УДК 004.94

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

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

МГТУ им. Н.Э. Баумана, Москва, 105005, Россия

Рассмотрены подходы к формированию имитационного стенда для моделирования действий нарушителя в защищенной информационно-телекоммуникационной инфраструктуре. Приведены основные требования к имитационному стенду, указаны основные задачи и перечень угроз информационной безопасности, дано представление о составе имитационного стенда, приведены архитектура имитационного стенда и краткое описание составляющих его элементов.

Ключевые слова: *моделирование действий нарушителя, информационная безопасность, угроза информационной безопасности, средство защиты информации.*

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 (ИС) для моделирования действий нарушителя в защищенной информационно-телекоммуникационной инфраструктуре 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 [1–3].

Имитационный стенд предназначен для моделирования следующих процессов [4, 5]:

- работы информационной системы при обработке защищаемой информации;
- взаимодействия технических средств информационной системы между собой и с необходимыми средствами защиты информации;
- работы данной системы в различных режимах, учитывающих особенности технологического процесса при реальных условиях функционирования;
- работы информационной системы в условиях реализации различных типов атак и угроз информационной безопасности;
- реакции средств защиты информации на различные атаки и угрозы.

При проектировании и создании ИС должно учитываться все разнообразие существующих и потенциальных угроз безопасности информации, их разнонаправленность и наличие множества различных вариантов и средств их реализации. Стенд должен давать возможность моделировать указанные ситуации для выполнения возлагаемых на него задач. Должны быть учтены новейшие отечественные и зарубежные разработки в информационной сфере. Кроме того, необходимо проводить постоянный мониторинг научных достижений. Информационный стенд 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 [6, 7].

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 [8, 9].

При создании ИС должна быть учтена возможность исследования основных угроз безопасности информации, таких как:

• утечка информации по техническим каналам;

• непосредственный и межсетевой несанкционированный доступ к информации;

• перехват информации путем внедрения устройств негласного съема информации;

• внедрение вредоносных программ;

• уничтожение, искажение, хищение и модификация технических средств, носителей информации, средств защиты информации, входящих в состав моделируемой информационной системы [10–12].

Основные исследуемые с помощью ИС направления связаны:

• с компьютерной безопасностью;

• технической защитой информации;

• обеспечением безопасности телекоммуникационной, информационной и инженерной инфраструктур.

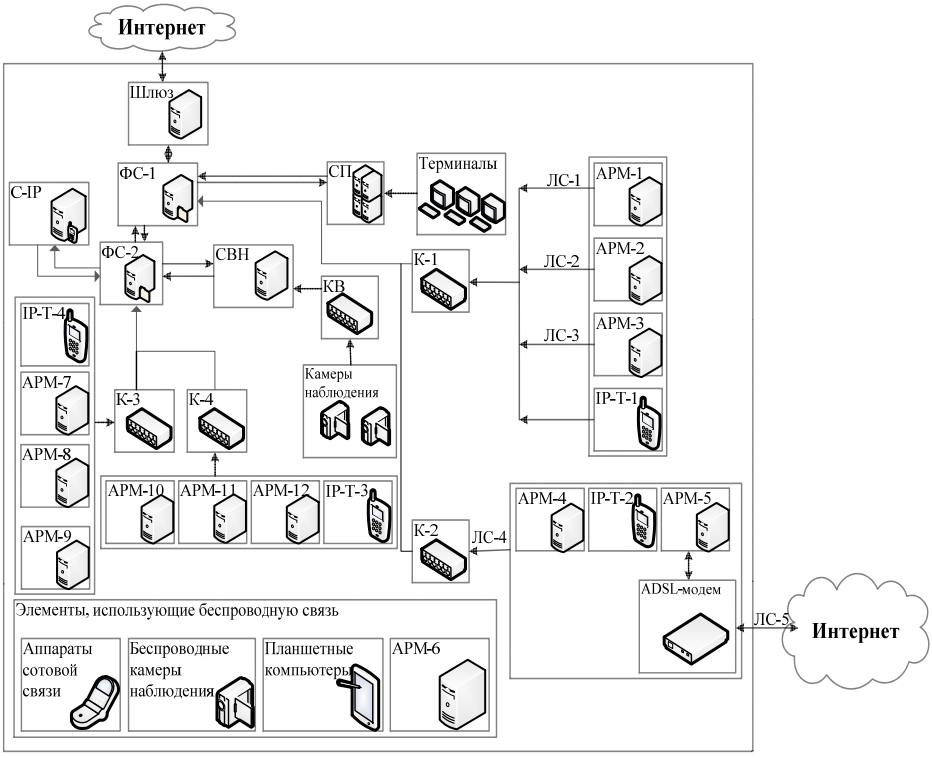

Схема имитационного стенда:

ФС-1, ФС-2 — файловые серверы; СП — серверы приложений; C-IP — сервер IP-телефонии; СВН — сервер видеонаблюдения; К-1, …, К-4, КВ — коммутаторы и маршрутизаторы; IP-T-1, …, IP-T-4 — IP-телефоны; ЛС-1 — оптоволоконный кабель; ЛС-2, ЛС-4 — коаксиальный кабель; ЛС-3 — витая пара; ЛС-5 — телефонный кабель; АРМ-1, …, АРМ-12 — автоматизированные рабочие места

