На правах рукописи

Ковалев Дмитрий Олегович

ВЫЯВЛЕНИЕ НАРУШЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПО ДАННЫМ МОНИТОРИНГА ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Специальность 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата технических наук

Автор: _____

Москва – 2011

Работа выполнена в Национальном исследовательском ядерном университете «МИФИ» (НИЯУ МИФИ)

Научный руководитель: кандидат технических наук, доцент
Милославская Наталья Георгиевна

Официальные оппоненты: доктор технических наук, с.н.с.,
член-корреспондент
академии криптографии РФ
Будзко Владимир Игоревич

кандидат физико-математических наук, с.н.с
Велигура Александр Николаевич

Ведущая организация: Всероссийский научно-исследовательский
институт проблем вычислительной техники
и информатизации (ВНИИПВТИ)

Защита состоится 23 ноября 2011 г. в 15 часов 00 минут на заседании диссертационного совета ДМ 212.130.08 при Национальном исследовательском ядерном университете «МИФИ» по адресу: 115409, г. Москва, Каширское шоссе., д.31, диссертационные советы при НИЯУ МИФИ, тел.: +7 (495) 323-95-26.

С диссертацией можно ознакомиться в библиотеке Национального исследовательского ядерного университета «МИФИ».

Отзывы в двух экземплярах, заверенные печатью организации, просьба направлять по адресу: 115409, г. Москва, Каширское шоссе., д.31, диссертационные советы при НИЯУ МИФИ, тел.: +7 (495) 323-95-26.

Автореферат разослан « ___» _____ 2011 г.

Ученый секретарь диссертационного совета:
Кандидат технических наук, доцент  Горбатов В.С.

I. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Информационно-телекоммуникационная сеть (ИТС) крупной корпоративной организации часто насчитывает десятки средств защиты информации (СЗИ), входящие в состав системы обеспечения информационной безопасности (СОИБ). Каждое из СЗИ может регистрировать сотни тысяч событий информационной безопасности (ИБ) в день. Большинство из этих сообщений ИБ являются результатом нормальной сетевой активности, и лишь немногие свидетельствуют о наличии реальных атак в ИТС. Поэтому в настоящее время мониторинг ИБ ИТС в динамически меняющейся сетевой среде является очень важной и сложной задачей. Для решения этой задачи используются системы мониторинга ИБ, которые осуществляют сбор сообщений ИБ, приведение их к единому виду, агрегацию и корреляцию для выявления аномальной сетевой активности. Примерами таких систем являются: Netforencics, Cisco MARS, IBM Tivoli, HP Arcsight и т.п.

Помимо сообщений ИБ современные системы мониторинга ИБ хранят в своем банке данных большое количество данных, имеющих отношения к ИБ: сведения об уязвимости конечных систем, сведения о выполнении политик ИБ и т.п. Совокупность информации, хранящейся в подобном банке данных, может быть использована для поддержки принятия решений по обеспечению ИБ. Однако объемы этих данных их разнородный характер делают сложным учет всех возможных параметров. Таким образом, возникает противоречие между наличием параметров, влияющих на обеспечение ИБ организации, и отсутствием методики, позволяющей одновременно учесть все эти параметры и дать на их основе некоторую консолидированную оценку результатов мониторинга ИБ. Положительный эффект от методики получения консолидированной оценки результатов мониторинга ИБ заключается в том, что она может быть использована для повышения защищенности в процессе обеспечения ИБ ИТС и реализации упреждающей защиты ИТС.

Данное противоречие может быть разрешено посредством оперативной обработки разнородных данных хранящихся в БД системы мониторинга ИБ и рас-

чета на их основе некоторой консолидированной оценки результатов мониторинга ИБ. Консолидированная оценка позволит учесть все множество данных, хранящихся в системе мониторинга ИБ, при этом сведя их к значимому, релевантному и понятному единому индикатору. Полученный индикатор может быть далее использован для принятия быстрых корректных ответных действий обслуживающим персоналом системы мониторинга ИБ.

В направлении исследования систем мониторинга ИБ работали многие отечественные и зарубежные ученые: П.Д. Зегжда, А.В Лукацкий, О.Б. Макаревич, В.В Романов, Д.В. Ушаков, И.А. Шелудько, R. Bidou, H. R. Debar, L. A. Johnson, R. Marchan, J. Myers, V. Paxson, J.S. Thomas, H. Zhang и другие.

В тоже время дальнейшего развития требуют методы обобщения результатов мониторинга ИБ, получения консолидированной оценки результатов мониторинга ИБ и способы построения централизованной упреждающей защиты.

Научно-технические проблемы защиты информационных ресурсов, информационных и телекоммуникационных систем определены в качестве основных направлений научных исследований в области обеспечения ИБ РФ, утвержденных Советом безопасности в 2008 г., что подчеркивает актуальность настоящей работы.

Тема работы соответствует пунктам 2, 14, 15 паспорта специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

Объект исследования. Объектом исследования являются системы мониторинга ИБ ИТС.

Предмет исследования. Предметом исследования являются методы и алгоритмы, используемые в работе систем мониторинга ИБ ИТС. В работе рассматриваются корпоративные ИТС, представляющие собой открытые среды с возможностью выхода в Интернет, а также сетевые атаки, которые могут быть идентифицированы посредством анализа данных, содержащихся в системах мониторинга ИБ. Рассматриваются системы мониторинга ИБ, построенные на базе реляционных СУБД.

Цель исследования. Целью работы является повышение защищенности ИТС посредством своевременного результативного выявления нарушений ИБ.

Задачи, решаемые для достижения поставленной цели. В рамках работы решаются следующие задачи:

1) исследовать методы и алгоритмы, используемые в работе систем мониторинга ИБ;

2) исследовать закон распределения количества сообщений ИБ;

3) разработать метод и алгоритм выявления нарушений ИБ в потоке сообщений ИБ;

4) разработать методику получения консолидированной оценки результатов мониторинга ИБ ИТС;

5) разработать практические рекомендации по улучшению систем мониторинга ИБ;

6) разработать программную реализацию, позволяющую получить консолидированную оценку результатов мониторинга ИБ и провести экспериментальную проверку ее работы.

