# АНАЛИЗ ЗАЩИЩЕННОСТИ РАСПРЕДЕЛЁННЫХ СИСТЕМ И МЕТОДОВ ТЕСТИРОВАНИЯ

## SECURITY ANALYSIS OF DISTRIBUTED SYSTEMS AND TESTING METHODS

***O. Rogova***
***T. Dobrzhinskaya***
***E. Fominova***

*Summary.* The basis of work on certification, audit and inspection of security of distributed automated information processing systems is the analysis of their security. This article summarizes the existing experience with security analysis. The article reviews the regulatory framework of this area, methods of security analysis. They are implemented in most government and commercial structures, and protection tools are used in world practice. This article describes common methods and means of protecting information systems. They are used in the practice of security analysis, are successful in the market of information protection.

Keywords: automated system, security, protection, informational infrastructure, computer networks, workstation, distributed systems, server, weakness.

***Рогова Олеся Сергеевна***
*Аспирант, Дальневосточный Федеральный университет*
*kozerog1991@gmail.com*
***Добржинская Татьяна Юрьевна***
*Аспирант, Дальневосточный Федеральный университет*
***Фоминова Екатерина Романовна***
*Аспирант, Дальневосточный Федеральный университет*

*Аннотация.* Основой работы по аттестации, аудиту и обследованию безопасности распределенных автоматизированных систем обработки информации является анализ их защищенности. Данная статья представляет собой обобщение существующего опыта осуществления анализа уязвимости распределенных систем. В статье обозревается нормативная база этой сферы, методы анализа защищенности, реализуемые в большинстве государственных и коммерческих структур, применяемые в мировой практике инструменты защиты. Описываются широко распространенные методы и средства, используемые в практике анализа защищенности, пользующиеся успехом на рынке защиты информации.

*Ключевые слова:* автоматизированная система, безопасность, защищенность, информационная инфраструктура, компьютерные сети, рабочая станция, распределенные системы, сервер, уязвимость.

Формирование информационной инфраструктуры корпоративной распределенной автоматизированной информационной системы (РАИС) с использованием современных сетевых технологий неизбежно сопряжено с проблемой защищенности от угроз и информационной безопасности (ИБ) данной инфраструктуры.

Системы защиты информации (СЗИ) в РАИС представлены двумя независимыми частями. Одна ветвь представлена связью между процессами или пользователями. Они могут располагаться на различных технических средствах (ТС). Принципиально защитить такой способ взаимодействия заключается в организации защищенного канала. Вторая часть СЗИ связана с авторизацией, позволяющей процессам получать исключительный доступ к ресурсам РАИС, которые обеспечиваются соответствующими правами. При этом авторизация и контроль доступом, как правило рассматриваются неразрывно друг от друга.

Анализ защищенности РАИС от угроз БИ представляет сложную процедуру. Специалисты, которые проводят анализу защищенности РАИС в современных условиях, должны владеть профессиональными качествами, связанными с умением оценивания и управления рисками. При этом специалист в области защиты информации обязан определять типовые угрозы и уязвимости, знать критерии, а так же подходы к анализу защищенности. В настоящее время он должен владеть методами и специальными программно-аппаратными инструментами анализа, которые применяются в компьютерных сетях (КС).

На современном этапе алгоритм действий аудиторов существенно различаются вследствие многообразия методик и средств анализа защищенности РАИС. При этом отсутствуют стандартизированные методики такого анализа. Анализ защищенности РАИС, корпоративной КС проводят по типовой методике, эффективность которой многократно подтверждалась на практике.

Используемые методы в типовой методике анализа защищенности РАИС можно разделить на следующие виды:

- анализ исходных данных, относящихся к РАИС, ее структуре;

- оценка рисков, вызванных угрозами ИБ в отношении ресурсов РАИС;
- анализ механизма ИБ организационного уровня. Данная методика также предусматривает анализ политики ИБ организации, документации по обеспечению режима ИБ, а также их оценку согласованности с требованиями актуальных нормативно-технической документации (НТД), соответствия рискам;
- анализ конфигурационного файла ТС. К ним относятся: маршрутизаторы, межсетевые экраны (МЭ), прокси-серверы, которые управляют межсетевым взаимодействием, почтовые серверы и DNS серверы и другие критические элементы РАИС;
- сканирование внешних и внутренних сетевых адресов локальной вычислительной сети (ЛВС) из сети Интернет;
- использование специальных программного обеспечения для конфигурационного анализа рабочих станций и серверов.

Данные методы анализа предусматривают применение активного и пассивного тестирования СЗИ.

Проведение теста СЗИ РАИС осуществляется обусловлено двумя целями. Во-первых, необходимо проверить эффективность механизма СЗИ, используемых в РАИС; устойчивость против потенциальных угроз и атак. Во-вторых, требуется определить уязвимости в защите. Традиционное применение получили два метода тестирования: «черный ящик» и «белый ящик».

В первом случае преимущественно используются сетевые сканеры в качестве основного средства тестирования. Они располагают базами данных (БД) известных уязвимостей.

Во случае использования метода «белый ящик» заключение об уязвимости основывается на анализе конфигурации применяемых СЗИ и системного программного обеспечения (ПО). После этого производится практическая проверка. Основной инструмент — программный агент средств анализа (СА) — используется при анализе защищенности на системном уровне.

