УДК 004.62:004.8

Метод оценки защищенности сети передачи данных в системе мониторинга и управления событиями информационной безопасности на основе нечеткой логики

Р. Р. Файзуллин[1], **В. И. Васильев**[2]

[1]rustamf-firt@mail.ru, [2]vasilyev@ugatu.ac.ru
[1, 2]ФГБОУ ВПО «Уфимский государственный авиационный технический университет» (УГАТУ)

Поступило в редакцию 01.11.2012

Аннотация. Рассмотрены аспекты разработки современных систем мониторинга и управления событиями информационной безопасности. Предложен метод оценки защищенности сети передачи данных, позволяющий оперативно регулировать порог формирования сигнала тревоги и предоставляющий количественную и качественную оценку защищенности сети.

Ключевые слова. *Сеть передачи данных; система мониторинга и управления событиями информационной безопасности; нечеткая логика; корреляция событий; важность инцидента ИБ*

В современных вычислительных сетях обрабатываются большие объемы данных. Для того чтобы на уровне локальных вычислительных сетей (ЛВС) обеспечивать требуемый уровень информационной безопасности (ИБ) и централизованный анализ рисков ИБ, часто бывает достаточным применение систем обнаружения вторжений (СОВ) и традиционных механизмов обеспечения безопасности.

Характерной особенностью сетей передачи данных (СПД) является комплексное использование большого числа разнообразных аппаратно-технических средств. Они различаются своими характеристиками, производительностью, аппаратными платформами и базовыми технологиями. Указанные обстоятельства породили ряд серьезных проблем для обеспечения информационной совместимости и безопасности систем, функционирующих в СПД [1]. Применение СОВ на уровне СПД оказывается малоэффективным, поскольку из-за еще бóльшего потока информации лицо, принимающее решение (ЛПР), получает такое количество сигналов тревоги, что оно не способно своевременно и адекватно на них отреагировать, а в случае автоматизации ответных действий остается высоким риск парализации всей СПД. Последнее обусловлено исполнением строгих настроек безопасности даже при незначительных признаках атаки.

Чтобы справляться с огромными потоками данных, обеспечивая при этом высокий уровень ИБ, а также централизованный мониторинг и анализ сети, существуют системы мониторинга и управления событиями информационной без-опасности (СМУСИБ) [2–3].

Под событием информационной безопасности понимается идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью. Под инцидентом ИБ понимается любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность. Инцидентами ИБ являются:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по ИБ;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа [4].

В статье предложен метод получения оценки защищенности СПД в режиме реального времени в СМУСИБ на основе нечеткой логики.

1. СОСТОЯНИЕ ВОПРОСА

Основными целями СМУСИБ являются уменьшение числа событий ИБ до такого количества, которое позволит своевременно реагировать и принимать оперативные решения, автоматизация анализа поведения сети с целью распознавания возможных атак и нарушителей, управление инцидентами ИБ, а также обеспечение соответствия ИБ нормативным требованиям по защите информации [5]. СМУСИБ собирает сведения от таких устройств, как хостовые и сетевые СОВ, межсетевые экраны (МЭ), антивирусные системы, маршрутизаторы, коммутаторы, серверы, операционные системы, системы аутентификации и другие агенты мониторинга [6].

В СМУСИБ выделяют пять основных этапов обработки событий:

- *нормализация*, представляющая собой сбор различных сообщений о событиях с агентов мониторинга и приведение их к единому формату;
- *агрегация* – определение и удаление дублируемых сообщений, распределение оставшихся сообщений по различным категориям, выделение событий ИБ;
- *корреляция* – анализ агрегированных данных и выявление закономерностей, сигнализирующих о проведении атаки;
- *приоритезация* – ранжирование событий ИБ по уровню важности;
- *визуализация* – графическое представление событий ИБ, прошедших через предыдущие этапы, идентификация атак и принятие соответствующих действий по их предотвращению и устранению последствий [5].

Наиболее интересным в теоретическом плане этапом обработки событий является корреляция событий ИБ, поскольку от данного этапа во многом зависит способность СМУСИБ распознавать угрозы ИБ.

