2. *Sheng G., Qi-Ming Z., Jian J., Cun-Ren L., Qing-xi T.* Parallel Processing of InSAR Interferogram Filtering with CUDA Programming // Science of Surveying and Mapping Engineering. 2015. № 1. P. 54–68.
3. *Potapov V.P., Popov S.E., Kostylev M.A.* Metod obrabotki radarnykh dannykh na baze sistemy massovo-parallel'nogo ispolneniya zadanij Apache Spark // Vychislitel'nye tekhnologii. 2017. T. 22, spets. vyp. 1. 2017. S. 60–74.
4. *Zinno I., Mossucca L., Elefante S., De Luca C., Casola V., Terzo O., Casu F., Lanari R.* Cloud Computing for Earth Surface Deformation Analysis Via Spaceborne Radar Imaging: A Case Study // IEEE Trans. Cloud Computing. 2016. № 4. P. 104–118.
5. Apache Spark Unified Analytics Engine for Large-Scale Data Processing. URL: http://spark.apache.org (date of the application: 11.05.2018).
6. *Rusinov Yu.L., Titov K.I., Sharov S.A.* Ispol'zovanie algoritmov mnogopotochnoj realizatsii dlya resheniya zadach sinteza radiolokatsionnogo izobrazheniya // Radiolokatsionnoe issledovanie prirodnykh sred: materialy XXIX Vserossijskogo simpoziuma (Sankt-Peterburg, 25–26 marta 2015 g.). SPb., 2015.
7. *Chistyakov V.P.* Kurs teorii veroyatnostej. M.: Nauka, 1987. 240 s.
8. *Kashtanov V.A., Ivchenko G.I., Kovalenko I.N.* Teoriya massovogo obsluzhivaniya. M.: Librokom, 2012. 306 s.
9. *Kremer N.Sh., Putko B.A.* Ekonometrika. M.: YuNITI-DANA, 2010. 328 s.
10. *Nechaj A.A., Borisov A.A., Borisova Yu.I.* Tochechnyj analiz dannykh distantsionnogo zondirovaniya zemli sredstvami yazyka programmirovaniya Python // Vestnik Rossijskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz i upravlenie". 2019. № 1. S. 49–55.
11. *Shajmardanov A.M., Nechaj A.A., Lepekhin S.V.* Matematicheskie modeli sistem avtomaticheskogo upravleniya s shirotno-impul'snoj modulyatsiej // Vestnik Rossijskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz i upravlenie". 2019. № 2. S. 27–39.

DOI: 10.25586/RNU.V9187.19.03.P.032 УДК 004.94

В.А. Минаев, К.М. Бондарь, Е.В. Вайц, И.А. Беляков

ДИСКРЕТНО-СОБЫТИЙНОЕ МОДЕЛИРОВАНИЕ ПРОЦЕССОВ МОНИТОРИНГА И УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Применен метод дискретно-событийного моделирования для описания процессов мониторинга и управления информационной безопасностью. В ходе имитационных экспериментов показано, что именно эти модели позволяют наиболее адекватно, в режиме реального времени представить процесс реагирования на компьютерные атаки, рассчитать резко меняющуюся при их реализации нагрузку на информационную систему, персонал, обеспечивающий ее защиту, наглядно отобразить функционирование подсистемы мониторинга и управления информационной безопасностью. Дискретно-событийная модель построена в среде AnyLogic и отражает сообщения об атаках из двух источников информации (внутренних и внешних), приходящие от рабочих станций, сетевых устройств, веб-ресурсов и средств защиты информации. Дается описание SIEM (Центр информационной безопасности и управления событиями), где последовательно производится сбор сообщений, их фильтрация, агрегация и корреляция. SIEM дает возможность распределить сообщения по степени риска: высокий, средний, низкий. Далее моделируется SOC (Центр операций по обеспечению безопасности) с тремя линиями обслуживания, отличающимися уровнями