Методы исследования. В качестве основных методов исследования применялись методы системного анализа, теории вероятности и математической статистики, теории нечетких множеств и нечеткой логики.

Основные научные результаты, полученные автором. На защиту выносятся следующие основные результаты работы:

1) метод и алгоритм выявления нарушений ИБ в потоке сообщений ИБ, основанный на динамически обновляемой таблице моментов для известного закона распределения сообщений ИБ;

2) методика получения консолидированной оценки результатов мониторинга ИБ, основанная на методах нечеткой логики и включающая в себя методы и алгоритмы выявления нарушений ИБ в потоке сообщений ИБ и получения консолидированной оценки.

Научная новизна. Научная новизна работы заключается в следующем:

1) исследован закон распределения количества сообщений ИБ для различных временных интервалов при отсутствии атак в ИТС, который в дальнейшем используется в методе выявления нарушений ИБ в потоке сообщений ИБ;

2) разработан метод выявления нарушений ИБ в потоке сообщений ИБ, основанный на динамически обновляемой таблице моментов для известного закона распределения сообщений ИБ. Данный метод позволяет определить допустимое количество сообщений ИБ на различных временных интервалах и, как следствие, случаи превышения допустимого количества сообщений, что может являться сигналом аномальной сетевой активности;

3) создана методика получения консолидированной оценки результатов мониторинга ИБ, включающая в себя методы и алгоритмы выявления нарушений ИБ в потоке сообщений ИБ и получения консолидированной оценки, используемые в процессе обеспечения ИБ ИТС.

Практическая значимость работы. Практическая значимость работы заключается в следующем:

1) результаты исследования могут использоваться организациями при проектировании и разработке собственных систем мониторинга ИБ и наметить дальнейшие перспективы развития систем мониторинга ИБ и комплексных систем защиты информации в целом;

2) программная реализация, позволяющая получить консолидированную оценку результатов мониторинга ИБ, может быть применена организациях в процессе обеспечения ИБ ИТС;

3) материалы диссертации также могут быть использованы при чтении курсов лекций по теории и практике защиты информации.

Достоверность результатов. Достоверность результатов исследования подтверждается формальными математическими выводами основных утверждений, сформулированных в работе, использованием известных проверенных на практике методов, соответствием предложенных улучшений общим архитектурным принципам построения СЗИ и результатами лабораторного эксперимента.

Реализация результатов исследования. Результаты диссертационной работы использованы в проектно-конструкторской деятельности ООО «ЛИНС-М», ЗАО «ДиалогНаука», использованы в составе комплекса защиты ИТС ОАО «Российский Сельскохозяйственный банк», а также внедрены в учебный процесс на факультете «Кибернетика и информационная безопасность» НИЯУ МИФИ. Внедрение результатов подтверждается соответствующими актами.

Апробация результатов и сведения о публикациях. Основные положения диссертационной работы нашли отражение в 13 публикациях по теме проведенного исследования, 4 из которых опубликованы в журналах Перечня ВАК и 9 тезисов научных докладов. Результаты диссертационной работы докладывались на Всероссийской научно-технической конференции «Проблемы информационной безопасности в системе высшей школы» (Москва, 2008-2010 гг.), конференции «Технологии Microsoft в теории и практике программирования» (Москва, 2008 г.), конференции «Информационная безопасность» (Красноярск, 2008 г.), международная конференция «Информационная безопасность» (Таганрог, 2008 г.), общероссийской научно-технической конференции «Методы и технические средства обеспечения безопасности информации» (Санкт-Петербург, 2008 г.), а также на семинарах кафедры «Информационной безопасности банковских систем» НИЯУ МИФИ (Москва, 2009-2010 гг.).

Структура и объем работы. Структура диссертации подчинена логике исследования и состоит из введения, четырех глав, заключения и списка литературы. Объем работы составляет 170 страниц, 42 рисунка, 19 таблиц, 4 приложения.

II. ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы исследования, сформулированы цель исследования и содержание поставленных задач, описаны объект и предмет исследования, указаны избранные методы исследования, определены научная новизна и практическая ценность выносимых на защиту результатов.

В первой главе производится анализ применения современных систем мониторинга в рамках комплексного подхода к обеспечению ИБ ИТС. Системы мониторинга ИБ ИТС исследуются с точки зрения архитектуры и функционального

устройства, используемых методов и алгоритмов и организационной структуры подразделения ИБ. Рассматриваются преимущества и недостатки различных систем мониторинга ИБ. На основании сделанных заключений делается вывод о том, что методика получения консолидированной оценки результатов мониторинга ИБ ИТС может быть использована при в процессе обеспечения ИБ и реализации упреждающей защиты ИТС.

Сетевая среда ИТС динамически меняется: появляются новые уязвимости, меняется ценность активов организации, возрастает количество известных атак, а также активность злоумышленников. При этом системы мониторинга ИБ хранят в своем банке данных большое количество информации, имеющей отношение к ИБ: сообщения ИБ, сведения об уязвимости конечных систем, сведения о выполнении политик ИБ. Совокупность информации, хранящейся в подобном банке данных, может быть использована для формирования консолидированной оценки и принятия на основании нее решения о том, какие меры защиты и в какой степени актуальны в текущий момент времени. Таким образом, консолидированная оценка используется оператором системы мониторинга в процессе обеспечения ИБ.