На сегодняшний день различают следующие разновидности корреляции событий:

- *корреляция, основанная на событиях* (например, если СОВ сообщает, что сигнатура А направлена на хост Б, а сканер уязвимостей «знает» о том, что хост Б является уязвимым, тогда срабатывает сигнал тревоги);
- *корреляция, основанная на правилах* (например, если одновременно имеют место события А, Б и В, то исполняется действие Г; либо если А повторяется более 3 раз в некотором интервале, то исполняется действие Б и т. п.);
- *корреляция, основанная на анализе аномалий* (например, если трафик на порте А превышает стандартное отклонение от образцов предыдущего трафика, то это может свидетельствовать о злонамеренных действиях);
- *корреляция, основанная на рисках* (например, если тип атаки = разрушительный (переполнение буфера), цель = критичный актив/ресурс (сервер) и сообщающее устройство = заслуживающее доверия (неперенастроенный Snort), то генерируется сигнал тревоги либо повышается уровень угрозы) [2].

Корреляция событий, основанная на рисках, может при этом значительно уменьшить количество правил, необходимых для эффективного распознавания угроз [2] и, как следствие, определения критичности инцидента ИБ. Критичность инцидентов ИБ, в свою очередь, определяет уровень защищенности сети. Поэтому указанная ниже задача будет решаться на основе корреляции событий, основанной на рисках.

2. ПОСТАНОВКА ЗАДАЧИ

В рамках исследований по направлению «Система мониторинга и управления событиями информационной безопасности в сетях передачи данных» разрабатываются следующие методы защиты информации:

- метод оценки защищенности СПД (в режиме реального времени);
- метод статистического анализа СПД;
- метод оценки соответствия политики ИБ.

Предметом данной статьи является разработка первого из указанных методов – метода оценки защищенности СПД, в котором реализуется возможность получения гибкой и быстрой настройки порога формирования сигнала тревоги для ЛПР. Актуальность метода обуславливается необходимостью получения достаточно сжатой информации о защищенности объекта исследования, чтобы можно было своевременно принять ответные действия по снижению рисков ИБ. Для этих целей требуется, чтобы по мере увеличения количества сигналов тревоги ЛПР могло снизить их до приемлемого количества.