распознавания компьютерных атак и, соответственно, уровнями подготовки персонала. Результаты экспериментов с моделью включают изучение времени реагирования на компьютерные атаки, времени ожидания в очереди, времени обработки в блоках SIEM и SOC, количества сообщений с обнаруженными совпадениями сигнатур, отражающими компьютерные атаки, а также исследование ситуации, при которой происходит резкое увеличение количества сообщений, передаваемых от источников в Центр мониторинга информационной безопасности. Программное обеспечение Anylogic позволяет проигрывать различные сценарии с применением дискретно-событийной модели, производить интерпретацию результатов компьютерных атак, проводить различные виды имитационных экспериментов, обходя сложности их практической реализации и удешевляя получение оценок состояния информационной безопасности. Имитационные эксперименты позволяют прогнозировать время реагирования на компьютерные атаки, изучить блоки фильтрации, агрегации и корреляции.
Ключевые слова: дискретно-событийное моделирование, информационная безопасность, мониторинг, имитационный эксперимент, компьютерная атака.

V.A. Minaev, K.M. Bondar, E.V. Vaits, I.A. Belyakov

DISCRETE AND EVENT MODELLING OF MONITORING AND MANAGEMENT PROCESSES OF INFORMATION SECURITY

The article uses the method of discrete-event modeling to describe the processes of monitoring and management of information security. In the course of simulation experiments it is shown that these models allow the most adequate, in real time to present the process of responding to computer attacks, to calculate the rapidly changing load on information system and personnel providing its protection, to visualize the functioning of the subsystem of monitoring and management of information security. The discrete-event model is created in AnyLogic software environment and reflects messages about attacks from two sources of information (internal and external), coming from workstations, network devices, web-resources and information security tools. SIEM (Security Information and Event Management) is described, where messages are sequentially collected, filtered, aggregated and correlated. SIEM makes it possible to distribute messages according to the degree of risk: high, medium, low. Next, the SOC (Security Operations Center) is modeled with three lines of service, the levels of recognition of computer attacks and, accordingly, the levels of staff training. The results of experiments with the model include the study of the response time to computer attacks, the waiting time in the queue, the processing time in SIEM and SOC systems, the number of messages with detected signature matches, resulting in computer attacks, as well as the study of the situation in which there is a sharp increase in the number of messages transmitted from sources to the information security monitoring Center. AnyLogic software allows to play different scenarios using discrete-event model, to interpret the results of computer attacks, to carry out various types of simulation experiments, avoiding the complexity of their practical implementation and reducing the cost of obtaining estimates of the information security state. Simulation experiments make it possible to predict the response time to computer attacks, to study the blocks of filtering, aggregation and correlation.
Keywords: discrete-event modeling, information security, monitoring, simulation experiment, computer attack.

Введение

Применительно к современным информационным системам все более актуализируется вопрос их защиты от компьютерных атак. Во многом это связано с тем, что сегодня за

такими атаками, как правило, стоят не злоумышленники-любители, а целые группы технически хорошо оснащенных киберпреступников.

Именно поэтому в Доктрине информационной безопасности Российской Федерации прямо указано, что состояние информационной безопасности в стране характеризуется:

- постоянным повышением сложности, увеличением масштабов и ростом координации при проведении компьютерных атак на объекты критической информационной инфраструктуры;
- усилением разведывательной деятельности иностранных государств;
- нарастанием угроз суверенитету, территориальной целостности, политической и социальной стабильности России [1].

С целью обеспечения устойчивого функционирования информационных систем, а также ликвидации последствий компьютерных атак создаются и совершенствуются центры мониторинга информационной безопасности (ЦМИБ). На сегодняшний день уже накоплен определенный опыт разработки ЦМИБ [2; 3], в рамках которого созданы и исследованы различные типы моделей указанных центров [4; 5; 6; 7; 8].

В то же время пока явно недостаточно работ по имитационному моделированию процессов мониторинга и управления событиями информационной безопасности. Хотя именно эти модели позволяют наиболее адекватно, в режиме реального времени представить процесс реагирования на компьютерные атаки, рассчитать резко меняющуюся при их реализации нагрузку на информационную систему, персонал, обеспечивающий ее защиту, наглядно отобразить функционирование подсистемы мониторинга и управления информационной безопасностью.

Дискретно-событийная модель Центра мониторинга информационной безопасности

Дискретно-событийная модель (ДСМ) ЦМИБ построена в среде AnyLogic [9] (рис. 1), которая использовалась для проведения имитационных экспериментов.

