ИМИТАЦИОННАЯ МОДЕЛЬ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ КОНТРОЛЯ НАРУШЕНИЯ ПОЛИТИКИ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

Бьядовский Е.И., Пестов А.В., С.Д. Лучинкин, Г.В. Путинцев, М.М. Монахова (Владимир)

В настоящее время, высокую актуальность обретают вопросы, связанные с формированием и контролем политики информационной безопасности корпоративных сетей передачи данных (КСПД). Данный документ играет определяющую роль в построении комплексной системы защиты. Данной тематике посвящено большое количество работ как отечественных, так и зарубежных специалистов. Сама проблема обусловлена тем, что с одной стороны обеспечение политики информационной безопасности должно реализовывать четко определенный, формализованный, комплексный подход, но с другой стороны, недостаточно механизмов, позволяющих это сделать. Существуют определенные узконаправленные подходы, но единой концепции к решению проблемы не существует.

Таким образом можно сделать вывод об актуальности вопроса формирования и контроля политики информационной безопасности, а также создания единой комплексной системы, решающей подобные вопросы.

С целью решения поставленной задачи была разработана автоматизированная система контроля нарушения политики безопасности (АСКПБ), представляющая из себя клиент-северное приложение контроля нарушения политики безопасности корпоративных сетей передачи данных (КСПД). Система подразумевает проверку параметров элементов КСПД, формируя пакет контроля (совокупность которых представляет из себя политику безопасности), таких, как конфигурация сетевого оборудования, конфигурация антивирусной защиты, конфигурация сетевых протоколов и т.д. на соответствие эталону и принимает решение о наличии нарушений политики по различным схемам: «схема одного события», «схема нескольких событий», «схема k событий из n».

В пакете, сформированном программой контроля, содержится один контролируемый параметр.

Сформирован некоторый пакет контроля из n параметров $X_1=\{x_1,x_2,\ldots,x_n\}$. Решение о нарушении политики ИБ принимается по значению истинности «истина» всех событий X_i пакета контроля одновременно (при выборе алгоритма схемы «И») либо решение принимается по значению истинности «истина» хотя бы одного из событий x_i пакета контроля (при выборе алгоритма схемы «ИЛИ»).

Решение принимается по значению истинности «истина» k из n событий пакета контроля. Считается, что нарушение ПИБ обнаружено, если в «слове контроля» содержится не менее k единиц (причем неважно с какими номерами).

С целью проведения экспериментов была создана имитационная модель системы, которая была установлена на тестовую КСПД. Схема тестовой КСПД приведена на рис. 1

Для сервера системы были определены следующие требования: работа под управлением операционной системы Windows 7, 8.1; минимальный объем оперативной памяти 1024 мегабайта; предустановленный NET FRAMEWORK версии 4 и выше; права администратора для учетной записи из под которой осуществляется запуск; подключение к сети.

Для клиентского устройства были определены следующие требования: работа под управлением операционной системы Windows 7, 8.1; минимальный объем оперативной памяти 1024 мегабайта; предустановленный NET FRAMEWORK версии 4 и выше.

Основными статистическими характеристиками измерителя АСКПБ являются вероятность обнаружения инцидента P и вероятность ложной тревоги Q.

С целью проведения тестовых экспериментов АСКПБ был случайным образом выделен ряд параметров политики ИБ элементов тестовой КСПД.

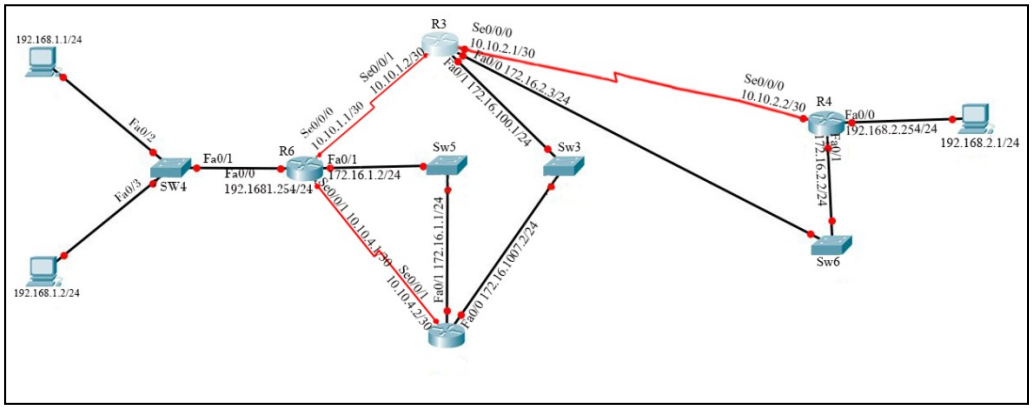

Рисунок 1 – схема тестовой КСПД

Их статистические исследования позволили выделить ряд факторов, характеризующих данные параметры, вызывающих нарушения политики ИБ КСПД.

Тестовая эксплуатация АСКПБ позволила определить основные характеристики и особенности измерителя системы, их значения приведены в таблице 1.

Ход эксперимента.

В качестве исходных данных в АСКПБ были занесены эталонные значения параметров (полученные в ходе статистических исследований тестовой КСПД), а также сформированы различные пакеты контроля для различных схем принятия решения.

