УДК 004.94

А.А. Герасимов, А.В. Мозговой, К.А. Пугачев, В.А. Кузнецов

Основы формирования имитационного стенда для моделирования действий нарушителя в защищенной информационно-телекоммуникационной инфраструктуре

В статье рассматриваются вопросы и подходы к формированию имитационного стенда для моделирования действий нарушителя в защищенной информационно-телекоммуникационной инфраструктуре, приводятся основные требования к имитационному стенду, указываются основные задачи и перечень угроз информационной безопасности, дается представление о составе имитационного стенда, приводится архитектура имитационного стенда и краткое описание элементов его составляющих.

ger-anton@mail.ru

Ключевые слова:

Моделирование, имитационный стенд, угроза информационной безопасности, средство защиты информации, безопасность.

In this article the questions and approaches to the formation of a simulation stand for modeling of violator's actions in the protected information and telecommunication infrastructure are reviewed, the basic requirements to simulation stand are given, the main objectives and the list of threats to information security are identifed, an idea of the composition of a simulation stand

is given, the architecture of a simulation stand and a brief description of the elements of its components are given.

Keywords:

Modeling, simulation stand, the threat of information security, protecting information means, security.

Моделирование и отработка возможных угроз защищаемой информации, атак на информационные ресурсы и реакций средств защиты информации на данные ситуации достигается путем разработки и практической реализации имитационного стенда для моделирования действий нарушителя в защищенной информационно-телекоммуникационной инфраструктуре (далее ИС) на базе современного оборудования. При моделировании должны учитываться новейшие способы хранения, обработки и передачи информации, способы и методы реализации угроз информации и противодействия им, а также научные достижения в данной сфере.

ИС предназначен для моделирования работы информационной системы при обработке защищаемой информации, моделирования взаимодействия технических средств информационной системы между собой и с необходимыми средствами защиты информации, моделирования работы данной системы в различных режимах работы, учитывающих особенности технологического процесса при реальных условиях функционирования,

моделирования работы информационной системы в условиях реализации различных типов атак и угроз информационной безопасности, а также моделирования реакции средств защиты информации на различные атаки и угрозы.

При проектировании и создании ИС должно учитываться всё разнообразие существующих и потенциальных угроз безопасности информации, их разнонаправленность и наличие множества различных вариантов и средств их реализации. ИС должен давать возможность моделировать указанные ситуации для достижения возлагаемых на него задач. Также должны быть учтены новейшие отечественные и зарубежные разработки в информационной сфере и необходимо проводить постоянный мониторинг научных достижений. ИС должен иметь возможность адаптироваться к изменяющимся условиям в области защиты информации и информационной безопасности, появлению новых средств и способов реализации атак и угроз безопасности информации и защиты от них.

Основными задачами работы ИС являются:

1) накопление, систематизация и реализация передовой научно-технической продукции;
2) обучение студентов на базе ИС;
3) повышение квалификации специалистов на базе ИС;
4) отработка сценариев реализации угроз, нападения и атак злоумышленника на защищаемые ресурсы;

5) проведение исследований технических средств, программного обеспечения и средств защиты информации;
6) формирование базы знаний по проводимым исследованиям;
7) разработка, создание и совершенствование средств защиты информации;
8) анализ уязвимостей существующих и разрабатываемых продуктов;
9) исследование технических каналов утечки информации и связанных с ними угроз;
10) исследование и анализ различных программных закладок;
11) исследование и анализ различных аппаратных закладок;
12) имитация действий злоумышленника в различных ситуациях;
13) имитация атак и угроз безопасности информации;
14) проведение НИР и ОКР.

При создании имитационного стенда должна быть учтена возможность исследования основных угроз безопасности информации:

- угрозы утечки информации по техническим каналам;
- угрозы непосредственного и межсетевого несанкционированного доступа к информации;
- угрозы перехвата информации путем внедрения устройств негласного съема информации.
- угрозы внедрения вредоносных программ;

- угрозы уничтожения, искажения, хищения и модификации технических средств, носителей информации, средств защиты информации, входящих в состав моделируемой информационной системы.

Основными исследуемыми направлениями ИС являются:

- направление, связанное с компьютерной безопасностью;
- направление, связанное с технической защитой информации;
- направление, связанное с обеспечением безопасности телекоммуникационной, информационной и инженерной инфраструктур.

