УДК 004.056

М.О. Калинин

Автоматическое управление информационной безопасностью как технология обеспечения целостности защищенных информационных систем

Сформулирована проблема отсутствия целостности защищенных информационных систем. Предложена технология, позволяющая решить данную проблему путем построения и применения концепции автоматического управления информационной безопасностью.

Ключевые слова: информационная безопасность, целостность, управление безопасностью.

Актуальность задач информационной безопасности привела к тому, что сегодня существует множество разнообразных решений и методик, обеспечивающих защиту информации. Традиционные способы, в том числе контроль доступа, аутентификация, аудит, криптография, составляют системообразующий каркас комплекса мер информационной безопасности, реализуемых в рамках построения и внедрения защищенных информационных систем (ЗИС). Такого рода решения характеризуются пассивностью по отношению к множеству угроз информационной безопасности. Их функциональность обеспечивается оперативностью администраторов безопасности, ответственных за применение, сопряжение и настройку средств безопасности.

В силу срабатывания при этом человеческого фактора невозможно добиться гарантированно-перманентной защищенности ЗИС, поскольку администратор не в состоянии отследить все изменения, происходящие в информационной среде (например, множество комбинаций настроек безопасности в современных ОС исчисляется миллиардами). Поэтому в усиление традиционных средств разрабатывается семейство инновационных решений и продуктов, дополняющих базовые: в том числе системы обнаружения вторжений, методы проактивной антивирусной защиты, системы анализа рисков. Цель таких средств – обеспечение активной безопасности и тем самым повышение скорости принятия мер защиты.

Комбинирование традиционных и инновационных методик представляет собой современный подход к реализации информационной безопасности в рамках любой ЗИС. Однако это обусловливает проблему отсутствия целостности ЗИС, которая проявляется в следующем:

– неконтролируемый состав применяемых в рамках одной ЗИС методов, технологий и их реализаций;

– ошибки администрирования безопасности;

– отсутствие взаимоувязанности средств защиты, интегрированных в ЗИС.

В качестве решения данной проблемы предлагаются новые технологии построения ЗИС: разработка безопасных систем «с нуля» с необходимым набором функций (например, ОС HP-UX [1], «доверенные» версии ОС [2]); специальные защитные и контролирующие прослойки в массовых ОС (например, RSBAC [3], GRSecurity [4]); изолирующие (туннельные и шлюзовые) технологии (например, Astaro Security Gateway [5]); делегирующая технология Multiple Independent Levels of Security (MILS) [6]. Однако и такие подходы не гарантируют безопасности ЗИС, так как решают только задачу обоснования и фиксации состава средств защиты. Вариативность предлагаемых решений открывает для злоумышленников новые возможности по нарушению безопасности за счет новых уязвимостей. Выявление и анализ состава ошибок администрирования безопасности, динамический контроль взаимоувязанности комплекса средств защиты при использовании таких технологий не проводится. Стандартный механизм контроля целостности путем контрольного суммирования в данном случае оказывается бесполезен, поскольку не учитывает системность комплекса средств защиты (совпадение сумм для каждого контролируемого компонента не может гарантировать целостность ЗИС в целом). В то же время, нарушения безопасности, возникающие в результате этих проблем, делают бесполезной любые качественные системы защиты. Автором предлагается технология, основанная на автоматическом управлении безопасностью, которая позволит обеспечить целостность ЗИС.

Эффективность противодействия угрозам информационной безопасности определяется не только составом применяемых средств защиты, но и тем, насколько их параметры согласуются с контекстом ЗИС. Контекст ЗИС образуют такие характеристики среды, как особенности информационной среды; условия эксплуатации; назначение и состав используемого системного и прикладного ПО; актуальные угрозы безопасности, а также связи между всеми ними. Таким образом, целостность ЗИС – это состояние взаимного соответствия параметров системного, прикладного ПО и средств защиты.

Обеспечение целостности ЗИС достижимо путем контроля и поддержания взаимоувязанности и единства используемых средств защиты в контексте ЗИС. Решение данной задачи учитывает такие факторы, как:

– применение большого количества ПО с множеством функциональных свойств и настроек;

– гетерогенность сетей, в которых участвуют различные ОС;

– необходимость передачи информации между удаленными компонентами ЗИС;

– необходимость учета изменений контекста ЗИС.

Технология обеспечения целостности ЗИС основывается на принципах:

– использования логической модели, описывающей и предсказывающей поведение ЗИС;

– задания отношений между требованиями безопасности и состояниями ЗИС в виде критериев;

– применения механизма допустимых отклонений безопасности;

– цикличности и перманентности выполняемых проверок безопасности ЗИС и ее адаптации к нарушениям безопасности путем их устранения или переконфигурирования параметров ЗИС.

Реализация этих принципов достигается при параметрическом управлении информационной безопасностью, которое предусматривает использование информации о текущих параметрах ЗИС, оценку безопасности состояний и по классической схеме с обратной связью адаптацию параметров ЗИС к происходящим воздействиям в рамках допустимых отклонений (см. рис.). Такой подход исключает рутинное администрирование ЗИС и обеспечивает динамическое поддержание и контроль безопасности в рамках требований безопасности к ЗИС.