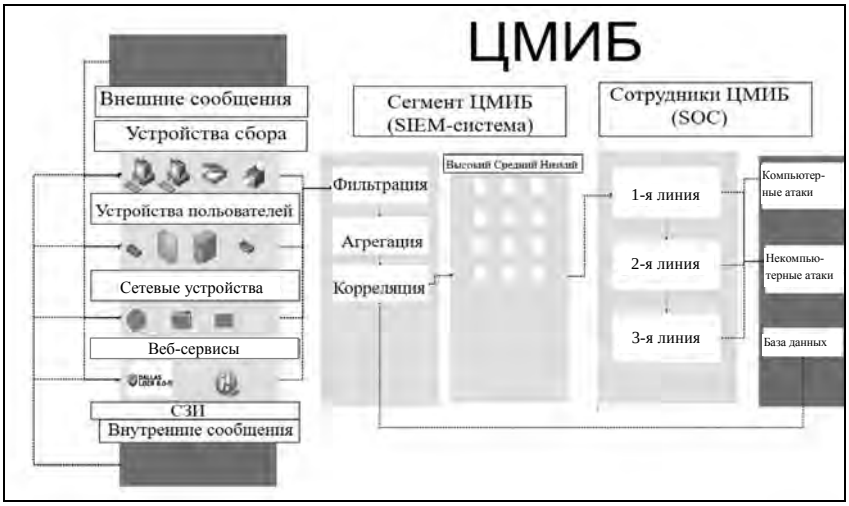

Рис. 1. Основные блоки дискретно-событийной модели ЦМИБ

На рисунке 1 введены следующие обозначения: SIEM – Security Information and Event Management (Центр информационной безопасности и управления событиями); SOC – Security Operations Center (Центр операций по обеспечению безопасности). Прокомментируем рисунок 1.

Первое, что нужно отметить: представленная схема отражает сообщения об атаках из двух источников информации (внутренних и внешних), приходящие от различных устройств. Такими источниками выступают рабочие станции, сетевые устройства, веб-ресурсы и средства защиты информации.

Рабочие станции пользователей предоставляют информацию о состоянии установленного программного обеспечения, его версиях, данные об аутентификации пользователя в системе, его иных действиях и запущенных процессах и т.д.

Сетевые устройства, представляя набор средств, передающих информацию, отражают трафик, помогающий понять взаимодействия рабочих станций и отследить действия злоумышленников.

Средства защиты информации позволяют установить требуемый уровень защищенности организации. Данные, поступающие в SIEM, дают возможность контролировать состояние различных включенных в систему устройств, а также выполнить команды администратора системы.

Далее сообщение попадает в SIEM-систему, где последовательно производится сбор сообщений, их фильтрация, агрегация и корреляция.

В *блоке фильтрации* поступающая информация разделяется на полезную для управления безопасностью системы и не имеющую такового свойства. После фильтрации полезная информация направляется в блок агрегации, а сообщения, не несущие полезных свойств в указанном нами смысле, передаются для последующего анализа в специальную базу данных.

Блок агрегации введен для объединения однотипных сообщений, приходящих из различных источников, в одну группу, что позволяет более точно определить вариант решений применительно к ней.

Затем сообщения поступают в *блок корреляции*, где производится сравнение с аналогами из базы данных компьютерных атак, что позволяет автоматизировать процесс реагирования на определенные их типы.

В конечном итоге обработка сообщений в SIEM дает возможность распределить сообщения по степени риска: высокий, средний, низкий.

После SIEM классифицированная информация поступает по 1-й линии в блок SOC для подтверждения правильности реагирования SIEM-системы. Если сотрудник, обслуживающий 1-ю линию, не может дать однозначный ответ на этот вопрос, информация передается на 2-ю линию.

Если и сотрудники, обслуживающие 2-ю линию, которые имеют более высокий уровень навыков распознавания сложных вариантов компьютерных атак, не решают задачу, то информация передается самым квалифицированным сотрудникам, относящимся к 3-й линии. Они проверяют правильность действий сотрудников 1-й и 2-й линий, при необходимости совершенствуют сигнатуры, позволяющие SIEM-системе более точно выявлять возможные компьютерные атаки.

Эксперименты с применением дискретно-событийной модели

На рисунке 2 приведены результаты моделирования функционирования ЦМИБ с использованием ДСМ для одного из вариантов ее исходных данных.

