Apache

Известны различные модели регрессионного анализа, позволяющие определить функциональную зависимость трендовой составляющей. Выбран метод, основывающийся на подборе максимального соответствия показателей математической модели показателям моделируемой системы. Анализ опыта таких компаний как General Motors и Kodak, при выборе аппроксимирующей модели позволил выбрать за основу трендовой составляющей степенной закон. Основываясь на типовых элементах процесса для рассматриваемого множества примеров, выбран следующий вид трендовой функции:

$$y(x) = b_0 \cdot b_1{}^x .$$

В ходе исследований были получены следующие формулы трендов временных рядов:

High $y(x) = 7.2218 \cdot 0{,}9873^x$

Middle $y(x) = 16.5603 \cdot 0{,}9807^x$

Low $y(x) = 3.5053 \cdot 0{,}9887^x$

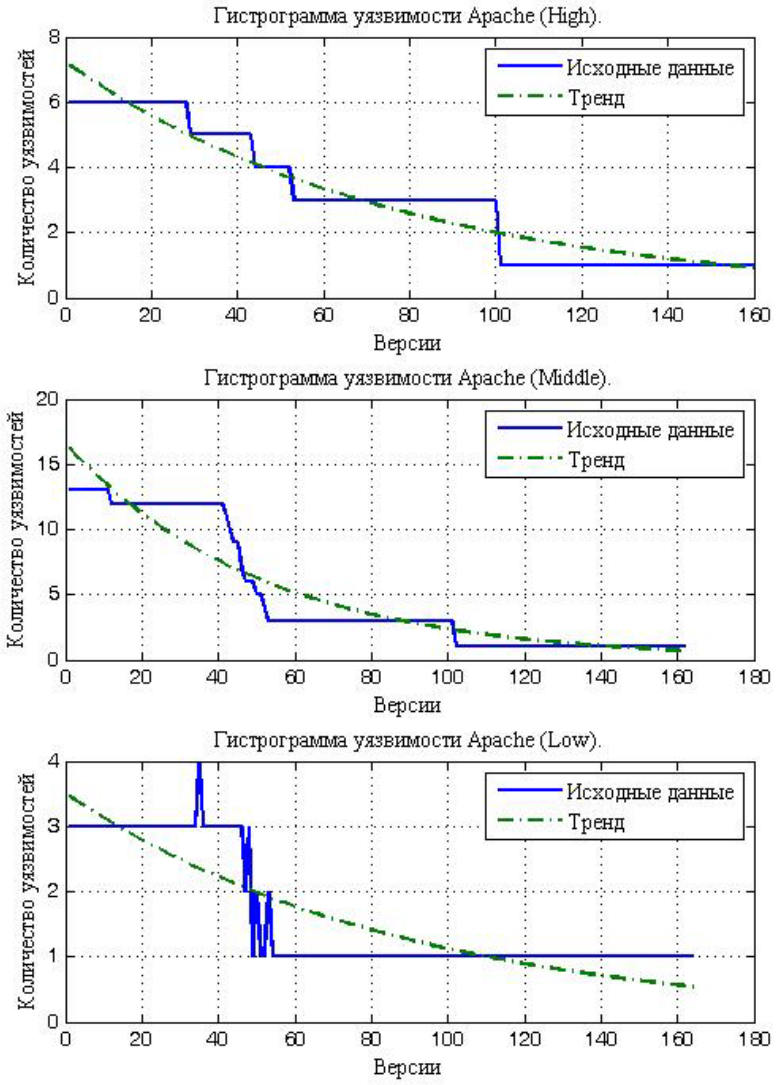

Рисунок 6 – Кривые основного тренда уязвимости в зависимости от версии

Из графика экспериментальных данных (см. Рис. 6) следует, что амплитуда колебаний затухает с течением времени. Для аппроксимации циклической составляющей была выбрана функция следующего вида:

$$y(x) = b_0 \cdot b_1{}^x + d \cdot f^x \cdot \cos(c \cdot x + a)$$

В работе были получены следующие формулы аппроксимирующих функций:

High $y(x) = 7.2218 \cdot 0{,}9873^x - 0.4958 \cdot 0{,}9983^x \cdot \cos(0{,}1021 \cdot x + 0{,}3689).$

Middle $y(x) = 16.5603 \cdot 0{,}9807^x + 1.5442 \cdot 0{,}9955^x \cdot \cos(0{,}1022 \cdot x + 3{,}0289).$ (1)

Low $y(x) = 3.5053 \cdot 0{,}9887^x + 0.3313 \cdot 0{,}9967^x \cdot \cos(0{,}1011 \cdot x + 2.9589).$

Адекватность предлагаемых математических зависимостей исходным данным обоснована на основе критерия Пирсона.