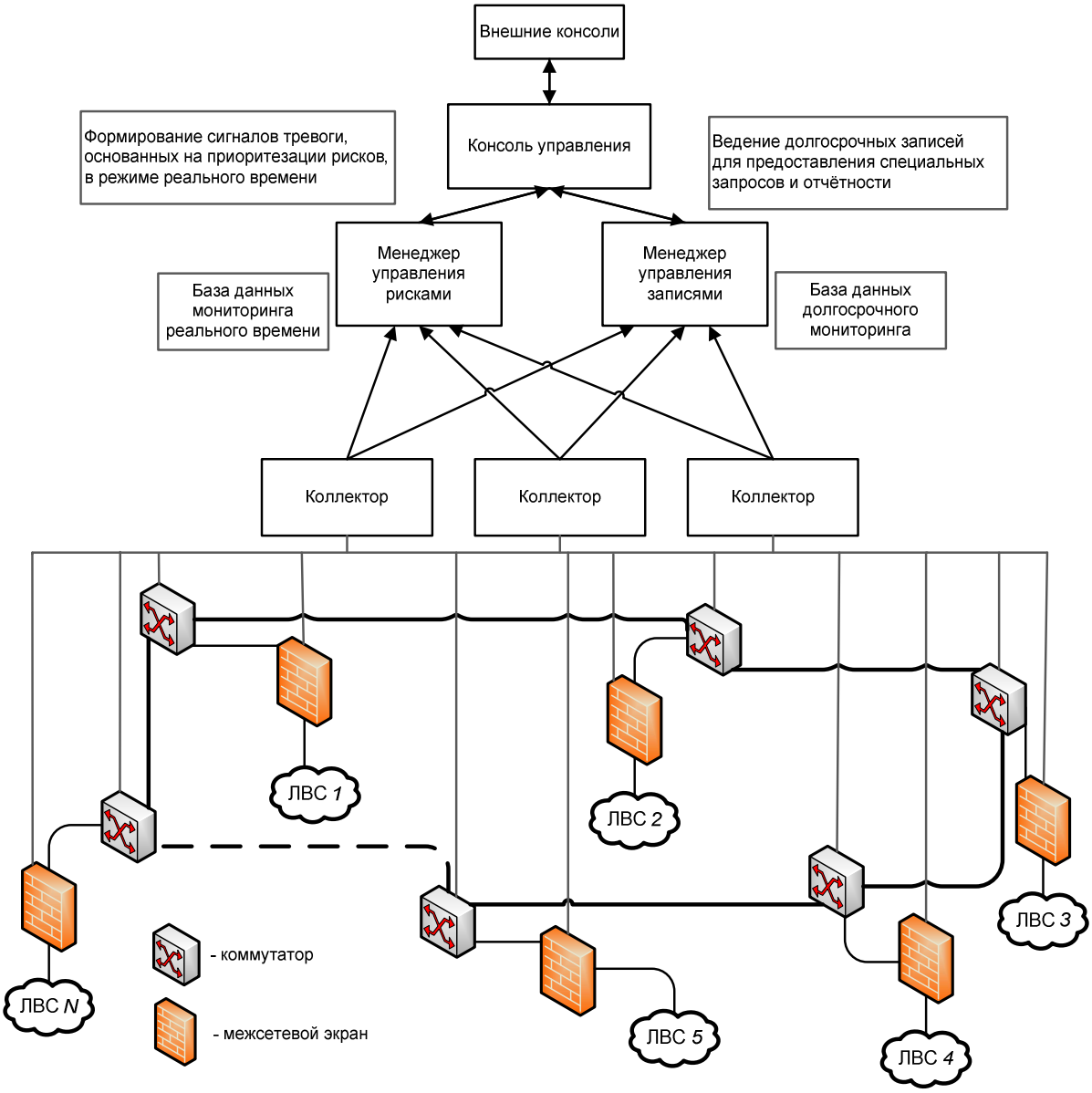

Рис. 1. Интегрированная архитектура СПД и СМУСИБ

Объектом исследования указанного направления является мультисервисная СПД (МСПД) с топологией типа «кольцо». Упрощенная интегрированная архитектура МСПД и СМУСИБ представлена на рис. 1.

3. МЕТОДИКА ИССЛЕДОВАНИЯ

В качестве методики исследования воспользуемся методами теории нечеткой логики.

Описание архитектуры СМУСИБ. Коммутаторы и МЭ играют роль генераторов сообщений. Сообщения могут быть основаны как на событиях, имевших место в СПД, так и на состоянии систем и сервисов (служб), генерирующих сообщения в результате реакции на некоторый внешний стимул или запрос [7].

Коллекторы выполняют функцию сбора данных с генераторов сообщений.

СМУСИБ включает в себя два модуля управления (менеджера). Первый – менеджер управления рисками – предназначен для формирования сигналов тревоги, основанных на приоритезации рисков, в режиме реального времени. Второй – менеджер управления записями – должен вести среднесрочные и долгосрочные записи в целях отчетности и предоставления отдельных запросов. Предлагаемый ниже метод оценки защищенности СПД является частью первого модуля, поскольку предназначен для

обеспечения безопасности в режиме реального времени.

Указанные модули и их базы данных, а также консоль центра управления безопасностью расположены в одной из ЛВС СПД, откуда и осуществляется централизованный мониторинг всей СПД.

Параметры ИБ СПД. В соответствии с подходом к анализу корреляций, основанным на анализе рисков, необходимо рассматривать три составляющие, на основании оценки которых осуществляется формирование сигнала тревоги (сообщения об инциденте ИБ) и/или понижается уровень защищенности. Такими составляющими являются: тип атаки; критичность актива (активов) ЛВС; уровень доверия сообщающему устройству.

В данном случае под уровнем атаки подразумевается лингвистическая оценка степени вредоносности атаки, представленная в терминах нечеткой логики «низкий – средний – высокий». Предполагается, что такая оценка предоставляется СОВ, являющейся составной частью системы защиты информации СПД.

Критичность активов ЛВС определяется в результате оценки ресурсов, обрабатываемых в каждой ЛВС, посредством классификации ресурсов и отнесения их к тем или иным уровням важности.