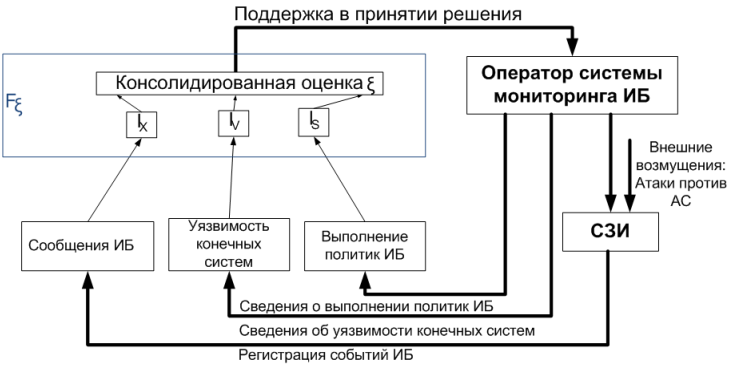


Рисунок 1. Система мониторинга ИБ ИТС

Формальная постановка задачи выглядит следующим образом: найти функцию $F_\xi: \{I_x, I_s, I_v\} \xrightarrow{F_\xi} \xi$, где I_x, I_s, I_v – показатели, позволяющие оценить количе-

ство сообщений ИБ, выполнение политик безопасности и уязвимости конечных систем соответственно, ξ – консолидированная оценка результатов мониторинга ИБ. Поскольку в рамках работы рассматриваются три типа исходной информации, хранящейся в БД системы мониторинга ИБ (выполнение политик ИБ, уязвимость конечных систем, сообщения ИБ), то $n = \overline{1,3}$.

Во второй главе производится разработка метода и алгоритма выявления нарушений ИБ в потоке сообщений ИБ. Основным результатом работы любой системы мониторинга ИБ является набор сообщений о выявленных событиях ИБ. В случае, если против ИТС направлена сетевая атака, то количество сообщений ИБ резко увеличивается. Это справедливо как для известных сетевых атак, так и для атак нулевого дня, поскольку СЗИ будут регистрировать большое количество сообщений ИБ, связанных с подозрительной сетевой активностью. Сложность заключается в том, чтобы оценить допустимое количество сообщений ИБ прежде, чем сделать заключение о том, что атака действительно имеет место.

На рис. 2 показан график количества сообщений ИБ при отсутствии атак на ИТС в рамках 10-минутных временных интервалов (значения фиксировались на протяжении одной недели). Из графика видно, что в разное время суток количество сообщений ИБ может значительно различаться. Также видно, что количество сообщений ИБ периодически повторяются изо дня в день с определенной погрешностью.

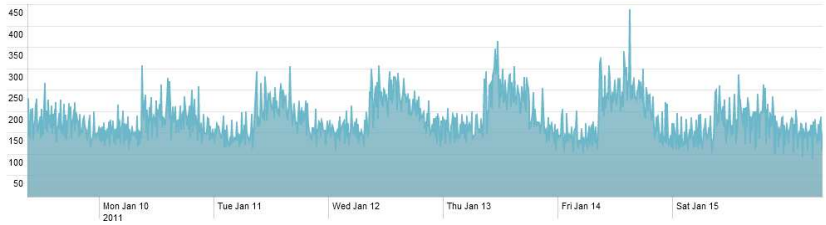


Рисунок 2 – Количество сообщений ИБ в рамках 10-минутных интервалов (Скриншот)

Таким образом, очевидно, что не существует единого порогового значения, которое можно задать заранее для идентификации атаки, и необходимо произво-

дить оценку количества сообщений ИБ, то есть найти функцию $f_1: i_1 = x_t \xrightarrow{f_1} I_x$, где $i_1 = x_t$ – число сообщений ИБ, полученных на t-ом интервале времени t, I_x – показатель, позволяющий оценить количество сообщений ИБ.

Решение данной задачи требует создания адаптивных пороговых значений, которые могли бы динамически обучаться шаблонам сообщений ИБ и постоянно находиться в актуальном состоянии по мере обновления данных.

С точки зрения математической статистики знание распределения количества сообщений ИБ для различного времени суток при отсутствии атак в ИТС позволит достаточно точно определить пороговые значения в нужный момент времени. В табл. 1 приведена статистика количества сообщений ИБ для одного из 10-минутных интервалов, собранная на испытательном стенде в течение 8 недель.

Таблица 1 – Количество сообщений ИБ в рамках 10-минутного интервала [сообщений, шт.]

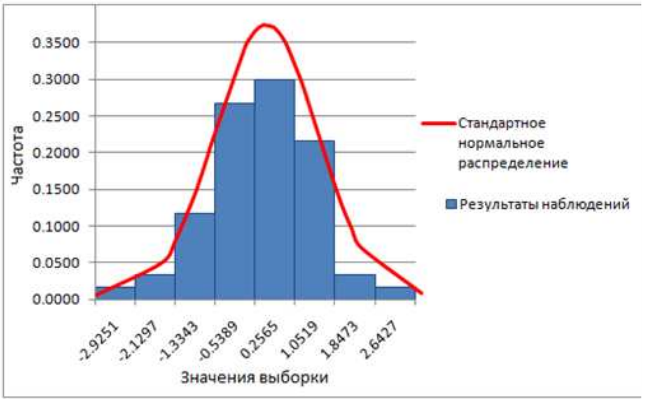
Неделя/День	**1**	**2**	**3**	**4**	**5**	**6**	**7**
1	173	154	173	175	162	178	163
2	164	180	172	180	184	180	173
3	164	173	180	174	184	187	184
4	173	184	176	184	192	174	180
5	210	175	175	195	176	185	178
6	185	157	184	185	140	197	185
7	174	180	163	178	184	179	181
8	173	180	175	174	165	173	161
Мат. ожидание(EX):		**176.5536**		**Дисперсия(DX):**		**121.0153**	

Для удобства работы со статистическими данными на основании табл. 1 рассчитана нормированная статистика $\frac{X-EX}{\sqrt{DX}}$, приведенная в табл. 2.

Таблица 2 – Нормированная статистика для количества сообщений ИБ [безразмерная величина]

Неделя/День	**1**	**2**	**3**	**4**	**5**	**6**	**7**
1	-0.3230	-2.0502	-0.3230	-0.1412	-1.3230	0.1315	-1.2321
2	-1.1412	0.3133	-0.4139	0.3133	0.6769	0.3133	-0.3230
3	-1.1412	-0.3230	0.3133	-0.2321	0.6769	0.9496	0.6769
4	-0.3230	0.6769	-0.0503	0.6769	1.4041	-0.2321	0.3133
5	3.0404	-0.1412	-0.1412	1.6768	-0.0503	0.7678	0.1315
6	0.7678	-1.7775	0.6769	0.7678	-3.3228	1.8586	0.7678
7	-0.2321	0.3133	-1.2321	0.1315	0.6769	0.2224	0.4042
8	-0.3230	0.3133	-0.1412	-0.2321	-1.0503	-0.3230	-1.4139
Мат. ожидание(EX):		**0.0000**		**Дисперсия(DX):**		**1.0000**	

Для проверки гипотезы о распределении количества сообщений ИБ в работе использовался непараметрический критерий Колмогорова. Выбор в пользу данного критерия обусловлен тем, что этот критерий достаточно прост, его можно применять для малых выборок и считается, что его мощность выше, чем у критерия χ^2. Гистограмма распределения для нормированной статистики количества сообщений ИБ представлена на рис. 3. Для построения гистограммы все множество значений выборки было разбито на $\sqrt{n} = \sqrt{56} \approx 8$ интервалов. Вид гистограммы позволяет выдвинуть гипотезу о том, что количество сообщений ИБ распределено по нормальному закону распределения.



