Наличие у производителя или поставщика ПО сертификата, подтверждающего отсутствие в продукции программных закладок, позволяет учитывать последнее обстоятельство вместе с тем, к сертифицированной продукции существенно повышается доверие старых заказчиков, крупных корпоративных потребителей. В нынешних условиях это очень важно.

Технологическая операция по динамическому анализу ПО предусматривает его тестирование. Причем, такое тестирование является углубленным, учитывающим не только функциональные возможности исследуемого ПО, но и его технологические и структурные особенности.

Полезность для разработчика для разработчика такого исследования, выполненного независимой организацией, очевидна.

Кроме того, результаты тестирования могут быть использованы разработчиком при сопровождении своего продукта, а также разработке новых версий или новых программных продуктов.

Следующий важный момент – процесс испытаний на отсутствие НДВ объективно предполагает тесный постоянный контакт испытателя и разработчика, что зачастую позволяет разработчику оперативно улучшать функциональные и потребительские свойства ПО непосредственно в процессе испытаний.

При этом в интересах разработчика испытания могут быть выполнены на его производственной базе.

О потребительских или маркетинговых преимуществах можно сказать следующее:

Государственный документ – сертификат – с определенной степенью вероятности, зависящей от уровня проведенного контроля, подтверждает тот факт, что в проверенном ПО нет явных программных конструкций, использование которых предполагает возможность НСД, нарушения целостности защищаемой информации.

По результатам проведенных испытаний ПО приобретает четкий идентификационный признак – зафиксированные контрольные суммы исходных и исполняемых файлов, позволяющий осуществлять мероприятия по контролю целостности сертифицированного ПО на этапах эго разработки, тиражирования и эксплуатации.

Тот факт, что за доставку к потребителю именно сертифицированного ПО отвечает не только его разработчик, но и проводившая испытания сертификационная лаборатория, которой нормативными документами вменены соответствующие контрольные функции, также имеет немаловажное значение для маркетинга.

Кроме того, рассматриваемый вид испытаний подтверждается соответствующим актом установки именно сертифицированного ПО на объектах конечных пользователей.

Наличие сертификата на отсутствие НДВ является неоспоримым преимуществом для программных решений, претендующих и дальше позиционироваться на государственном рынке СЗИ, поскольку процедура подтверждения и пролонгации действия сертификата, основана на анализе соответствия сертифицированных свойств вновь представляемого на сертификацию продукта по отношению к аналогичным свойствам сертифицированного эталона.

Таким образом, еще раз можно подчеркнуть то, что, используя сертифицированное на отсутствие НДВ в ПО заказчик получает средства, которые с определенной степенью вероятности делают две простые вещи:

корректно и гарантированно выполняют функции по защите его информации;

не имеют встроенных механизмов, позволяющих нанести этой информации вред.

ПРОФИЛЬ ЗАЩИТЫ ДЛЯ ОПЕРАЦИОННОЙ СИСТЕМЫ СЕРВЕРА ДЕМИЛИТАРИЗОВАННОЙ ЗОНЫ

А.И. МАТУК, С.Л. ПУГАЧ, Г.Д. ТОМИНА

1. Роль и место "Критериев оценки безопасности информационных технологий" в сфере защиты информационных технологий.

"Критерии оценки безопасности информационных технологий" ("Критерии") регламентируют все стадии разработки и квалификационного анализа продуктов и систем ИТ, отвечающих требованиям информационной безопасности. "Критерии" устанавливают метрики информационной безопасности и являются основой для создания и развития глобальной системы сертификации безопасности продуктов и систем ИТ. Согласно "Критериям" [1], безопасность ИТ может быть достигнута посредством применения предложенной в них технологии разработки и общей схемы сертификации продуктов и систем ИТ.

"Критерии" позволяют использовать множество независимых частных показателей безопасности и ранжировать требования безопасности по частично упорядоченному набору шкал. Отказ от единой шкалы ранжирования требований безопасности позволяет достичь адекватности реализации средств защиты объекта оценки (ОО) принятой политике безопасности организации, что свидетельствует о преобладании "качества" обеспечения защиты над "количеством" и позволяет потребителю не только приспособить требования к своим нуждам, но и оптимизировать выбор средств защиты по критерию качество/стоимость.

"Критерии" определяют множество типовых требований, которые в совокупности с механизмом Профилей защиты позволяют пользователям создавать частные наборы требований, отвечающие их нуждам. Разработчики могут использовать Профиль защиты как основу для создания спецификаций

своих продуктов. Профиль защиты и спецификации средств защиты составляют Задание по обеспечению безопасности, которое используется для оценки конкретных систем и продуктов ИТ.