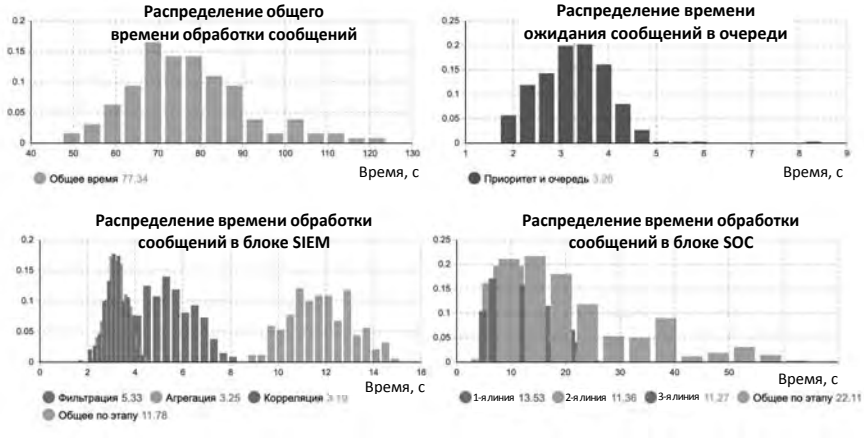

Рис. 2. Результаты моделирования работы ЦМИБ

Эти результаты включают диаграммы распределения общего времени реагирования на компьютерные атаки, времени ожидания в очереди, времени обработки в блоках SIEM и SOC. Кроме того, приведены количественные данные о средних временах по каждой диаграмме распределения.

Подобные эксперименты с моделью дают возможность генерации статистических данных о работе ЦМИБ без произведения практических, не всегда реально осуществимых и, как правило, дорогостоящих измерений, необходимых для совершенствования работы Центра мониторинга и оптимизации управления информационной безопасностью.

На рисунке 3 показано, каким образом меняется количество компьютерных атак в зависимости от времени, в сумме затраченного на обработку сообщений сотрудниками 1-й и 2-й линий.

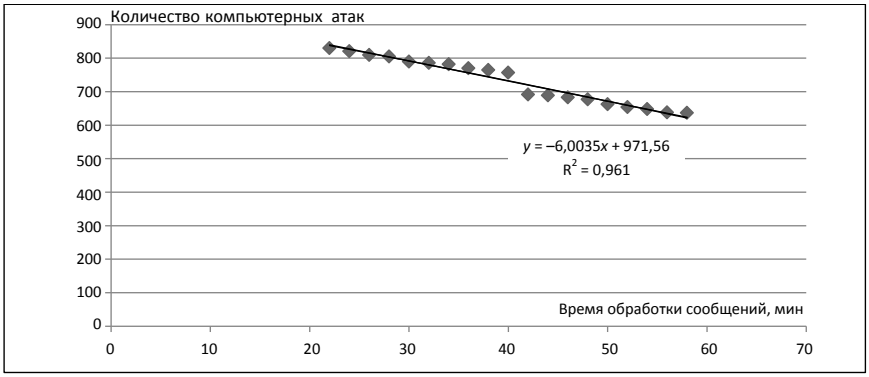

Рис. 3. Изменение числа компьютерных атак от суммарного времени обработки сообщений сотрудниками 1-й и 2-й линий

Очевидно, что при увеличении временных затрат на обработку сотрудниками сообщений число возможных компьютерных атак снижается. И это логично, поскольку поступающие сообщения проверяются более тщательно. Но, с другой стороны, увеличиваются затраты на содержание квалифицированного кадрового персонала ЦМИБ и снижается его готовность к обработке сообщений при их критическом увеличении. ДСМ позволяет произвести необходимые расчеты кадрового персонала в различных условиях функционирования ЦМИБ.

Одним из важных показателей функционирования ЦМИБ является количество сообщений с обнаруженными совпадениями сигнатур, отражающими компьютерные атаки, в сравнении со всеми обрабатываемыми сообщениями (рис. 4). Нужно подчеркнуть, что в данном случае совпадение сигнатур с использованием модели ЦМИБ показывает, какая доля сообщений стопроцентно отсеивается. В рассматриваемом случае она равна 0,24.