Проверка гипотезы H_0 показала, что исходные временные ряды соответствуют рядам, построенным по функциям (1) (см. Рис. 7) .

Для вычисления статистики Пирсона была использована следующая формула:

$$\chi^2 = N\sum_{i=1}^{k}\frac{(p_i^{emp} - p_i^{teor})^2}{p_i^{teor}},$$

где p_i^{teor}, p_i^{emp} - вероятность попадания уровня уязвимости в i-ый интервал в исходном и теоретическом рядах;

N – суммарное число уязвимостей версий в исходном временном ряду;

k – количество точек временного ряда.

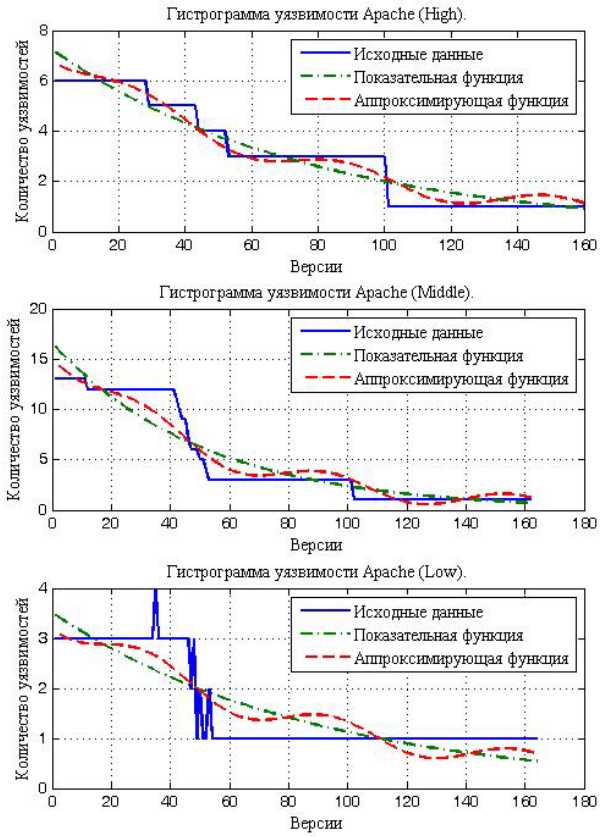

Рисунок 7 – Аппроксимация кривых уязвимостей на базе выбранных функций

В результате были получены следующие значения χ^2 (Таблица 1).

Таблица 1

Класс уязвимости	χ^2
High	10.8327
Middle	37.7546
Low	18.1643

Согласно данной таблицы значений для критерия Пирсона при заданном коли-

честве степеней свободы $k-1=160$ и значении $\alpha=0{,}01$ получаем следующее значение для $\chi^2_{табл}=204.5301$. Так как все $\chi^2<\chi^2_{табл}$, поэтому гипотезы H_0 принимаются на самом минимальном уровне значимости $\alpha=0{,}01$.

Таким образом, отмечается, что для уровня значимости $\alpha=0{,}01$ по критерию согласия Пирсона функциональные зависимости, представленные табличными исходными данными и теоретические (1), соответствуют друг другу.

Для прогнозирования будущих значений предлагается применить полученные функции (1) с учетом номера версии продукта.

Точность предложенного метода оценивается на основе сравнения среднего абсолютного отклонения функции описанного метода и среднего абсолютного отклонения функции на основе экспертного метода. В первом приближении экспертная оценка может быть представлена либо линейной, либо степенной функцией (см. Рис. 7), отражающей основной тренд процесса. Среднее абсолютное отклонение (MAD) рассчитано по следующей формуле:

$$MAD=\frac{\sum_{i=1}^{n}\left|y_i-\tilde{y}_i\right|}{n}$$

где y_i – вычисленное в i-ой точке значение временного ряда ;

$\tilde{y}_i$ – наблюдаемое в i-ой точке значение ряда;

n - количество точек временного ряда.

Таблица 2

	Класс уязвимости	Линейная	Степенная	Степенная функция с циклической составляющей
MAD	*High*	0.5737	0.5250	0.3882
	Middle	2.1398	1.5542	1.0730
	Low	0.5568	0.4630	0.3921

Как видно из Таблицы 2 предложенный в работе метод позволяет получить оценку точнее экспертного оценивания в два раза.