Квалификация уровня безопасности является методом определения соответствия продукта или системы ИТ запросам потребителя. Запросы определяются в результате анализа рисков и выбранной политики безопасности организации.

Квалификационный анализ может осуществляться как параллельно с разработкой продукта или системы ИТ, так и после ее завершения.

Схема процесса квалификационного анализа включает три стадии [2]:

1. Анализ Профиля защиты на предмет его полноты, непротиворечивости, реализуемости и возможности использования в качестве набора требований для анализируемого продукта.

2. Анализ Задания по обеспечению безопасности на предмет его соответствия требованиям Профиля защиты, а также полноты, непротиворечивости, реализуемости и возможности использования в качестве эталона при анализе продукта или системы ИТ.

3. Анализ продукта или системы ИТ на предмет соответствия Задания по обеспечению безопасности.

Результаты квалификационного анализа влияют на повышение качества работы производителей в процессе проектирования и разработки продуктов и систем ИТ. В продуктах, прошедших проверку на соответствие уровням гарантии, вероятность появления ошибок, недостатков защиты и уязвимостей существенно меньше, чем в продуктах, не прошедших оценку. Применение "Критериев" позволяет упростить и стандартизировать формирование требований, разработку продуктов ИТ, их оценку и сертификацию.

Основными документами, описывающими все аспекты безопасности продуктов и систем ИТ, с точки зрения пользователей и разработчиков являются соответственно Профиль защиты и Задание по обеспечению безопасности.

2. Профиль защиты

Профиль защиты определяет требования безопасности к определенной категории продуктов и систем ИТ, не уточняя методы и средства их реализации.

Профили защиты распространяются на программные, аппаратные и аппаратно-программные средства обеспечения безопасности.

Профиль защиты определяет необходимый перечень функциональных и гарантийных требований безопасности, предъявляемых к продукту или системе ИТ, при обработке информации, представляющей ценность для собственника (в частности, применительно к Профилю защиты ОС сервера для использования в государственных органах управления – при обработке информации ограниченного распространения, не отнесенной к государственным секретам).

Настоящий Профиль защиты применяется к программным средствам безопасности ОС сервера отечественного и импортного производства при их использовании в демилитаризованной зоне.

Положение настоящего Профиля защиты предполагается сделать обязательным для применения расположенными на территории Республики Беларусь заказывающими органами (потребителями продуктов и систем ИТ), разработчиками таких продуктов и систем, и экспертами (испытателями) в качестве руководства при покупке, разработке, применении и оценке защищенных продуктов и систем ИТ в государственных организациях.

3. Особенности ОС сервера демилитаризованной зоны сети как продукта ИТ.

Объектом оценки, исследуемым в Профиле защиты является ОС сервера общего назначения устанавливаемая на компьютеры-сервера демилитаризованной зоны сети (ДМЗ), имеющей выходы во внешние сети передачи данных.

ОО служит платформой для сетевых приложений ДМЗ, поддерживает защищенную передачу через недоверенную внешнюю сеть при обработке информации ограниченного распространения и может включать специализированные пакеты (service packs, add-ons и т.д.) для расширения основных функциональных возможностей. Обеспечение защиты активов ОО и осуществление политики безопасности выполняет Комплекс средств обеспечения безопасности объекта оценки (КСБО), который представляет собой совокупность программных средств защиты, входящих в состав ОО. Все операции аудита производятся компонентами КСБО.

ОО поддерживает выполнение процессов, активируемых субъектами: исполняемым кодом программ сервисов-приложений, порождающих системные процессы, и пользователями. Пользователи и системные процессы учитываются при всех операциях ОО за счет применения механизмов порождения процессов, которые действуют или от имени конкретного пользователя, или от имени уникально опознаваемого системного процесса. Порожденный процесс запрашивает и использует ресурсы от имени уникального идентификатора, связанного с пользователем или системным процессом.

ОО предназначен для использования в сетевой среде и поддерживает протоколы различного уровня (канальные, сетевые, транспортные, прикладные) для обеспечения одного или более типов связи в сетях различных топологий.