Уровень доверия сообщающему устройству (его репутация) определяется с целью повышения достоверности выявления атак. Под репутацией в данном контексте понимается «общественное» мнение об IP-адресах в СМУСИБ. Последняя может оценить всю совокупность сообщений, связанных с тем или иным событием ИБ, и принять правильное управленческое решение, например, отправить на межсетевой экран команды, которые заблокируют атаку злоумышленника. При этом в работе СМУСИБ могут иметь место как ложные срабатывания, так и пропуски действительных атак (ошибки первого и второго рода). Любая неверная идентификация инцидента ИБ приведет к нежелательным для ЛВС последствиям: в одном случае ЛВС будет признана как неблагонадежная (в случае ложного срабатывания), в другом – как ненадежная (в случае пропуска действительных атак). Для сокращения этих ошибок используется репутация устройств (портов). Если заданный IP-адрес ранее был замечен при проведении атаки в СПД, то он, скорее всего, либо принадлежит злоумышленнику, либо заражен вредоносным программным обеспечением, и, как следствие, репутация у него плохая. Если же IP-адрес в противоправных действиях замечен не был, то это не влияет на его репутацию [7].

МЭ, через которые ЛВС различных организаций подключены к СПД, и коммутаторы являются основными источниками, предоставляющими сведения о сетевой активности в СПД, то есть сообщающими о ЛВС устройствами. Поэтому каждой ЛВС соответствуют свои МЭ и коммутатор. Особенностью данного сегмента сети является то, что каждая ЛВС имеет свои средства защиты информации. Исходя из этого, можно судить о различных уровнях защиты информации в каждой ЛВС. В связи с этим предлагается использовать дополнительный параметр при корреляции событий, основанной на рисках, – уровень защиты ЛВС.

Необходимость применения данного параметра заключается в сокращении количества сигналов тревоги. Иными словами, если известно, что ЛВС имеет высокий уровень защиты, то не следует уделять инциденту ИБ пристального внимания в режиме реального времени.

Описанные выше параметры ИБ представляются в терминах нечеткой логики, они характеризуют каждую отдельную ЛВС и образуют кортеж множеств:

$$\text{Параметры ИБ ЛВС} = \{At, As, P, T\}, \quad (1)$$

где At – уровень атаки; As – критичность активов ЛВС; P – уровень защиты ЛВС; T – уровень доверия сообщающему устройству.

Можно составить матрицу нечетких правил, в которой для определенного набора значений параметров будет представлено итоговое значение, указывающее на важность инцидента ИБ ЛВС, как показано в табл. 1.

Таблица1

Матрица нечетких правил

	Уровень атаки (At)	Критичность активов ЛВС (As)	Уровень защиты ЛВС ($P_{ЛВС}$)	Уровень доверия сообщающему устройству (T)	Важность инцидента ИБЛВС (I)
1.	Н	Н	В	В	Н
2.	Н	Н	В	С	Н
3.	Н	Н	С	В	Н
4.	Н	В	В	С	С
5.	Н	В	С	В	С
6.	С	Н	В	В	Н
7.	С	Н	В	С	С
	…				
z.	В	В	Н	Н	В

Примечание. Н – низкий; С – средний; В – высокий

Однако такая таблица будет весьма большой (например, при пяти возможных значениях каждого параметра количество различных строк таблицы будет равно 5 × 5 × 5 × 5 = 625 строкам), а в случае необходимости внесения изменений в итоговые значения потребуется переписать таблицу, что является длительной процедурой.

Оценка важности инцидента ИБ ЛВС. Для более эффективного решения поставленной задачи, в том числе быстрого изменения уровня важности инцидента ИБ ЛВС, можно использовать формулу (2), в которой учитываются все описанные выше параметры. Важность инцидента ИБ отдельной ЛВС ($I_{ЛВС}$) здесь определяется как:

$$I_{ЛВС} = k(m) \times At \times As \times P_{ЛВС} \times T, \qquad (2)$$

где $k(m)$ – нормирующий коэффициент, позволяющий представить полученный результат в диапазоне [0; 1]. Для параметров ИБ с 5-уровневой градацией $k(5) = 0{,}0016$.

Для применения формулы (2) необходимо произвести преобразования нечетких переменных, после которых каждой нечеткой переменной будет соответствовать положительное целое число в диапазоне [1; 5]. Преобразования представлены в табл. 2–5.