ИС состоит из 5-и серверов: двух файловых, сервера IP-телефонии и видеоконференций и одного сервера приложений с подключаемыми к ним по каналам связи устройствами, моделирующими функционирующую информационную систему. Один из файловых серверов является основным, второй – вспомогательным, между ними предусмотрено зеркалирование информационных ресурсов для защиты их от утери и искажения. К серверу приложений подключаются по каналам связи терминальные системы, предназначенные для работы на ресурсах сервера. Сервер IP-телефонии и видеоконференций предназначен для моделирования IP-связи и видеоконференций в информационной системе. К ИС через коммутаторы К-1 - К-4 подключены 4 группы автоматизированных рабочих мест (АРМ), а также прочие устройства (мобильные устройства, планшеты, видеокамеры),

через коммутатор КВ – камеры системы видеонаблюдения. Подключение АРМ осуществляется с помощью различных типов проводных линий связи (витая пара, коаксиальный кабель, оптоволоконные линии связи), а также беспроводного соединения (Wi-Fi, Wi-Max, Bluetooth) для обеспечения возможности моделирования различных вариантов утечки информации при ее передаче между устройствами по всем типам соединений. Также моделируется выход имитационного стенда в открытые сети связи (в том числе Internet) посредством ADSL-модема, который подключен к одному из АРМ, и других соединений, исходящих непосредственно от ИС. В зависимости от конкретных задач исследования соединительные линии могут считаться защищенными, либо открытыми, выходящими за пределы контролируемой зоны информационной системы и находящимися в ее пределах. Технические средства могут рассматриваться как элементы защищаемой информационной системы (с использованием средств защиты информации либо без них), и как ресурсы злоумышленника. При работе имитационного стенда возможно моделирование процессов удаленного доступа к ресурсам и распределенной обработки данных. Предполагается, что все элементы имитационного стенда расположены в одном помещении.

Схема ИС указана на рисунке 1.

Перечень технических средств ИС: персональный компьютер (12 шт.), файловый сервер (2 шт.), сервер приложений (1 шт.), сервер IP-телефонии и видеоконференций (1 шт.), сервер системы видеонаблюдения (1 шт.),

коммутатор (3 шт.), маршрутизатор (2 шт.), терминалы (3 шт.), ADSL-модем (2 шт.), камера видеонаблюдения (2 шт.), беспроводная камера видеонаблюдения (2 шт.), аппарат сотовой связи (2 шт.), планшетный компьютер (2 шт.), IP-телефоны (4 шт.).

Для исследования информационного взаимодействия защищаемых информационных систем ИС комплектуется средствами защиты информации от ее утечки по различным каналов.

Для исследования программных средств, в том числе средств защиты информации, в ИС должны использоваться средства тестирования.

Для исследования возможности перехвата обрабатываемой в моделируемой информационной системе информации, а также передаваемой по каналам связи, в ИС должны использоваться средства измерения и регистрации информативных сигналов.

Список литературы

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. СПб.: Питер, 2003. 864 с.

2. Гаранин М.В., Журавлев В.И., Кунегин С.В. Системы и сети передачи данных: Учебное пособие. М.: Радио и связь, 2001. 336 с.

3. Кучерявый А.Е., Цуприков А.Л. Сети связи следующего поколения. М.: ФГУП ЦНИИС, 2006. 280 с.

4. Защита информации в телекоммуникационных системах: Учебник для высших учебных заведений МВД России / В.А. Минаев [и др.]. Воронеж: Воронежский институт МВД России, 2002. 300 с.

5. Информационная безопасность телекоммуникационных систем (технические вопросы): Учебное пособие для системы высшего профессионального образования России / А.В. Заряев [и др.]. М.: Радио и связь, 2004. 388 с.

6. Герасимов А.А., Скрыль С.В. Проблема моделирования процессов обеспечения безопасности информации, относящейся к персональным данным // Охрана, безопасность и связь – 2009: Материалы Всероссийской научно-практической конференции. Воронеж, 2009. С. 204-206.

7. Функциональные аспекты аналитико-имитационного моделирования компьютерных систем / А.А. Герасимов [и др.] // Техника и безопасность объектов уголовно-исполнительной системы – 2011: Сборник материалов Международной научно-практической конференции. Воронеж, 2011. С. 329-331.