В работе сопоставляются описанный во второй главе аналитический метод оценки и прогнозирования уровня защищённости с технологическими (экспериментальными) методами обнаружения уязвимостей.

Используя информацию о текущем уровне уязвимости информационной системы, полученную в результате обращения к международным базам данных, а также разработанный метод прогнозирования уровня уязвимости на основе теории временных рядов, можно оценить, какое количество уязвимостей каждого класса будет в ней присутствовать. Имея представление о том, сколько возможных уязвимостей в новой версии может быть, и, зная, сколько на текущий момент обнаружено, можно определить возможное количество ещё не выявленных угроз безопасности с помощью следующего выражения:

$$V\Delta = V_f - V_r,$$

где V_f – предполагаемое количество уязвимостей, рассчитанное по методу,

предложенному в работе;

V_r – количество обнаруженных в текущей версии уязвимостей;

$V\Delta$ – число потенциально существующих, но ещё не обнаруженных уязвимостей.

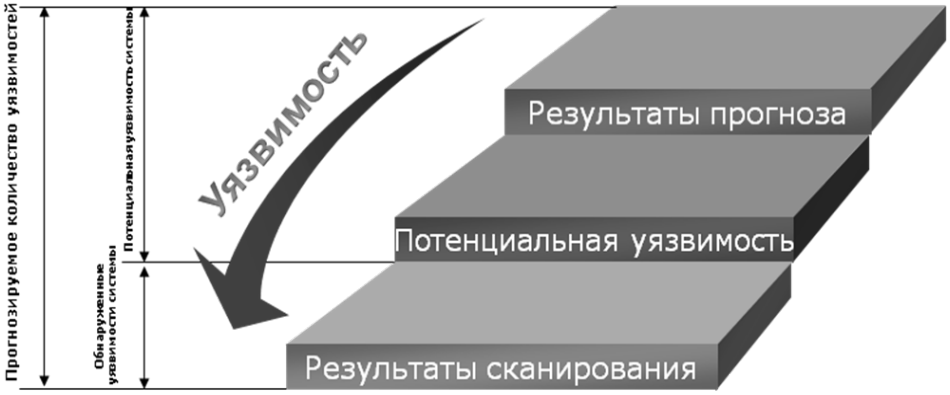

Рисунок 8 – Процесс объединения оценок

Зная величину уровня потенциально существующих $V\Delta$ угроз безопасности (см. Рис. 8), но не зная их локализации в системе (подсистемах), решение задачи обеспечения защиты выглядят неопределённо. Таким образом, возникает задача поиска и обнаружения слабых мест в системе безопасности существующей системы, с учётом всех особенностей её конфигурационных настроек, свойств и характеристик установленного оборудования и программного обеспечения, а также мест возможного проникновения злоумышленников (учет этого в аналитических расчётах трудно реализуем). Из этого делается вывод, что необходима некоторая программно-аппаратная платформа, имеющая эффективные алгоритмы анализа уровня защищённости, что способствует своевременному выявлению новых угроз безопасности. Для создания такой системы необходимо решить задачу системного анализа.