Таблица 2

Преобразование нечеткой переменной «Уровень атаки» в числовые значения

Нечеткий параметр	Численное значение
Очень низкий	1
Низкий	2
Средний	3
Высокий	4
Очень высокий	5

Низкому уровню защиты и низкой репутации будут соответствовать большие числовые значения, и наоборот. Самый критичный инцидент ИБ может иметь максимальное числовое значение 1, а самый незначительный – 0,0016.

Таблица 3

Преобразование нечеткой переменной «Уровень защиты ЛВС» в числовые значения

Нечеткий параметр	Численное значение
Очень низкий	5
Низкий	4
Средний	3
Высокий	2
Очень высокий	1

Таблица 4

Преобразование нечеткой переменной «Критичность активов ЛВС» в числовые значения

Нечеткий параметр	Численное значение
Очень низкая	1
Низкая	2
Средняя	3
Высокая	4
Очень высокая	5

Таблица 5

Преобразование нечеткой переменной «Уровень доверия сообщающему устройству» в числовые значения

Нечеткий параметр	Численное значение
Очень низкий	5
Низкий	4
Средний	3
Высокий	2
Очень высокий	1

Таким образом, зная числовые значения всех четырех параметров ИБ ЛВС, можно получить числовую оценку важности инцидента ИБ ЛВС, представляемую в диапазоне от 0 до 1.

Оценка уровня защищенности СПД. Зная важность инцидентов ИБ для каждой ЛВС, можно получить числовую (количественную) оценку уровня защищенности СПД в целом по формуле:

$$P_{СПД} = \prod_{i=1}^{n} (1 - I_{ЛВСi}), \qquad (3)$$

где n – количество ЛВС в СПД; $I_{ЛВСi}$ – важность инцидента ИБ i-й ЛВС.

Подставив значение $I_{ЛВСi}$ из формулы (2), получаем итоговую формулу, позволяющую получить количественную оценку защищенности СПД:

$$P_{СПД} = \prod_{i=1}^{n} (1 - k(m) \times At_{ij} \times As_{ij} \times P_{ЛВСij} \times T_{ij}), \qquad (4)$$

где n – количество ЛВС в СПД; $k(m)$ – нормирующий коэффициент, позволяющий представить полученный результат в диапазоне [0; 1]; At_{ij} – уровень атаки на i-й ЛВС, равный j-му числовому значению; As_{ij} – критичность активов в i-й ЛВС, равная j-му целому числовому значению; P_{ij} – уровень защиты i-й ЛВС, равный j-му числовому значению; T_{ij} – уровень доверия сообщающему устройствуi-й ЛВС, равный j-му целому числовому значению.

На основе значений количественной оценки защищенности СПД можно получить значения

качественной оценки защищенности СПД по табл. 6.

Таблица 6

Зависимость значений качественной оценки защищенности СПД от значений количественной оценки защищенности СПД

Значения количественной оценки защищенности СПД	Значения качественной оценки защищенности СПД
$0 \le P_{СПД} < 0{,}5$	Очень низкая
$0{,}5 \le P_{СПД} < 0{,}7$	Низкая
$0{,}7 \le P_{СПД} < 0{,}85$	Средняя
$0{,}85 \le P_{СПД} < 0{,}95$	Высокая
$0{,}95 \le P_{СПД} \le 1$	Очень высокая

Для формирования сигнала тревоги (в виде визуализации на дисплее монитора, отправки SMS-сообщения и т.п.) ЛПР задает пороговое значение $P^*_{СПД}$, достижение которого вызовет формирование сигнала.

Пример. В качестве примера рассмотрим следующую ситуацию. В СПД имеется 4 ЛВС. СОВ выявляет атаку на двух МЭ, подключенных к разным ЛВС. Для одного МЭ атака имеет уровень «высокий – 4»; критичность активов в данной ЛВС «средняя – 3», уровень защиты – «низкий – 4», а уровень доверия сообщающему устройству – «очень высокий – 1». Для второго МЭатака имеет «средний – 3» уровень; «низкую – 2» критичность активов, «высокий – 2»уровень защиты и «высокий – 2» уровень доверия МЭ. Порог $P^*_{СПД}$, заданный ЛПР, равен 0,8.

На остальных сетевых устройствах атак выявлено не было, поэтому важность инцидентов ИБ на них равна 0.