ОО обеспечивает:

а) удаленный доступ к внешнему объекту ИТ через недоверенную сеть (т.е. механизмы, функционирующие в этой ОС, взаимодействуют с механизмами в других продуктах ИТ или с другой ОС для безопасного обмена информацией через недоверенную сеть);

б) доступ к внешнему объекту ИТ, функционирующему в среде объекта оценки;

в) разделяемые ресурсы, совместно используемые в сети, такие как сетевой диск, общие папки и т.д.;

г) виртуальный каталог, т.е. именованные точки подключения пользователя к сервисам-приложениям, функционирующим в среде ОО;

д) многопротокольную маршрутизацию для сетевых пакетов;

е) доступ к службе сетевой регистрации, т.е. именованную точку подключения к серверу регистрации;

ж) назначение уникального идентификатора каждому полномочному пользователю;

и) назначение уникального идентификатора каждому системному процессу, включая те, которые не выполняются от имени пользователя (например, процессы, стартовавшие подобно процессу "inetd" в Unix);

к) аутентификацию полномочного пользователя, прежде чем разрешить ему выполнить любые действия, отличные от установленных для открытого доступа набора безопасных операций (например, чтение с общедоступного Web-сайта);

л) проведение аудита для обеспечения подотчетности действий контролируемых пользователей, для обнаружения возможных нарушений политики обеспечения безопасности объекта оценки (ПБО) и реакции на них;

м) управление разрешением на доступ, т.е. инициализация, назначение и изменение прав доступа (например: чтение, запись, выполнение) к объектам, относительно:

1) имени логического объекта или членства в группе;

2) ограничений, накладываемых условиями эксплуатации (например, время суток и точка входа);

н) управление доступом к приложениям, функционирующим в среде ОО, по правилу: запрет или разрешение;

п) управление соединениями к серверам доверенной зоны по правилу: запрет или разрешение;

р) управление распределением ресурсов с целью воспрепятствовать исчерпанию ресурса;

с) обнаружение некоторых опасных состояний;

т) обеспечение надежного восстановления ОО, в случае системных сбоев, обнаружения опасных состояний;

у) поддержка автоматизированной инструкции для оказания помощи при проверке поставки, инсталляции, функционировании и администрировании ОО.

4. Требования безопасности к современным ОС сервера общего назначения для использования в демилитаризованной зоне корпоративной сети

Предполагается, что ОО не содержит явных недостатков и ошибок разработчиков, установлен и сконфигурирован в соответствии с техническими условиями (ТУ) и нормативно-технической документацией. Контроль корректности функционирования и конфигурации КСБО, а также общий контроль за соблюдением мер безопасности на объекте осуществляет администратор безопасности. ОО должен быть расположен в зоне контроля физического доступа. Профиль защиты рассчитан на два типа санкционированного доступа пользователей: открытый доступ и полномочный доступ. Считается, что технические возможности для осуществления попыток обхода КСБО существуют только при открытом доступе со стороны внешней сети, не контролируемой организацией, при открытом доступе со стороны доверенной зоны возможности обхода КСБО существенно снижаются за счет применения комплекса административных и технических мер защиты доверенной зоны.

ОО может применяться для защиты информации в распределенных информационных системах, используемых в коммерческом секторе и государственных органах.

При использовании в государственных органах ОО обеспечивает минимальные требования защиты:

– при обработке информации, представляющей ценность для собственника;

– при обработке информации ограниченного распространения.

При обработке информации ограниченного распространения, доступ к ней может быть разрешен только полномочным пользователям согласно предписанным ролям.

При использовании в коммерческом секторе ОО обеспечивает:

– базовые требования защиты при обработке информации, представляющей ценность для собственника;

– минимальные требования защиты при обработке информации ограниченного распространения. При обработке информации ограниченного распространения, доступ к ней может быть разрешен только полномочным пользователям согласно предписанным ролям.

При применении в государственных органах и коммерческом секторе ОО используется в информационных системах, в которых главную угрозу безопасности доверенной зоне и ДМЗ представляет внешняя сеть, поэтому главная задача КСБО – противостоять угрозе со стороны внешней сети. Угроза ОО со стороны доверенной зоны для обоих применений закрывается программно-техническими средствами защиты внешних объектов ИТ доверенной зоны. При применении в государственных органах угроза со стороны доверенной зоны закрывается дополнительно организационными мерами.

Профиль защиты обеспечивает следующие функциональные возможности:

– поддержку политики принудительного контроля доступа субъектов к объектам. Политики основаны на идентификации субъекта и разрешают или запрещают действия;

– формирование данных аудита;

– формирование данных, подтверждающих подлинность пользователя;