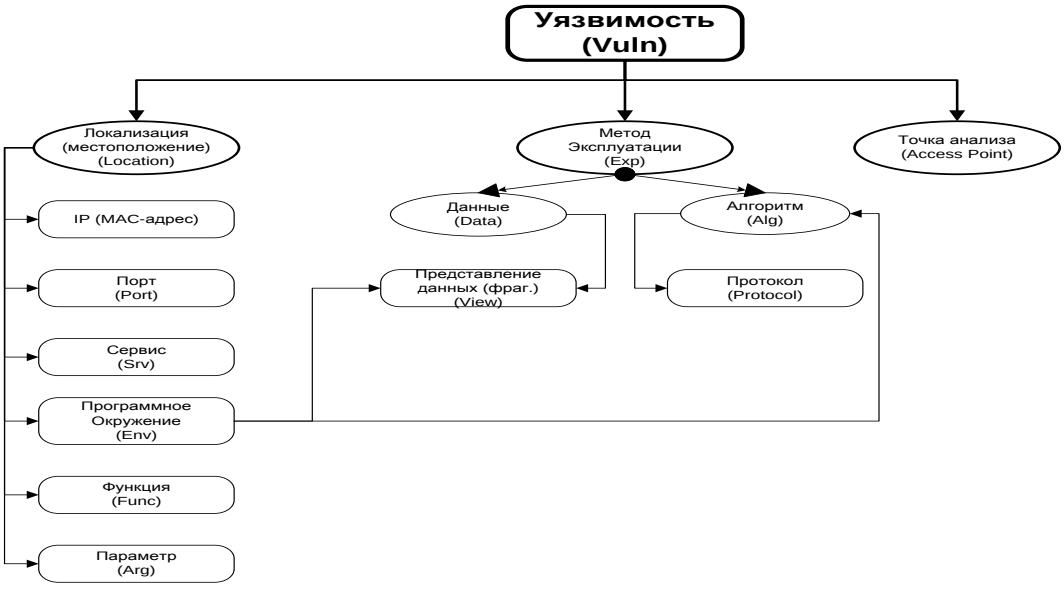

Рисунок 9 – Структурно-функциональная модель уязвимости

Отмечается, что в процессе анализа защищённости ключевую роль играет разработка структурно-функциональной модели уязвимости (см. Рис. 9), на основе которой предлагается четырёхступенчатая технология аудита защищенности компьютерных систем.

На первом этапе (см. Рис. 10) выполняется сканирование портов целевой системы с целью определения точек возможного проникновения через работающие сетевые сервисы.

На втором этапе снимаются отпечатки (*Service-fingerprinting*) с запущенных на открытых портах сервисов и обеспечить их последующую идентификацию вплоть до номера установленной версии.

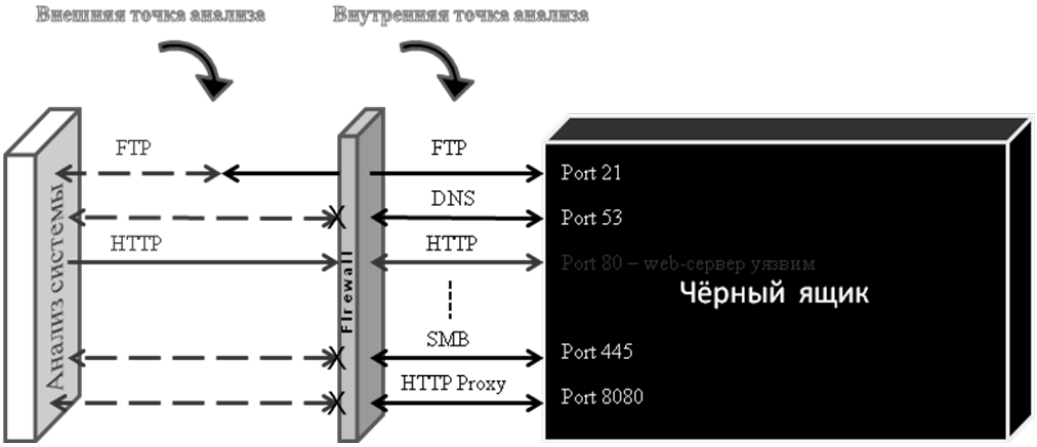

Рисунок 10 – Процесс сканирования информационной системы

На третьем этапе, исходя из уже собранной информации по комбинациям открытых портов, видов и версиях запущенных сервисов, особенностей реализации стеков доступных протоколов, выполняется идентификация операционной системы (OS-*fingerprinting*) вплоть до установленных пакетов комплексных обновлений и патчей.

На четвёртом этапе, имея уже собранную ранее информацию, становится возможным осуществление поиска уязвимостей уровня сети. На данном этапе опорной информацией выступают «слушающие» порт идентифицированные сервисы и определённая на третьем шаге операционная система.

С учетом вышеизложенного предлагаются технологии и методы технического анализа, позволяющие извлечь из целевой системы всю предварительную информацию, необходимую для более детального анализа системы на предмет её уязвимости, в связи с чем подробно разбирается алгоритм атаки злоумышленника на целевую систему.

Предлагается функциональная модель системы поиска и анализа уязвимостей.

В работе рассматриваются вопросы, связанные с разработкой программного прототипа сканера системы безопасности (*CISGuard*). Рассмотрена концепция программного комплекса, его ключевые особенности, такие как универсальность, особенности сканирующего ядра, функциональные особенности. Дано детальное описание качества и этапов сканирования. Разработана архитектура всей системы (см. Рис. 11). Предложены ключевые функции ядра.