СМУСИБ осуществляет корреляцию событий ИБ по формуле (4) и получает количественную оценку защищенности СПД:

$$P_{СПД} = \prod_{i=1}^{4}(1 - k(5) \times At_{ij} \times As_{ij} \times P_{ЛВСij} \times T_{ij}) =$$
$$= (1 - 0{,}0016 \times 4 \times 3 \times 4 \times 1) \times (1 - 0{,}0016 \times 3 \times$$
$$\times 2 \times 2 \times 2) \times (1 - 0) \times (1 - 0) =$$
$$= 0{,}9232 \times 0{,}9616 \times 1 \times 1 = 0{,}88774912.$$

С помощью полученного результата по табл. 6 получаем качественную оценку защищенности СПД.

Поскольку значение $P_{СПД}$превышает заданныйпорог $P^*_{СПД}$ ($P_{СПД}$ > 0,8), то СМУСИБ не уведомляет ЛПР об инцидентах ИБ, но отображает при этом как количественную (0,88774912), так и качественную («Высокая») оценку защищенности СПД на консоли управления.

Схема получения оценки. Вышеописанный метод можно представить в виде схемы, проиллюстрированной на рис. 2.

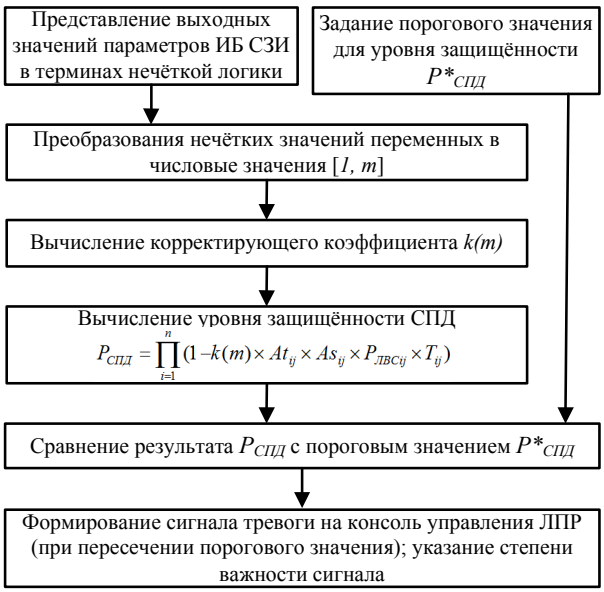

Рис. 2. Схема получения оценки уровня защищенности СПД

Дальнейшим развитием предложенного метода является получение оценки защищенности СПД на основе суммарных рисков в заданном интервале времени.

ВЫВОДЫ

Таким образом, предложенный метод оценки защищенности СПД позволяет быстро регулировать порог формирования сигнала тревоги. При этом на консоли управления указывается как количественная, так и качественная оценки защищенности СПД.

Преимуществом метода является простота реализации, а также удобство в изменении настроек данного модуля СМУСИБ. Метод применим для глобальных вычислительных сетей и СПД любой топологии.

СПИСОК ЛИТЕРАТУРЫ

1. Комплексная защита крупных корпоративных сетей передачи данных / С. Д. Белов [и др.] // Системный анализ и информационные технологии: тр. 3-й Международн. конф. М., 2009. С. 20–29.

2. **Swift D.** Practical Application of SIM/SEM/SIEM Automating Threat Identification. SANSInstitute, 2007. – p. 38.

3. **Полубелова О. В., Саенко И. Б., Котенко И. В.** Методы представления данных и логического вывода для управления информацией и событиями безопасности // Тр. 5-й Российск. мультиконф. по проблемам управления. СПб., 2012. С. 723–728.

4. **ГОСТ Р ИСО/МЭК 27001-2006** «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». М.: Стандартинформ, 2008. 32 с.

5. **Karlzen H**. An Analysis of Security Information and Event Management: The Use of SIEMs for Log Collection, Management and Analysis. Department of Computer Science and Engineering, University of Gothenburg, Göteborg, 2009. P. 45.

6. **Сердюк В**. Применение средств мониторинга событий ИБ в качестве инструмента для эффективной защиты от Интернет-угроз. URL: http://www.gosbook.ru/system/files/documents/2011/01/31/3_Serdiuk.ppt (дата обращения 05.10.2012).