ПО, которые позволяют анализировать защищенность РАИС, делятся на два больших класса программ. Первый класс формирует сетевой уровень СА защищенности. К нему относятся сетевые сканеры (СК). Второй класс образуют СА системного уровня защищенности. Здесь находятся иные средства. Каждый класс СА обладает своими достоинствами и недостатками. Однако, при практическом применении они взаимно являются взаимно дополняющими друг друга СА.

Для функционирования СК требуется один компьютер, который обладает сетевым доступом к анализируемой системе. В связи с этим необходимость в установке для каждой анализируемой РАИС своего агента не требуется.

СА защиты, использующие интеллектуальные программные агенты, обладают более высоким потенциалом более в сравнении с СК. В то же время, применение программных агентов полностью заменить сетевое сканирование не может. Эти СЗИ требуют совместного использования. Следует отметить, что СК характеризуются простотой, доступностью, относительной дешевизной, являются более эффективным СА защищенности.

Современные методики анализа защищенности РАИС, основаны на критериальной оценке безопасности информационных технологий. По результатам соответствующего анализа устанавливаются классы и уровни защищенности. Методы и средства обеспечения безопасности с критериями оценок представлены в национальном стандарте ГОСТ Р ИСО/МЭК 15408–1–2012 (2–2013, 3–2013), международном стандарте информационной безопасности ISO 17799 (аналог британского стандарта BS7799–1:1999), а так же в организационно-распорядительных документах, нормативных и методических документах по технической защите информации Федеральной службы по техническому и экспортному контролю (ФСТЭК), других НТД.

К настоящему времени отечественная НТД в сфере анализа СЗИ существенно обновлена и соответствует актуальному состоянию развития ТС, КС, РАИС. Наряду с этим ФСТЭК проводит постоянную актуализацию фонда организационно-распорядительной документации, нормативных и методических документов по технической защите информации. На сегодняшний день техническая защита РАИС регулируется тремя Федеральными законами № 149-ФЗ от 27.07~<2006 г., № 152-ФЗ от 27.06. 2006 г., № 5485–1 от 21.07. 1993 г., пятью указами Президента РФ № 1203 от 30.11. 1995 г., № 188 от 6.03.1997 г., № 351от 17.03. 2008 г., № 646 от 5.12.2016 г., № 569 от 25.11.2017 г., семью приказами и решением ФСТЭК от 5.03.2010 г., № 489 от 31.08.2010 г., № 17 от 11.02.2013 г., № 21от 18.02.2013 г., № 151/786/461 от 31.12.2013 г., № 27 от 15.02.2017 г., № 49 от 23.03.2017 г., Госстандартом ГОСТ Р ИСО/МЭК 15408–1–2002, одиннадцатью руководящими и методическими документами ФСТЭК, 58 национальными стандартами и тремя рекомендациями по стандартизации Росстандарта Российской Федерации.

Схема оценки безопасности РАИС, которая основывается на подходах стандарта ГОСТ Р ИСО/МЭК 15408 позволяет получить реальные результаты защищенности отечественных РАИС. На данных момент подготов-

лены профили защиты для МЭ и других СЗИ, а так же типовые стандартизированные профили защиты. Они соответствуют классам защищенности, которые устанавливаются ФСТЭК. Существует типовая методика анализа защищенности РАИС с использованием специализированного ПО.

Методы анализа защищенности используют как активное, так и пассивное тестирование СЗИ, которое производится ручным способом и с использованием специализированного ПО.

Номенклатура специализированного ПО, предназначенного для анализа защищенности РАИС, представлена достаточно широко. Стоит отметить, что большое количество свободно распространяемого ПО практически не уступают коммерческим образцам. Однако для проведения глубокого анализа защищенности РАИС, существует необходимость использования коммерческого ПО такого уровня как, например, Symantec ESM и Internet Security Systems.

В настоящий момент задачи анализа защищенности РАИС хорошо проработаны. Этому способствует большое количество средств и методов для проведения подобного анализа. Методики, по которым проводятся анализ и аудит безопасности РАИС на соответствие критериям, приведенным в международных и национальных стандартах, дают возможность на практике получить исчерпывающую информацию о ее свойствах, в том числе связанных с ее уязвимостью. Практический анализ защищенности РАИС осуществляется с применением ПО, в достаточном количестве представленном на рынке СЗИ.

ЛИТЕРАТУРА

1. Распределенные системы. Принципы и парадигмы / Э. Таненбаум, М. ван Стеен. — СПб.: Питер, 2003. — 877 с: ил. — (Серия «Классика computer science»)
2. Бабич А.В., Берсенев Г. Б. Алгоритмы динамической балансировки нагрузки в распределенной системе активного мониторинга // Известия ТулГУ. Технические науки. 2011. № . 3. С. 251–261.
3. Цветков В.Я., Алпатов А. Н. Проблемы распределенных систем // Перспективы науки и образования, 2014. № 6(12). С. 31–36
4. Laprie, J.-C: «Dependability — Its Attributes, Impairments and Means.» In Randell, B., Laprie, J.-C, Kopetz, H., and Littlewood, B. (eds.), Predictably Dependable. Computing Systems, pp. 3–24. Berlin: Springer-Verlag, 1995.
5. Pfleeger, C: Security in Computing. Upper Saddle River, NJ: Prentice Hall, 2nd ed., 1997


Журнал «Современная наука: актуальные проблемы теории и практики»

Дальневосточный Федеральный университет