Рис. 4. Статистика совпадений сигнатур компьютерных атак и поступивших сообщений в процессе моделирования

Не менее важным показателем является доля отфильтрованных сообщений. В нашем эксперименте 90% всех сообщений после этапа фильтрации передаются в последующие блоки для анализа, соответственно, 10% направляются для хранения в базу данных. Каждое сообщение, поступившее в нее, сигнализирует о возможной компьютерной атаке и анализируется сотрудниками ЦМИБ.

Рассмотрим ситуацию, при которой происходит резкое увеличение количества сообщений, передаваемых от источников в ЦМИБ. Пусть это увеличение составит от 10 до 20 сообщений в минуту (рис. 5).

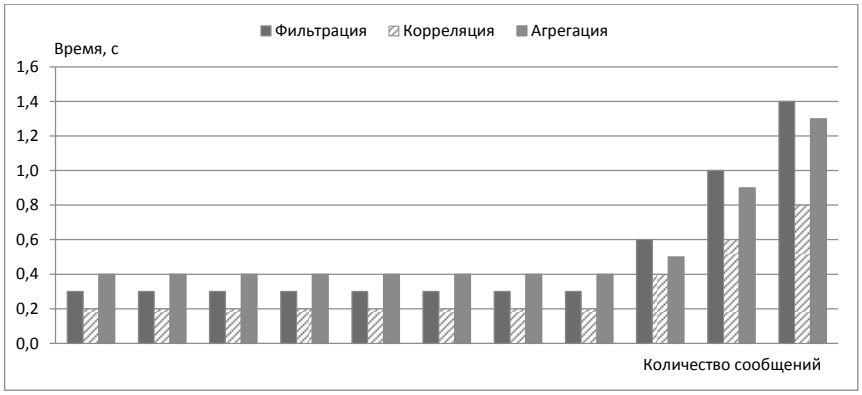

Рис. 5. Функционирование блоков ЦМИБ при резком увеличении сообщений

Выводы

1. Для исследования функционирования центров мониторинга информационной безопасности, созданных в различных ведомствах и отраслях России, весьма эффективно применение дискретно-событийных моделей, позволяющих делать весьма качественные оценки и прогнозы характеристик внешних и внутренних сообщений, включая сообщения о компьютерных атаках.

2. Избранное в качестве среды имитационного моделирования программное обеспечение платформы Anylogic позволяет проигрывать детальные сценарии с применением дискретно-событийной модели ЦМИБ, производить интерпретацию результатов моделирования компьютерных атак, проводить различные виды имитационных экспериментов, обходя сложности их практической реализации и удешевляя получение важных оценок состояния информационной безопасности.

3. Имитационные эксперименты с ДСМ ЦМИБ позволяют прогнозировать время реагирования на компьютерные атаки и количество сообщений о них при различных нагрузках, оценить количество компьютерных атак, определяемых SIEM-системой, изучить блоки фильтрации, агрегации и корреляции.

4. Дальнейшим развитием ДСМ ЦМИБ является уточнение и детализация описываемых факторного комплекса, параметров блоков SIEM и SOC, а также характеристик сообщений, включая критические режимы функционирования центров мониторинга информационной безопасности [10; 11].

Литература

1. Доктрина информационной безопасности Российской Федерации: утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646. Доступ из справ.-правовой системы «КонсультантПлюс».
2. Zimmerman C. Ten Strategies of a World-Class Cybersecurity Operations Center. McLean: The MITRE Corporation, 2014. 334 p.
3. *Gordon S.* Operationalizing Information Security: Putting the Top 10 SIEM Best Practices to Work. URL: https://ru.scribd.com/read/206534734/ Operationalizing-Information-Security-Putting-the-Top-10-SIEM-Best-Practices-to-Work# (date of the application: 19.06.2019).
4. *Федорченко А.В., Левшун Д.С., Чечулин А.А., Котенко И.В.* Анализ методов корреляции событий безопасности в SIEM-системах. Ч. 1 // Труды СПИИРАН. 2016. Вып. 47. С. 5–27.
5. *Федорченко А.В., Левшун Д.С., Чечулин А.А., Котенко И.В.* Анализ методов корреляции событий безопасности в SIEM-системах. Ч. 2 // Труды СПИИРАН. 2016. Вып. 6 (49). С. 208–225.
6. *Kotenko I.V., Chechulin A.A.* A Cyber Attack Modeling and Impact Assessment Framework // Proceedings of 5th International Conference on Cyber Conflict 2013 (CyCon 2013). [S. l.], 2013. P. 119–142.
7. *Ahmadinejad S.H., Jalili S., Abadi M.* A Hybrid Model for Correlating Alerts of Known and Unknown Attack Scenarios and Updating Attack Graphs // Computer Networks. 2011. № 55. P. 2221–2240.
8. *Karlzen H.* An Analysis of Security Information and Event Management: The Use of SIEMs for Log Collection, Management and Analysis. Gothenburg: University of Gothenburg, 2009. 45 p.