Частота	Значение выборки
0.0167	-2.9251
0.0333	-2.1297
0.1167	-1.3343
0.2667	-0.5389
0.3000	0.2565
0.2167	1.0519
0.0333	1.8473
0.0167	2.6427

Рисунок 3. Гистограмма распределения количества сообщений ИБ

Для приведенной статистики мера расхождения между теоретическими значениями нормального распределения и эмпирическими значениями выборки $\lambda = \sup_x |F_n(x) - F(x)|\sqrt{n} = 1.2848$, что является меньше, чем $\lambda_\alpha \approx 1.36$ для уровня значимости $\alpha = 0.05$. Таким образом, гипотеза о распределении количества сообщений ИБ принимается при данном уровне значимости. Аналогичные результаты были получены для всех 10-минутных интервалов при уровне значимости $\alpha = 0.05$.

Математическое ожидание и дисперсия распределения на соседних временных интервалах должны не очень сильно отличаться, поэтому их оценки могут

быть получены в результате интерполяции по значениям, хранящимся в специально для этого созданной таблице моментов (имеются в виду 1-ый и 2-ой моменты случайной величины). В ходе экспериментов было установлено, что метод квадратичной интерполяции позволяет получить наиболее точные значения оценок математического ожидания и дисперсии. Таблица моментов используется для отслеживания цикличности сообщений ИБ. В рамках данной работы таблица моментов содержит 24 значения для математического ожидания и 24 значения дисперсии, соответствующие каждому часу в сутках. В типовой организации размеры таблицы моментов будут выбираться исходя из цикличности сообщений ИБ. Значения, хранящиеся в таблице моментов, динамически обновляются посредством экспоненциального скользящего среднего после получения очередного количества сообщений ИБ. Метод экспоненциального скользящего среднего представляет собой взвешенное скользящее среднее, у которого веса уменьшаются экспоненциально с удаленностью рассчитываемой величины от текущего значения наблюдения. Комбинация методов интерполяции значений таблицы моментов и расчета значений экспоненциальным скользящим средним позволяет оценивать как цикличность сообщений ИБ, так и долговременные тенденции.

Функция f_1 реализуется последовательностью из четырех основных шагов, которые применяются каждый раз при получении очередного количества сообщений ИБ x_t:

1) интерполировать значения в таблице моментов и получить оценку параметров для нормального распределения F_t для t-го интервала времени;

2) обновить значения таблицы моментов в соответствие с полученным значением количества сообщений ИБ x_t;

3) оценить количество сообщений ИБ x_t путем расчета стандартной оценки Z_t на основании параметров распределения F_t;

4) рассчитать значение показателя I_x на основании стандартной оценки Z_t.

Пусть x_t – это количество сообщений, полученное на t-ом интервале времени, который соответствует циклу c, часу h ($1 \leq h \leq H$) и минуте m ($1 \leq m \leq M$), где H=24 – количество часов в дне, M=60 – количество минут в часе.

На первом шаге происходит получение оценок математического ожидания $\widehat{\mu_{h,m}}$ и дисперсии $\widehat{\sigma^2_{h,m}}$ нормального распределения на t-ом интервале времени получаются в результате квадратичной интерполяции значений математического ожидания и дисперсии, хранящихся в таблице моментов $\{(E_h, D_h)$: h=1,…,H$\}$.

Пусть арифметическое среднее M=60 математических ожиданий, полученных в результате интерполяции в рамках одного часа, равно соответствующему значению E_h из таблицы моментов. Аналогично арифметическое среднее M=60 дисперсий, полученных в результате интерполяции в рамках одного часа, равно соответствующему значению D_h из таблицы моментов.

Тогда, если взять три последовательных часа (-1,0], (0,1], (1,2], то можно определить коэффициенты квадратической интерполяции (A,B,C):

$$\int_{-1}^{0}(At^2+Bt+C)dt=\frac{A}{3}-\frac{B}{2}+C=E_{-1}M$$

$$\int_{0}^{1}(At^2+Bt+C)dt=\frac{A}{3}+\frac{B}{2}+C=E_{0}M$$

$$\int_{1}^{2}(At^2+Bt+C)dt=\frac{7A}{3}-\frac{3B}{2}+C=E_{1}M$$

Решение данной системы уравнений относительно A,B,C дает:

$$A=M(E_{-1}-2E_0+E_1)/2$$

$$B=M(E_0-E_{-1})$$

$$C=M(2E_{-1}+5E_0-E_1)/6$$

Пусть $m_1=\frac{m-1}{M}$, $m_2=\frac{m}{M}$ – две последовательные минуты, тогда значение оценки математического ожидания, полученное в результате процедуры интерполяции, соответствующей минуте m часа h равно:

$$\widehat{\mu_{h,m}}=\int_{m_1}^{m_2}(At^2+Bt+C)dt=\frac{A}{3M}({m_1}^2+m_1m_2+{m_2}^2)+\frac{B}{2M}(m_1+m_2)+\frac{C}{M}$$

Таким образом, выведено выражение для расчета оценки $\widehat{\mu_{h,m}}$ из сохраненных значений математических ожиданий в таблице моментов.