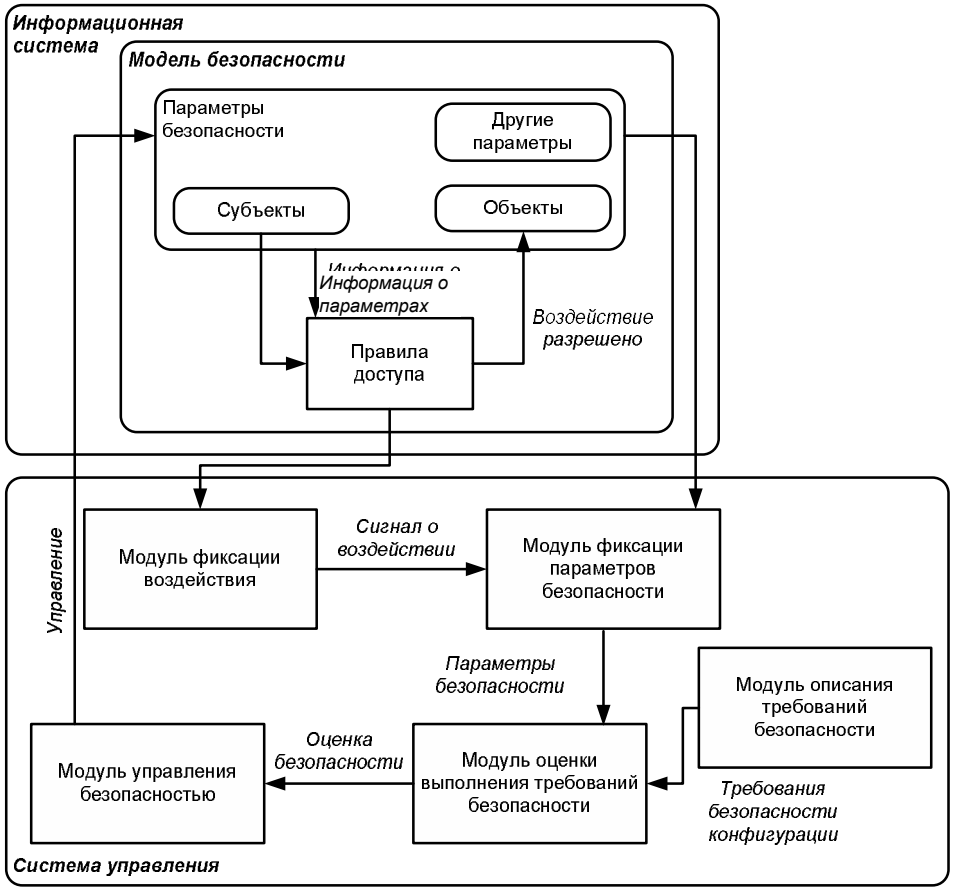

Схема параметрического управления безопасностью ЗИС

Данная технология позволяет контролировать соответствие ЗИС требованиям безопасности, регламентам эксплуатации, назначению и текущим задачам ЗИС, контролировать инвариантность информационной среды по всем компонентам ЗИС, оценивать интегральные характеристики информационной среды ЗИС; вычислять нормализованное представление безопасности конфигурации. Применение данной технологии позволяет оперативно, целенаправленно и эффективно реагировать на негативные изменения, происходящие в ЗИС в процессе ее эксплуатации. За счет присутствия управляющего цикла обеспечивается постоянное поддержание интегральной информационной устойчивости функционирования ЗИС, предотвращая недоступность ресурсов, отказы сервисов, сбои и нарушения безопасного их функционирования, что полностью отвечает необходимости регулярного и перманентного обеспечения безопасности информационных систем [7]. Применение данной технологии позволяет оптимизировать управление информационной безопасностью, повысить эффективность эксплуатации инфраструктуры ЗИС, снизить персональные квалификационные требования.

Литература

1. HPUX, http://docs.hp.com.
2. Trusted Solaris, www.sun.com/software/solaris/ /trustedsolaris.
3. RSBAC, www.rsbac.org/documentation/rsbac_handbook.
4. GRSecurity, http://grsecurity.org.
5. Astaro Security Gateway. http://www.astaro.com/ /our_products/astaro_security_gateway.
6. Alves-Foss J. A multi-layered approach to security in high assurance system development /J. Alves-Foss, C. Taylor and P. Oman // Proc. of 37th Annual Hawaii Int. Conf. on System Science (HICSS–37), – Hawaii, 2004.
7. ГОСТ Р ИСО/МЭК 27001. Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования.

Максим Олегович Калинин
ГОУ ВПО «Санкт-Петербургский государственный политехнический университет», к.т.н., доцент
Эл. почта: max@ssl.stu.neva.ru

M.O. Kalinin
Automatic security control as a technique providing systems integrity
The paper discusses a problem of systems integrity referred to the security components wholeness. A technique is presented to solve this problem with permanent automatic security control.
Keywords: information security, integrity, automatic security control.