7. **Ковалев Д.О.** Выявление нарушений информационной безопасности по данным мониторинга информационно-телекоммуникационных сетей. НИЯУ «МИФИ». М.: 2011. 170 с.

ОБ АВТОРАХ

Файзуллин Рустам Рафитович, асп. каф. выч. техники и защиты информации. Дипл. спец. по защите информации (УГАТУ, 2008). Дипл. магистр наук по инф. системам (Ун-т Брайтона, 2010). Готовит дисс. о системах мониторинга и управления событиями инф. безопасности.

Васильев Владимир Иванович, проф., зав. той же каф. Дипл. инженер по пром. электронике (УГАТУ, 1970). Д-р техн. наук по системн. анализу и автоматическ. управлению (ЦИАМ, 1990). Иссл. в обл. многосвязн., многофункц. и интел. систем.

METADATA

Title: Protectability assessment method of a data-transmission network in security information and event management system on a basis of fuzzy logic.

Authors: R. R. Fayzullin[1], V. I. Vasilyev[2]

Affiliation:
[1] Ufa State Aviation Technical University (UGATU), Russia.
[2] Ufa State Aviation Technical University (UGATU), Russia.

Email: [2]vasilyev@ugatu.ac.ru.

Language: Russian.

Source: Vestnik UGATU (Scientific journal of Ufa State Aviation Technical University),2013, Vol. 17, No. 2 (55), pp. 150–156. ISSN 2225-2789 (Online), ISSN 1992-6502 (Print).

Abstract: Aspects of the development of modern security information and event management systems are reviewed. Protect ability assessment method of a data-transmission network is suggested. The method lets promptly adjust a threshold of alarm signals formation as well as provide quantitative and qualitative protectability valuations of the network.

Keywords: Data-transmission network; security information and event management system; fuzzy logic; events correlation; importance of the information security incident.

References (English Transliteration):

1. Belov S.D., Zhizhimov O.L., Fedotov A.M., Osipov G.S., Tikhomirov I.A., Sochenkov I.V. “Complex protection of large-scale corporative data-transmission networks”, in *Proc. of 3rd International Workshop on Systems Analysis and Information Technologies(SAIT-2009)*, Zvenigorod, Russia, 2009, pp. 20-29.(In Russian).
2. Swift D.*Practical Application of SIM/SEM/SIEM Automating Threat Identification*. SANS Institute, 2007.– p. 38.
3. PolubevaO. V., SaenkoI.B., KotenkoI.V. “Methods of data presentation and logical output for information and security events management”, in*Proc. of 5th Russian multiconference of management problems (October 9-11, 2012, Saint-Petersburg)*. P. 723-728.(In Russian).
4. *Federal standard R ISO/IEC 27001-2006 «Information technology. Security techniques.Information security management systems.Requirements»*. – Moscow.: Standatrinform, 2008. – 32 p. (In Russian).
5. Karlzen H. *An Analysis of Security Information and Event Management: The Use of SIEMs for Log Collection, Management and Analysis*. Department of Computer Science and Engineering, University of Gothenburg, Göteborg, 2009.P. 45.
6. Serdyuk V. *Application of information security events monitoring techniques as an instrument for effective protection from Internet threats*. URL: http://www.gosbook.ru/system/files/documents/2011/01/31/3_Serdiuk.ppt (date 05.10.2012).(InRussian).
7. KovalevD.O. *Detection of information security breach on a basis of monitoring of information-telecommunication networks*. National research nuclear university “MEPhI”. – Moscow.: 2011. – 170 p. (In Russian).

Aboutauthors:

1. Fayzullin, Rustam Rafitovich, Postgrad. student, Dept. of Computer Engineering and Information Protection. Information Security Specialist (USATU, 2008).Master of Science in Information Systems (University of Brighton, 2010).Prepares diss. about SIEM systems.
2. Vasilyev, Vladimir Ivanovich, Prof., Head of Dept. of Computer Engineering and Information Protection. Dipl. engineer in Industrial Electronics (USATU, 1970). Dr. of Tech. Sci. (CIAM, 1990). Invest. inmultiply connected, multifunctional and intellectual systems.