Аналогичным образом для дисперсии:

$$A' = M(D_{-1} - 2D_0 + D_1)/2$$

$$B' = M(D_0 - D_{-1})$$

$$C' = M(2D_{-1} + 5D_0 - D_1)/6$$

$$\widehat{\sigma^2_{h,m}} = \int_{m_1}^{m_2}(A't^2 + B't + C')dt = \frac{A'}{3M}({m_1}^2 + m_1 m_2 + {m_2}^2) + \frac{B'}{2M}(m_1 + m_2) + \frac{C'}{M}$$

Интерполяция коэффициентов (A, B, C) и (A', B', C'), использующихся для расчета оценок математического ожидания и дисперсии, производится раз в час. Интерполяция сглаживает как значения внутри часа, так и между часами, поскольку коэффициенты зависят от хранящихся в таблице моментов оценок для данного часа, а также двух смежных с ним часов.

На втором шаге происходит обновление значений таблицы моментов. При обновлении значений таблицы моментов сложная ситуация возникает в случае экстремальных значений количества сообщений ИБ. Большой разброс значений может привести к резкому увеличению математического ожидания и дисперсии, что в свою очередь означает длинные хвосты распределения и неоднозначность выявления атаки в будущем. Если просто перестать учитывать экстремальные значения в расчетах, то это приведет к недооценке математического ожидания и дисперсии, то есть получится распределение с очень короткими хвостами и большим количеством ложных срабатываний. Таким образом, ситуации экстремальных значений количества сообщений ИБ необходимо обрабатывать особенно. Возможны следующие варианты:

1) очень большое экстремальное значение $x_t > x_{0.9999}$ – в этом случае в расчетах вместо x_t используется произвольное значение x'_t из интервала: $x_{0.99} < x'_t < x_{0.9999}$, где $x_{0.99}$,$x_{0.9999}$ – квантили распределения F_t уровней 0.99 и 0.9999 соответственно;

2) очень маленькое экстремальное значение $x_t < x_{0.0001}$ – в этом случае в расчетах вместо x_t используется произвольное значение x''_t из интервала: $x_{0.0001} < x''_t < x_{0.01}$, где $x_{0.01}$,$x_{0.0001}$ – квантили распределения F_t уровней 0.01 и 0.0001 соответственно;

3) отсутствие количества сообщений ИБ на интервале t – в этом случае в расчетах используется произвольное значение x'''_t из интервала: $x_{0.01} < x'''_t <$

$x_{0.99}$ где $x_{0.01}$,$x_{0.99}$ – квантили распределения F_t уровней 0.01 и 0.99 соответственно.

Математическое ожидание и дисперсия сохраняются в таблицу моментов по истечении каждого часа. Обновленное значение математического ожидания для нормального распределения на t-ом интервале времени, заканчивающимся на минуте m и часу h цикла c, рассчитывается как экспоненциальное скользящее среднее от двух величин: 1) $\widehat{\mu_{h,m}}$, полученной в результате интерполяции 2) x_t, которое является количеством наблюдаемых сообщений ИБ (с учетом правил для экстремальных или отсутствующих значений указанных выше):

$\widehat{\mu_{h,m}}' = (1 - w_c)\widehat{\mu_{h,m}} + w_c x_t$; $w_c = w + \frac{1-w}{1+c}$, где

w – некоторый фиксированный вес, принимающий значения между 0 и 1. w_c – временный вес для текущего цикла, который снижается до постоянного веса w по мере прохождения циклов и позволяет быстрее определить значение математического ожидания при инициализации системы. Фактически после прохождения большого количества циклов выражение принимает вид:

$\widehat{\mu_{h,m}}' = (1 - w)\widehat{\mu_{h,m}} + w x_t$

Выражение для дисперсии выводится следующим образом:

так как $D_n = \frac{1}{n}\sum_1^n (X_i - \overline{X_n})^2$, где $\overline{X_n} = \frac{1}{n}\sum_{i=1}^n X_i$, то:

$D_{n+1} = \frac{1}{n+1}[nV_n + (X_{n+1} - \overline{X_n})^2 + 2(\overline{X_n} - \overline{X_{n+1}})(X_{n+1} - \overline{X_n}) +$

$+(n+1)(\overline{X_n} - \overline{X_{n+1}})^2]$

Поскольку $\overline{X_n} - \overline{X_{n+1}} = \frac{1}{n}\sum_{i=1}^n X_i - \frac{1}{n+1}\sum_{i=1}^{n+1} X_i = \frac{\overline{X_{n+1}} - X_{n+1}}{n}$, то:

$D_{n+1} = \frac{n}{n+1} D_n + \frac{1}{n+1}(X_{n+1} - \overline{X_n})(X_{n+1} - \overline{X_{n+1}})$,

Приняв $w_c = \frac{1}{n+1}$, получается выражение для обновленного значения оценки дисперсии для t-го интервала времени:

$\widehat{\sigma_{h,m}^2}' = (1 - w_c)\widehat{\sigma_{h,m}^2} + w_c(x_t - \widehat{\mu_{h,m}})(x_t - \widehat{\mu_{h,m}}')$

Значения математического ожидания и дисперсии в таблице моментов не меняются в течение всего цикла. Для того чтобы в конце цикла обновить таблицу моментов по мере поступления наблюдений, рассчитываются временные значе-

ния математического ожидания E'_h и дисперсии D'_h. E'_h и D'_h инициализируются нулевыми значениями в начале часа по мере поступления наблюдений x_t обновляются по следующим формулам:

$$E'_h = E'_{h,M};\ E'_{h,m} = \frac{(m-1)E'_{h,m-1} + \widehat{\mu_{h,m}}'}{m};\ E'_{h,0} = 0;$$

$$D'_h = D'_{h,M};\ D'_{h,m} = \frac{(m-1)D'_{h,m-1} + \left(\widehat{\sigma^2_{h,m}}\right)'}{m};\ D'_{h,0} = 0;$$

В конце цикла полученные E'_h и D'_h замещают сохраненные в таблице моментов E_h и D_h соответственно, которые используются в следующем цикле.

На третьем шаге производится оценка x_t. Атаки в ИТС характеризуются повышенным количеством сообщений ИБ. Сниженное количество сообщений ИБ является индикатором того, что одно или несколько СЗИ вышло из строя. Таким образом необходимо отслеживать оба типа ситуаций.