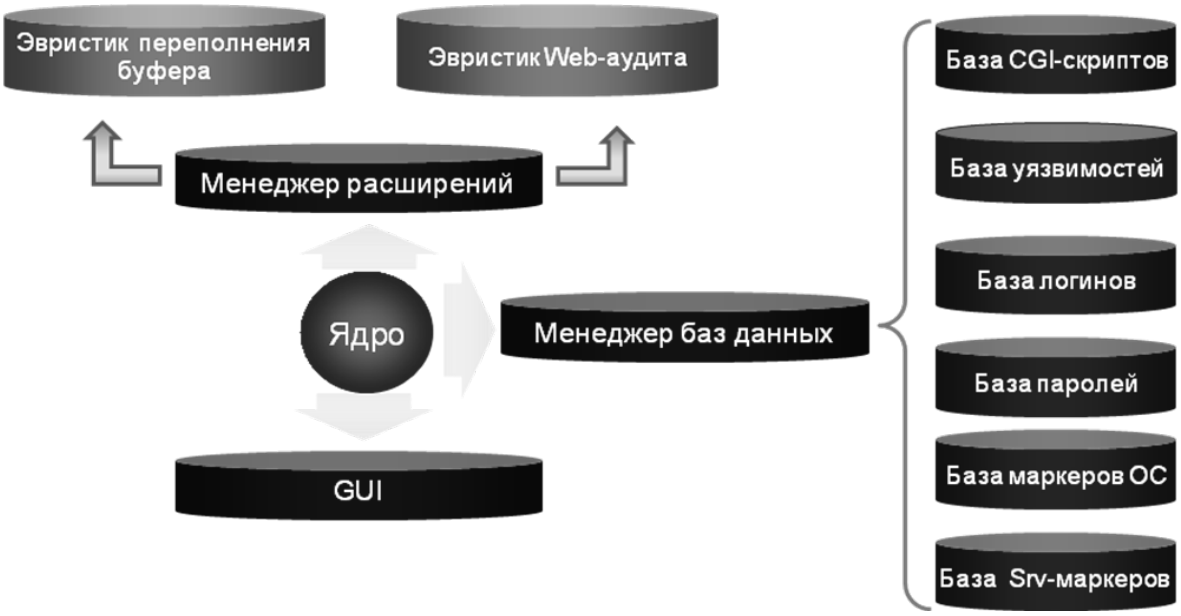

Рисунок 11– Архитектура программного комплекса анализа защищенности

Отмечается, что несмотря на то что *CISGuard* работает под управлением Microsoft Windows он проверяет все доступные его возможностям уязвимости независимо от программной и аппаратной платформы узлов. Программный комплекс работает с уязвимостями на разных уровнях - от системного до прикладного.

К особенностям сканирующего ядра отнесены:

- *Полная идентификация сервисов на случайных портах.* Обеспечивается проверка на уязвимость серверов со сложной нестандартной конфигурацией, в том случае, когда сервисы имеют произвольно выбранные порты.
- *Эвристический метод определения типов и имен серверов (HTTP, FTP, SMTP, POP3, DNS, SSH) вне зависимости от их ответа на стандартные запросы.* Используется для определения настоящего имени сервера и корректной работы проверок в тех случаях, если конфигурация WWW-сервера скрывает его настоящее имя или заменяет его на другое имя.
- *Проверка слабости парольной защиты.* Производится оптимизированный подбор паролей к большинству сервисов, требующих аутентификации, помогая выявить слабые пароли.
- *Анализ контента WEB-сайтов.* Анализ всех скриптов HTTP-серверов (в первую очередь, пользовательских) и поиск в них разнообразных уязвимостей: SQL инъекций, инъекций кода, запуска произвольных программ, получения файлов, межсайтовый скриптинг (XSS) и т.д.
- *Анализатор структуры HTTP-серверов.* Позволяет осуществлять поиск и анализ директорий доступных для просмотра и записи, давая возможность находить слабые места в конфигурации системы.

- *Проведение проверок на нестандартные DoS-атаки.* Обеспечивает возможность включения проверок "на отказ в обслуживании", основанных на опыте предыдущих атак и хакерских методах.
- *Специальные механизмы, уменьшающие вероятность ложных срабатываний.* В различных видах проверок используются специально под них разработанные методы, уменьшающие вероятность ошибочного определения уязвимостей.

Разработан интерфейс программного комплекса. Рассмотрен пример санкционированного аудита целевых информационных систем, подтверждающий высокую эффективность предложенных решений.