Значения параметров установлены в соответствии с требованиями типовой политики в первом случае и с изменением пяти параметров (с номерами 1,3,7,8,9) во втором. Система была запущена 100 раз в режиме полной проверки, за максимальное

время, по каждому из алгоритмов принятия решения. Пороговое значение вероятности обнаружения $P = 0{,}3$, а ложной тревоги $Q = 0{,}2$. Кроме того, для схемы «комбинация событий» была установлена [1,3,7,8], а для схемы «*k* событий из *n*» k=5.

По итогам эксперимента полученные результаты были усреднены. Результаты приведены в таблице 2. Значения P и Q зависят от многих факторов, но наиболее значимая зависимость прослеживается от максимального времени работы системы. Так, можно сделать вывод о том, что чем дольше функционирует система, тем снижается риск ложного обнаружения инцидента ИБ (в случае достижения максимума).

Таким образом по результатам экспериментов были сделаны следующие выводы:

1. АСКПБ имеет высокую вероятность ложного срабатывания при ситуации «эксперимент отсутствует» только в случае работы по схеме «одно событие»;
2. При функционировании АСКПБ по всем схемам инциденты ИБ были обнаружены, минимальное время обнаружения было достигнуто при функционировании по схеме «Несколько событий»;
3. АСКПБ функционирует без сбоев на КСПД характерной для малых предприятий и предлагается к внедрению. В дальнейшем планируется проведение экспериментов на тестовых КСПД, характерных для крупных предприятий, функционирующих на различных протоколах и состоящих из оборудования, обладающего различными характеристиками.

По мнению авторов, АСКПБ позволит снизить время на обнаружение и устранение инцидентов ИБ, таким образом позволив снизить время простоя КСПД, а также поддерживать производительность КСПД на должном уровне.

Таблица 1. Характеристики параметров, используемых в эксперименте

№	Фактор (ы)	Параметр	Источник (и)	Характеристики измерителя			Особенности измерителя		
				$t_{мин}$	$t_{макс}$	$t_{ср}$	$P(t_{ср})$	$Q(t_{ср})$	
1	Антивирусная защита (АВЗ) не установлена, не активизирована на шлюзе HTTP FTP; АВЗ не установлена, не активизирована на почтовых системах SMTP/POP3; АВЗ не установлена, не активизирована на файловых серверах; АВЗ не установлена, не активизирована на ПС.	Конфигурация АВЗ	Реестр рабочей станции или сервера по путям: [HKEY_LOCAL_MACHINE\ SYSTEM\ CurrentControlSet\ Services; HKEY_LOCAL_MACHINE\System\ CurrentControlSet\Control \GroupOrderList. (команда «gwmi Win32_SystemDriver»).	210	695	496	0,19	0,07	антивирусной программой и системой должен быть разрешен доступ к конфигурации в реестре; конфигурация антивируса проверяется только в реестре; конфигурация реестра может не соответствовать реальной.
	Имеется доступ к активному сетевому оборудованию не только у системного администратора	Конфигурация сетевого оборудования	Оперативная память	545	1084	766	0,47	0,046	конфигурация считывается последовательно (построчно); обмен данных происходит по telnet протоколу; перед обработкой данные разбиваются на логические единицы.

Секция2

	На портах не установлен режим управления доступом	Конфигурация режима управления доступом на портах сетевого оборудования	Оперативная память	601	1374	1181	0,63	0,048	конфигурация считывается последовательно (построчно); обмен данных происходит по telnet протоколу; перед обработкой данные разбиваются на логические единицы; сопоставление происходят на уровне интерфейсов.
	Проверка наличия функции логирования всех процессов связанных с сетевыми соединениями	Логи процессов, связанных с сетевыми соединениями	Буфер АСО	501	755	607	0,69	0,018	буфер может быть очищен в любой момент времени и данные будут не достоверны; обмен данных происходит по telnet протоколу..
	Имеется множественный доступ к журналу аудита	Права доступа к журналу аудита	Конфигурационный файл журнала аудита на сервере по пути «c:\accconf.xml»	742	1129	944	0,5	0,03	в правах могут быть прописаны дополнительные, системные пользователи, несоответствующие политике, но не привносящие реального нарушения; возможно обращение к файлу

									конфигурации в момент его чтение системой (ошибка доступа).
	Не корректная частная виртуальная сети	Протоколы VPN	Оперативная память	654	1104	885	0,59	0,12	конфигурация считывается последовательно (построчно); обмен данных происходит по telnet протоколу; перед обработкой данные разбиваются на логические единицы.

Таблица 2 – Результаты эксперимента при отсутствии нарушения политики ИБ

Схема принятия решения	Время работы системы (сек.)	Выявлено нарушение
По одному событию	85,4	Да
По схеме «Несколько событий»	97,5	Нет
По схеме «*k* событий из *n*)	86,1	Нет
Комбинация событий	119,7	Нет

Таблица 3 – Результаты эксперимента при наличии нарушения политики ИБ

Схема принятия решения	Время работы (сек.)	Наличие нарушения
По одному событию	89,1	Да
По схеме «Несколько событий»	99,3	Да
По схеме «*k* событий из *n*)	132,1	Да
Комбинация событий	123,7	Да