Стенд состоит из пяти серверов (рисунок): двух файловых, сервера IP-телефонии и видеоконференций, сервера системы видеонаблюдения и 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 зеркалиро-

вание 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 имитационному стенду через коммутаторы К-1, …, К-4 подключены четыре группы автоматизированных рабочих мест (АРМ) и прочие устройства (мобильные средства, планшеты, видеокамеры), а 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 путем беспроводного соединения (Wi-Fi, Wi-Max, Bluetooth), благодаря чему появляется возможность моделировать различные варианты утечки информации при ее передаче между устройствами по всем типам соединений. Также моделируется выход ИС в открытые сети связи (в том числе в Интернет) посредством ADSL-модема, который подключен к одному из АРМ, и с помощью 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 [8, 12]. Технические средства могут рассматриваться как элементы защищаемой информационной системы (с использованием средств защиты информации либо без них) и как ресурсы злоумышленника. При работе ИС можно моделировать процессы удаленного доступа к ресурсам и распределенной обработки данных [11–13]. Предполагается, что все элементы имитационного стенда расположены в одном помещении.

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.), терминал (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-телефон (4 шт.).

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

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

Для исследования возможности перехвата информации, обрабатываемой в моделируемой информационной системе, а также передаваемой по каналам связи, в ИС должны использоваться средства измерения и регистрации информативных сигналов [12].

ЛИТЕРАТУРА

[1] Олифер В.Г., Олифер Н.А. *Компьютерные сети. Принципы, технологии, протоколы*. Санкт-Петербург, Питер, 2003, 864 с.

[2] Гаранин М.В., Журавлев В.И., Кунегин С.В. *Системы и сети передачи данных.* Москва, Радио и связь, 2001, 336 с.

[3] Золотарева Е.А., Асеев В.Н. Имитационная модель для оценки временных характеристик средств противодействия угрозам безопасности элементов информационной сферы. *Информация и безопасность,* 2003, вып. 2, с. 147–149.

[4] Заряев А.В., Минаев В.А., Остапенко А.Г., Скрыль С.В. *Защита информации в телекоммуникационных системах*. Воронеж: Воронежский институт МВД России, 2002, 300 с.

[5] Заряев А.В., Новокшанов И.В., Скрыль С.В. *Информационная безопасность телекоммуникационных систем (технические вопросы)*. Москва, Радио и связь, 2004, 388 с.

[6] Советов Б.Я., Яковлев С.А. *Моделирование систем.* 3-е изд. Москва, Высшая школа, 2001, 343 с.

[7] Бусленко В.Н. *Автоматизация имитационного моделирования сложных систем*. Москва, Наука, 1977, 239 с.

[8] Герасимов А.А., Скрыль С.В. Проблема моделирования процессов обеспечения безопасности информации, относящейся к персональным данным. *Охрана, безопасность и связь – 2009. Материалы Всерос. науч.-практ. конф*. Воронеж, 2009, с. 204–206.

[9] Петренко П.Б., Ромендик Р.В., Герасимов А.А., Мозговой А.В. Функциональные аспекты аналитико-имитационного моделирования компьютерных систем. *Техника и безопасность объектов уголовно-исполнительной системы – 2011. Сб. материалов Междунар. науч.-практ. конф.* Воронеж, 2011, с. 329–331.

[10] Меньшаков Ю.К. *Теоретические основы технических разведок*. Москва, Изд-во МГТУ им. Н.Э. Баумана, 2008, 536 с.

[11] 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.

[12] 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.

[13] Кучерявый А.Е., Цуприков А.Л. *Сети связи следующего поколения*. Москва, ФГУП ЦНИИС, 2006, 280 с.

Статья поступила в редакцию 28.06.2013

Ссылку на эту статью просим оформлять следующим образом:

Герасимов А.А., Мозговой А.В., Пугачев К.А., Кузнецов В.А. Основы формирования имитационного стенда для моделирования действий нарушителя в защищенной информационно-телекоммуникационной инфраструктуре. *Инженерный журнал: наука и инновации,* 2013, вып. 11. URL: http://engjournal.ru/catalog/it/security/1018.html

Герасимов Антон Андреевич родился в 1985 г., окончил МГТУ им. Н.Э. Баумана в 2009 г. Канд. техн. наук, доцент кафедры «Защита информации» МГТУ им. Н.Э. Баумана. Автор более 15 статей, 1 монографии и 3 методических указаний по тематике «Защита информации». e-mail: ger-anton@mail.ru

Мозговой Андрей Валериевич родился в 1986 г., окончил МГТУ им. Н.Э. Баумана в 2009 г. Ассистент кафедры «Защита информации» МГТУ им. Н.Э. Баумана. Автор более 10 статей и 1 методических указаний по тематике «Защита информации». e-mail: runc.nsd@gmail.com

Пугачев Кирилл Александрович родился в 1987 г., окончил МГТУ им. Н.Э. Баумана в 2010 г. Ассистент кафедры «Защита информации» МГТУ им. Н.Э. Баумана. Автор 1 статьи и 1 методических указаний по тематике «Защита информации». e-mail: pugachev_ka13@mail.ru

Кузнецов Виктор Александрович родился в 1989 г., окончил МГТУ им. Н.Э. Баумана в 2012 г. Ассистент кафедры «Защита информации» МГТУ им. Н.Э. Баумана. e-mail: viktor_kuznetsov@mail.ru