9. *Карпов Ю.Г.* Имитационное моделирование систем. Введение в моделирование с AnyLogic 5. СПб.: БХВ-Петербург, 2006. 400 с.
10. *Чекалкин А.А., Скрыль С.В., Минаев В.А.* Комплексный технический контроль эффективности мер безопасности систем управления в органах внутренних дел: учебное пособие для высших учебных заведений МВД России. Ч. 2: Практические аспекты технической разведки и комплексного технического контроля. М.: Горячая линия – Телеком, 2006. 205 с.
11. *Кулаков В.Г. и др.* Защита информации в телекоммуникационных системах: учебник для высших учебных заведений МВД России. Воронеж: ВИ МВД России, 2002. 300 с.

Literatura

1. Doktrina informacionnoj bezopasnosti Rossijskoj Federacii: utverzhdena Ukazom Prezidenta Rossijskoj Federacii ot 5 dekabrya 2016 g. № 646. Dostup iz sprav.-pravovoj sistemy "Konsul'tantPlyus".
2. *Zimmerman C.* Ten Strategies of a World-Class Cybersecurity Operations Center. McLean: The MITRE Corporation, 2014. 334 p.
3. *Gordon S.* Operationalizing Information Security: Putting the Top 10 SIEM Best Practices to Work. URL: https://ru.scribd.com/read/206534734/ Operationalizing-Information-Security-Putting-the-Top-10-SIEM-Best-Practices-to-Work# (date of the application: 19.06.2019).
4. *Fedorchenko A.V., Levshun D.S., Chechulin A.A., Kotenko I.V.* Analiz metodov kor-relyacii sobytij bezopasnosti v SIEM-sistemah. Ch. 1 // Trudy SPIIRAN. 2016. Vyp. 47. S. 5–27.
5. *Fedorchenko A.V., Levshun D.S., Chechulin A.A., Kotenko I.V.* Analiz metodov korrelyacii sobytiĭ bezopasnosti v SIEM-sistemah. Ch. 2 // Trudy SPIIRAN. 2016. Vyp. 6 (49). S. 208–225.
6. *Kotenko I.V., Chechulin A.A.* A Cyber Attack Modeling and Impact Assessment Frame-work // Proceedings of 5th International Conference on Cyber Conflict 2013 (CyCon 2013). [S. l.], 2013. P. 119–142.
7. *Ahmadinejad S.H., Jalili S., Abadi M.* A Hybrid Model for Correlating Alerts of Known and Unknown Attack Scenarios and Updating Attack Graphs // Computer Networks. 2011. №. 55. P. 2221–2240.
8. *Karlzen H.* An Analysis of Security Information and Event Management: The Use of SIEMs for Log Collection, Management and Analysis. Gothenburg: University of Gothenburg, 2009. 45 p.
9. *Karpov Yu.G.* Imitacionnoe modelirovanie sistem. Vvedenie v modelirovanie s AnyLogic 5. SPb.: BHV-Peterburg, 2006. 400 p.
10. *Chekalkin A.A., Skryl' S.V., Minaev V.A.* Kompleksnyj tekhnicheskij kontrol' effektivnosti mer bezopasnosti sistem upravleniya v organah vnutrennih del: uchebnoe posobie dlya vysshih uchebnyh zavedenij MVD Rossii. Ch. 2: Prakticheskie aspekty tekhnicheskoj razvedki i kompleksnogo tekhnicheskogo kontrolya. M.: Goryachaya liniya – Telekom, 2006. 205 s.
11. *Kulakov V.G. i dr.* Zashchita informacii v telekommunikacionnyh sistemah: uchebnik dlya vysshih uchebnyh zavedenij MVD Rossii. Voronezh: VI MVD Rossii, 2002. 300 p.