Поскольку нормальные распределения на различных временных интервалах будут иметь различные параметры, то для того, чтобы сравнивать наблюдения x_t между собой их предварительно необходимо нормировать. Для этого рассчитывается нормированная статистика $Z_t = \frac{x_t - \widehat{\mu_{h,m}}}{\sqrt{\widehat{\sigma^2_{h,m}}}}$.

На четвертом шаге производится расчет значения I_x по методу экспоненциального скользящего среднего от Z_t по следующей формуле:

$I_x = (1-w)I_{x-1} + wZ_t$, где $Z_t = \frac{x_t - \widehat{\mu_{h,m}}}{\sqrt{\widehat{\sigma^2_{h,m}}}}$ для веса w в интервале (0,1], $I_0 = 0$.

Показатель I_x позволяет учитывать как магнитуду, так и длительность изменений. Например, резкий скачок количества сообщений (высокая магнитуда, но короткая длительность) может вывести I_x за пороговые значения точно также, как последовательность менее выраженных, но необычных скачков сообщений ИБ (малая магнитуда, но большая длительность) могут свидетельствовать об атаке. Для того, чтобы учитывать длительность изменений используется вес w, принимающий значения в интервале (0,1]. Значение w выбирается для каждой организации отдельно, либо опытным путем, либо на основании экспетных оценок.

В третьей главе производится разработка методики получения консолидированной оценки ξ результатов мониторинга ИБ. Методика получения консолидированной оценки результатов мониторинга ИБ включает в себя методы и алгоритмы выявления нарушений ИБ в потоке сообщений ИБ, получения консолидированной оценки и выработки рекомендаций по настройке СЗИ на ее основе.

Для получения консолидированной оценки формально требуется найти функцию $F_\xi: \{I_x, I_s, I_v\} \xrightarrow{F_\xi} \xi$, где I_x, I_s, I_v – показатели, позволяющие оценить количество сообщений ИБ, выполнение политик безопасности и уязвимости конечных систем соответственно, ξ – консолидированная оценка. Для решения данной задачи применяются методы теории нечетких множеств и нечеткой логики. Алгоритм получения консолидированной оценки представлен на рис.4.

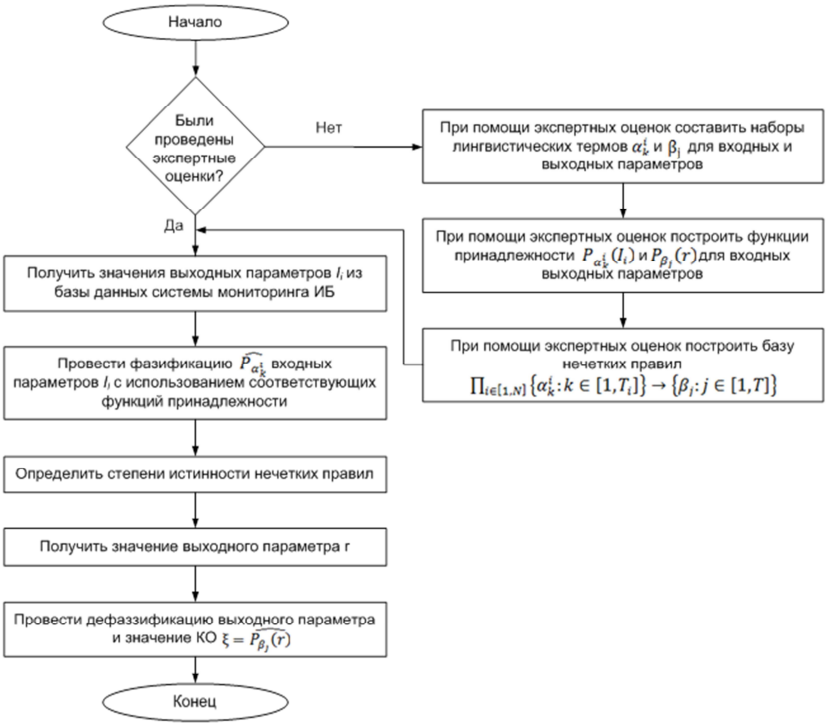


Рисунок 4. Алгоритм получения консолидированной оценки

Алгоритм включает следующие шаги:

1) если экспертные оценки не были проведены, то провести экспертные оценки, в противном случае перейти к шагу 5;
2) на основании экспертных оценок составить набор лингвистических термов, характеризующих значения входных параметров I_i: $\alpha_k^i, k \in [1, T_i]$ и выходного параметра r: β_j, $j \in [1, T]$, где T_i – количество термов параметра I_i, T – количество термов выходного параметра r. В качестве термов α_k^i, β_j используются лингвистические значения вида: «низкий», «средний», «высокий» и т. д.;
3) на основание экспертных оценок построить функции принадлежности для всех входных параметров I_i: $\{P_{\alpha_k^i}(I_i): i \in [1, N], k \in [1, T_i]\}$ и для выходного параметра r: $\{P_{\beta_j}(r): j \in [1, T]\}$, где I_i и r – переменные значения входных и выходного параметров. Функции принадлежности определяют соответствие входных и выходного параметров нечетким множествам. Нечеткие множества формализуют лингвистические высказывания вида: «Большое количество уязвимостей», «Малое количество сообщений ИБ» и т. д.;
4) на основании экспертных оценок построить базу нечетких правил в виде набора правил вида $\prod_{i \in [1,N]} \{\alpha_k^i : k \in [1, T_i]\} \to \{\beta_j : j \in [1, T]\}$;
5) получить оценки параметров I_i из банка данных системы мониторинга ИБ;
6) провести фаззификацию входных параметров, определить значения функций принадлежности, соответствующие оценкам, полученным на шаге 2: $\widehat{P_{\alpha_k^i}}, k \in [1, T_i]\ i \in [1, N]$;
7) определить степени истинности для каждого из нечетких правил;
8) рассчитать значение выходного параметра r на основании степеней истинности нечетких правил;
9) вычислить результирующее значение ξ путем дефаззификации выходного параметра $\xi = \widehat{P_{\beta_j}(r)}$.