8. Меньшаков Ю.К. Теоретические основы технических разведок. М.: МГТУ им. Н.Э. Баумана, 2008. 536 с.

9. Советов Б.Я., Яковлев С.А. Моделирование систем: Учебник для вузов. М.: Высшая школа, 2001. 3-е изд., переработанное и доп. 343 с.

10. Герасимов А.А., Мозговой А.В., Черсков Д.А. Принципы моделирования механизмов утечки информации в интересах оценки эффективности противодействия утечке // Информация и безопасность. 2011. Вып. 1. С. 149-150.

11. Бусленко В.Н. Автоматизация имитационного моделирования сложных систем. М.: Наука, 1977. 239 с.

12. Особенности построения и реализации имитационных моделей автоматизированных информационных систем органов внутренних дел / С.В. Скрыль [и др.] // Охрана-97: Доклады Всероссийской научно-практической конференции. Воронеж, 1998. С. 8-11.

13. Золотарева Е.А., Асеев В.Н. Имитационная модель для оценки временных характеристик средств противодействия угрозам безопасности элементов информационной сферы // Информация и безопасность. 2003. Выпуск 2. С. 147-149.

14. Имитационное моделирование механизмов защиты информации / В.К. Джоган [и др.] // Информация и безопасность. 2008. Вып. 2. С. 136-138.

15. Герасимов А.А., Джоган В.К., Мозговой А.В. Имитационная модель информационных процессов в компьютерных системах в условиях обеспечения их защищенности // Информация и безопасность. 2012. Вып. 1. С. 79-84.

References

1. Olifer V.G., Olifer N.A. Computer networks. Principles, technologies, protocols: Textbook for high schools. St. Petersburg.: Peter, 2003. 864 p.

2. Garanin M.V., V. Zhuravlev, S.V. Kunegin. Systems and data networks: Textdook. M.: Radio and communication, 2001. 336 p.

3. Kucheryavy A.E., A.L. Tsuprik. Next-generation communication networks. M.: FSUE CSRI, 2006. 280 p.

4. Data protection in telecommunication systems: Textbook of Russian Ministry of Internal Affairs for higher education / V.A. Minaev [etc.] Voronezh: Voronezh Institute of Ministry of Internal Affairs of Russia, 2002. 300 p.

5. Information security of telecommunication systems (technical issues): Textbook for the system of higher education in Russia / A.V. Zaryaev [etc.] M.: Radio and communication, 2004. 388 p.

6. A.A. Gerasimov, S.V. Skril. The problem of modeling the security of information relating to personal data / / Protection, security and communication - 2009: Proceedings of the All-Russian scientific-practical conference. Voronezh, 2009. pp. 204-206.

7. The functional aspects of the analytical and simulation modeling of computer systems / A.A. Gerasimov [etc.] / / Technique and security of the objects of the correctional system - 2011: Proceedings of the International scientific and practical conference. Voronezh, 2011. pp. 329-331.

8. Menshakov J.K. Theoretical basis of technical intelligence. M.: BMSTU, 2008. 536 p.

9. Sovetov B.J., Yakovlev S.A. Simulation systems: Textbook for high schools. M.: Higher School, 2001. 3rd ed., revised and enlarged. 343 p.

10. A.A. Gerasimov, A.V. Mozgovoy, D.A. Cherskov. Principles of modeling the mechanisms of information leakage in the interest of evaluating the effectiveness counter the diversion of / / Information and Security. 2011. Issue. 1. pp. 149-150.

11. Buslenko V.N. Automation simulation of complex systems. M.: Nauka, 1977. 239 p.

12. Features of construction and implementation of simulation models of automated information systems of the interior affairs agency / S.V. Skril [etc.] / / Guard-97: Reports of All-Russian scientific-practical conference. Voronezh, 1998. pp. 8-11.

13. E.A. Zolotarev, V.N. Aseev. Simulation model for estimating of timing means to counter threats to security elements of the information sphere / / Information and security. 2003. Issue 2. pp. 147-149.

14. Simulation of information security / V.K. Joghan [etc.] / / Information and Security. 2008. Issue 2. pp. 136-138.

15. A.A. Gerasimov, V.K. Joghan, A.V. Mozgovoy. Simulation model of information processes in computer systems while ensuring their protection // Information and security. 2012. Issue 1. pp. 79-84.