В заключении работы приводятся основные результаты, полученные в процессе проводимых исследований и итоговые выводы по диссертационной работе.

Основные выводы и результаты

1. Выполнен анализ существующих подходов и методов оценки уровня защищённости информационных систем. Проведённый анализ выявил недостаточную проработанность вопросов получения достоверных результатов анализа уровня защищённости и его прогнозирования.

2. Разработана модель оценивания защищенности сложных информационных систем на основе предполагаемых точек входа и разбиения всей системы на подсистемы - блоки со своими характеристиками уровня уязвимости. В рамках предложенной концепции становится возможным создание систем с заранее определёнными характеристиками защищённости, что, в свою очередь, увеличивает надёжность системы в долгосрочной перспективе.

3. Разработан метод оценки уровня защищённости ИС, который в отличие от существующих экспертных оценок, позволяет на основе накопленных мировым сообществом баз данных уязвимостей информационных систем спрогнозировать с использованием модели временных рядов более достоверные результаты.

4. Разработана структурно - функциональная модель уязвимости с использованием теоретико-множественного подхода, позволяющая параметрически описать каждую уязвимость, систематизировать и структурировать имеющиеся данные по уязвимостям с целью создания соответствующих баз для автоматизированных систем аудита.

5. Разработаны архитектура и прототип системы динамического анализа защищенности вычислительных сетей с применением техник эвристического анализа уязвимостей (программный комплекс CISGuard). К достоинствам предлагаемого комплекса можно отнести его открытую расширяемую архитектуру и использование унифицированных баз уязвимостей. Получены практические результаты на основе санкционированного автоматизированного анализа вычислительных сетей ряда отечественных предприятий, свидетельствующие об эффективности предложенных методов и технологий анализа защищённости.

Основные публикации по теме диссертации

Публикации в периодических изданиях из списка ВАК:

1. Политов, М. С. Двухуровневая оценка защищённости информационных систем / М. С. Политов, А. В. Мельников // Вестн. Уфим. гос. авиац.-техн. ун-та. Сер. Упр., вычисл. техника и информатика. 2008. Т. 10, № 2 (27). С. 210–214.

2. Политов, М. С. Полная структурная оценка защищённости информационных систем / М. С. Политов, А. В. Мельников // Доклады Томского государственного университета систем управления и радиоэлектроники. Томск : Томск. гос. ун-т, 2008. Ч. 1, № 2 (18). С. 95–97.

Другие публикации:

3. Политов, М. С. Проблемы анализа информационных систем / М. С. Политов. // Доклады конференции по компьютерным наукам и информационным технологиям (CSIT). Уфа : Уфим. гос. авиац.-техн. ун-т, 2005. Т. 2. С. 216–218.

4. Политов, М. С. Анализ защищённости информационных систем / М. С. Политов, А. В. Мельников // Математика, механика, информатика : докл. Всерос. науч. конф. Челябинск : Челяб. гос. ун-т, 2006. С. 107–108.

5. Политов, М. С. Многофакторная оценка уровня защищённости информационных систем / М. С. Политов, А. В. Мельников // Безопасность информационного пространства : материалы междунар. науч.-практ. конф. Екатеринбург : Урал. гос. ун-т путей сообщ., 2006. С. 146.

6. Политов, М. С. Комплексная оценка уязвимости информационных систем / М. С. Политов // Доклады конференции по компьютерным наукам и информационным технологиям (CSIT). Уфа – Красноусольск, 2007. Уфа : Уфим. гос. авиац.-техн. ун-т, 2007. Т. 2. С. 160–162.

ПОЛИТОВ Михаил Сергеевич

ЭКСПЕРИМЕНТАЛЬНО-АНАЛИТИЧЕСКИЙ МЕТОД ОЦЕНКИ И ПРОГНОЗИРОВАНИЯ УРОВНЯ ЗАЩИЩЁННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ МОДЕЛИ ВРЕМЕННЫХ РЯДОВ

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Подписано к печати _._.__. Формат 60x84 $^{1}/_{16}$.
Бумага офсетная. Печать офсетная. Гарнитура Таймс.
Усл. печ. л. 1,0. Уч.-изд. л. 1,0.
Тираж 100 экз. Заказ .

Челябинский государственный университет
454001 Челябинск, ул. Бр. Кашириных, 129
Издательство Челябинского государственного университета
454001 Челябинск, ул. Молодогвардейцев, 57б.