В четвертой главе производится разработка программной реализации, позволяющей получить консолидированную оценку результатов мониторинга ИБ, и экспериментальная проверка ее работы. Для проведения эксперимента и получения статистических данных в рамках работы использовался стенд, представленный на рис. 5. Стенд, используемый для проведения лабораторного эксперимента, основан на программно-аппаратном комплексе Spirent ThreatEx 3.30, предназначенном для эмуляции сетевых атак, сетевом оборудовании компании Cisco, ПЭВМ и серверах под управлением ОС Windows, реализованных в виде виртуальных машин VMWare.

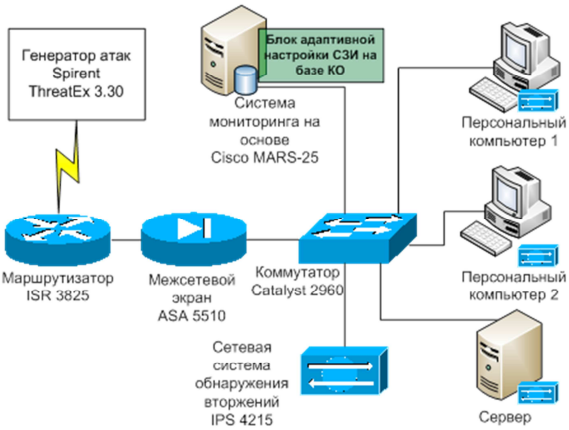


Рисунок 5. Схема испытательного стенда

В рамках эксперимента был разработан блок адаптивной настройки СЗИ на базе консолидированной оценки. Данный блок предназначен для считывания значения консолидированной оценки из банка данных системы мониторинга и автоматизации настройки СЗИ. В зависимости от значения консолидированной оценки результатов мониторинга ИБ блок адаптивной настройки СЗИ отправляет один из трех вариантов настроек, представленных в табл. 3. Фактически данный блок осуществляет симуляцию работу оператора системы мониторинга ИБ.

В ходе работы сделано предположение, что в корпоративных ИТС различные варианты настроек СЗИ будут также заранее разработаны и регламентированы в нормативной документации.

Лабораторный эксперимент проводился посредством генерации определенного количества атак против ИТС при помощи программно-аппаратного комплекса Spirent ThreatEx.

Перед каждой итерацией эксперимента выбирались количество сообщений ИБ, вариант состояния уязвимости ИТС и вариант выполнения политик ИБ при этом настройки СЗИ сбрасывались до минимального уровня. Итерация эксперимента проводилась в течение часа, в рамках которого сетевые атаки были равномерно распределены во времени. Таким образом значение консолидированной оценки в течение часа динамически менялось и на основании этого значения применялся тот или иной вариант настроек СЗИ.

Таблица 3 – Варианты настроек СЗИ

Объект настройки	Минимальные настройки	Стандартные настройки	Усиленные настройки
МЭ	Списки контроля доступа	Более строгие правила в списках контроля доступа Включение анализа пакетов для ряда протоколов	Включение анализа пакетов для всех протоколов Включение ограничений по количеству сессий
СОПВ	СОПВ работает в режиме обнаружения вторжений	СОПВ работает в режиме предотвращения вторжений	СОПВ работает в режиме предотвращения вторжений и блокирования атакующего
СОПВ уровня хоста	Блокирует все известные атаки, разрешает подозрительные действия	Блокирует все известные атаки, запрашивает пользователя о подозрительных действиях	Блокирует все известные атаки, запрещает подозрительные действия
Функции защиты браузера	Средний уровень безопасности	Умеренно-высокий уровень безопасности	Высокий уровень безопасности

Результаты эксперимента представлены на рис. 6. Было произведено 27 итераций эксперимента, соответствующих всевозможным комбинациям трех вариантов количества сообщений ИБ, трех вариантов состояния уязвимостей ИТС, и трех вариантов выполнения политик ИБ. Система мониторинга ИБ ИТС на базе консолидированной оценки в среднем позволила заблокировать на 25.35% атак.

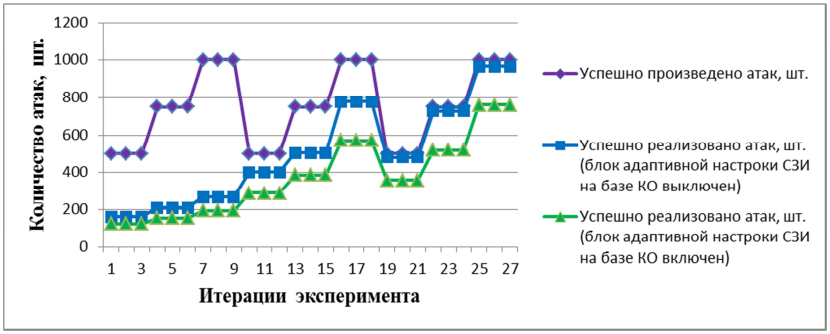


Рисунок 6. Результаты эксперимента

Результаты испытаний показали, что система мониторинга ИБ, основанная на методике получения консолидированной оценки результатов мониторинга ИБ, может быть использована для повышения защищенности в процессе обеспечения ИБ ИТС и реализации упреждающей защиты ИТС.

III. Основные выводы по результатам исследования

Основным результатом диссертационной работы является разработка методики получения консолидированной оценки результатов мониторинга ИБ. Методы и алгоритмы, входящие в состав методики получения консолидированной оценки результатов мониторинга ИБ позволяют повысить защищенность в процессе обеспечения ИБ и реализации упреждающей защиты ИТС.

В соответствии с поставленными задачами в диссертации получены следующие результаты:

1) Проанализированы современное состояние систем мониторинга ИБ, включая уровень технического обеспечения, уровень методов и алгоритмов и уровень организационного обеспечения систем мониторинга ИБ, а также методы и алгоритмы, используемые в них. На основе анализа литературных источников и документов, связанных с системами мониторинга ИБ, произведена формальная постановка задачи определения функции получения консолидированной оценки результатов мониторинга ИБ.
2) Исследован закон распределения количества сообщений ИБ посредством использования непараметрического статистического критерия Колмого-

рова на уровне значимости $\alpha = 0.05$. Знание данного закона позволяет определить случаи аномального количества сообщений ИБ, сигнализирующие об атаках в ИТС и разработать метод выявления нарушений ИБ в потоке сообщений ИБ ИТС.

3) Создан метод выявления нарушений ИБ в потоке сообщений ИБ, основанный на динамически обновляемой таблице моментов для нормального закона распределения сообщений ИБ. Данный метод использует технику квадратичной интерполяции значений, хранящихся в таблице моментов, для получения оценок математического ожидания и дисперсии, являющихся параметрами закона распределения количества сообщений ИБ на заданном интервале времени.
4) Построен алгоритм выявления нарушений ИБ в потоке сообщений ИБ. Данный алгоритм позволяет практически реализовать метод выявления нарушений ИБ в потоке сообщений ИБ ИТС и предоставить входные данные для метода и алгоритма адаптивной настройки СЗИ.
5) Разработана методика получения консолидированной оценки результатов мониторинга ИБ. Данная методика включает в себя методы и алгоритмы выявления нарушений ИБ в потоке сообщений ИБ и получения консолидированной оценки результатов мониторинга ИБ.
6) Исследованы системы мониторинга ИБ и на основе полученных результатов выработаны практические рекомендации по их улучшению, которые включают: блок адаптивной настройки СЗИ, многоуровневую систему хранения сообщений ИБ, развитие корреляционного анализа сообщений ИБ и межкорпоративную корреляцию событий ИБ. Данные улучшения позволят повысить качество мониторинга ИБ и, как следствие, защищенность ИТС.
7) Разработана программная реализация, позволяющая получить консолидированную оценку результатов мониторинга ИБ. Данная программная реализация применима для систем мониторинга ИБ, использующих в своем составе стандартные СУБД и может работать в любых локальных и глобальных сетях, использующих в качестве основы для передачи информации стек протоколов TCP/IP.

IV. Список опубликованных работ по теме диссертации

Статьи в журналах, включенных ВАК в перечень ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные научные результаты диссертаций

1) Ковалев Д.О. Идеология и реализация операционных центров информационной безопасности / Д.О. Ковалев // Безопасность информационных технологий. – 2008. – N4. С. 103.
2) Ковалев Д.О., Милославская Н.Г. Межкорпоративная корреляция событий информационной безопасности / Д.О. Ковалев // Безопасность информационных технологий. – 2010. – N1. С. 76-80.
3) Ковалев Д.О. Оценка количества сообщений ИБ в автоматизированных системах как метод выявления сетевых атак / Д.О. Ковалев // Безопасность информационных технологий. – 2011. – N1. 44-50 С.
4) Ковалев Д.О., Милославская Н.Г. Методика адаптивной настройки Средств защиты информации на базе консолидированной оценки результатов мониторинга информационной безопасности / Д.О. Ковалев // Информация и безопасность. Воронеж. 2011. – Т14 Ч1. С 45-53.

Тезисы научных докладов

5) Ковалев Д.О., Милославская Н.Г. Операционные центры информационной безопасности / Д.О. Ковалев // В сб. Научная сессия МИФИ – 2008. XV Всероссийская научно-техническая конференция «Проблемы информационной безопасности в системе высшей школы», – М: МИФИ, 2008 г., С. 75-77
6) Ковалев Д.О., Милославская Н.Г. Современные центры управления безопасностью / Д.О. Ковалев // В сб. докладов X Международная конференция «Информационная безопасность», Таганрог, 24-27 июня 2008 г., С. 26-29.
7) Ковалев Д.О., Милославская Н.Г. Построение операционного центра по информационной безопасности / Д.О. Ковалев // В сб. Методы и технические средства обеспечения безопасности информации: Материалы XVII

Общероссийской научно-технической конференции. – Спб.: Изд-во Политехнического ун-та, 2008 г., С. 85.

8) Ковалев Д.О., Милославская Н.Г. Особенности построения современных систем управления информационной безопасностью / Д.О. Ковалев // В сб. Докладов Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых «Научная сессия ТУСУР-2008». – 2008. № 2(18), часть 1. – С. 112-113.
9) Ковалев Д.О., Милославская Н.Г. Особенности реализации операционного центра информационной безопасности / Д.О. Ковалев // В сб. Научная сессия МИФИ – 2009. XVI Всероссийская научно-техническая конференция «Проблемы информационной безопасности в системе высшей школы», – М: МИФИ, 2009 г., Том 3, С. 200.
10) Д.О.Ковалев, Н.Г. Милославская. Межкорпоративная корреляция событий информационной безопасности / Д.О. Ковалев // В сб. Научная сессия НИЯУ МИФИ – 2010. XVII Всероссийская научно-техническая конференция «Проблемы информационной безопасности в системе высшей школы», – М: НИЯУ МИФИ, 2010 г., Том 3, С 155.
11) Д.О.Ковалев, Н.Г. Милославская. Адаптивная защита автоматизированной банковской системы в операционных центрах информационной безопасности / Д.О. Ковалев // Труды научной сессии НИЯУ МИФИ – 2010. XVII Всероссийская научно-техническая конференция «Проблемы информационной безопасности», – М: НИЯУ МИФИ, 2010. Том 5. – С.205-207.
12) Д.О.Ковалев, Н.Г. Милославская. Адаптивная защита автоматизированной банковской системы при помощи операционного центра информационной безопасности / Д.О. Ковалев // В сб. Научная сессия НИЯУ МИФИ – 2010. XVII Всероссийская научно-техническая конференция «Проблемы информационной безопасности в системе высшей школы», – М: НИЯУ МИФИ, 2010 г., Том 3, С 155.
13) Д.О.Ковалев, Н.Г. Милославская. Адаптивные операционные центры управления информационной безопасностью в банковских средах / Д.О.

Ковалев // В сб. международной научно-технической конференции «Информационная безопасность 2010», Таганрог 2010 г., С 92.

Ковалев Дмитрий Олегович

ВЫЯВЛЕНИЕ НАРУШЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПО ДАННЫМ МОНИТОРИНГА ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Подписано в печать 19.10.2011

Тираж 100 экз.

Типография НИЯУ МИФИ.

115409, г. Москва, Каширское ш., 31