– просмотр данных аудита;
– ограничения на просмотр данных аудита;
– выборочный просмотр данных аудита;
– избирательный аудит;
– защита журнала данных аудита;
– действия в случае возможной потери данных аудита;
– ограниченное управление доступом;
– управление доступом на основе атрибутов безопасности;
– передача данных пользователя без атрибутов безопасности
– прием данных пользователя без атрибутов безопасности;
– ограниченная защита остаточной информации;
– базовая конфиденциальность обмена данными;
– целостность передаваемых данных;
– обработка отказов аутентификации;
– определение атрибутов пользователя;
– проверка секретов;
– выбор момента времени аутентификации;
– сочетание механизмов аутентификации;
– повторная аутентификация;
– аутентификация с защищенной обратной связью;
– выбор момента времени идентификации;
– связи пользователь-субъект;
– управление режимами работы средств безопасности КСБО;
– управление атрибутами безопасности;
– инициализация атрибутов безопасности;
– управление данными КСБО;
– ограниченный срок действия авторизации;
– роли безопасности;
– тестирование абстрактной машины;
– сбой с сохранением безопасного состояния;
– конфиденциальность передаваемых данных, обеспечиваемая КСБО;
– обнаружение модификации передаваемых данных КСБО;
– автоматическое восстановление;
– обнаружение подмены;
– невозможность нарушения политики безопасности ОО;
– разделение на области КСБО;
– базовая согласованность данных КСБО при взаимных обменах;
– тестирование КСБО;
– максимальные нормы;
– ограничение области применения атрибутов;
– базовое ограничение числа одновременных сеансов;
– блокирование сеанса связи КСБО;
– блокирование сеанса связи пользователем;
– завершение сеанса связи КСБО;
– установленные по умолчанию сообщения о доступе к ОО;
– хронология доступа к ОО;
– открытие сеанса связи с ОО;
– надежный канал передачи данных.

Профиль защиты не обеспечивает:
– поддержку политики контроля доступа, основанную на метках безопасности;
– защиту от преднамеренного злоупотребления полномочными пользователями предоставленными правами доступа;
– приемлемую защиту от сложных атак (например, атаки класса "отказ в обслуживании");
– достаточную защиту от ошибок при инсталляции и конфигурировании ОО и администрировании КСБО.

Уровень гарантии оценки (УГО) для рассматриваемого Профиля защиты выбран как УГО 2 " Структурно тестируемый" в соответствии с СТБ 34.101.3 с необходимыми усилениями (УГО-ДМЗ).

Уровень гарантии ПЗ выбран исходя из следующих соображений:

– УГО-ДМЗ соответствует уровню гарантий поставляемых на рынок серийных ОС серверов;
– затраты на проведение сертификационных испытаний по более высокому уровню гарантии оценки, производимые третьей стороной высоки и нецелесообразны

В то же время меры защиты ОС сервера с гарантиями УГО-ДМЗ достаточны для управления группами пользователей и обеспечивают защиту от простых атак.

Литература

1. СТБ 34.101.1-3 Информационная технология. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. 2001.

2. Common Evaluation Methodology for Information Technology Security. Version 0.6 11.01.97

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ХАОС-ПРЕОБРАЗОВАНИЙ

В.А. ЧЕРДЫНЦЕВ, А.Н. МОЛОСНОВ

Преобразование сообщений на основе нелинейных динамических систем (НДС) обеспечивает относительно высокую степень защиты информации в каналах связи. Рассматривается класс преобразований, использующих нелинейные дифференциальные уравнения и нелинейные отображения. Формулируются условия неискажённого воспроизведения сообщений, оценивается влияние мультипликативных и аддитивных помех на качество обобщённой синхронизации систем.

Даётся классификация методов модуляции хаос-процессов, порождаемых НДС: линейные и нелинейные. Линейные методы основаны на отображениях вида:

$$x_{n+1} = \lambda_n + F(x_n,...,x_{n-k}),$$

где λ_n – сообщение, x_n – преобразованное сообщение, $F(...)$ — нелинейная функция.

Нелинейные методы предполагают модуляцию параметров и начальных условий в отображении:

$$x_{n+1} = F(x_n,...,x_{n-k},\lambda_n)$$

Обсуждаются вопросы синхронизации прямых и обратных преобразователей в присутствии аддитивных и мультипликативных канальных помех. Формулируются условия обеспечения качественной синхронизации и выделения сообщений. Приводятся примеры построения систем передачи данных с хаос-процессами.

Показано, что простейшие НДС (1, 2-го порядков) обеспечивают эффективное хаотическое кодирование и декодирование данных. Приводятся результаты моделирования хаос-преобразователей.

Приводятся примеры построения псевдохаотических генераторов для криптографии, стойкость которых обеспечивается чувствительностью к начальным условиям и вычислительной непредсказуемостью одномерных отображений.

ПРЕОБРАЗОВАНИЕ ДИСКРЕТНЫХ СООБЩЕНИЙ В КАНАЛАХ С ЗАЩИТОЙ ИНФОРМАЦИИ

А.Н. МОЛОСНОВ, Ю.А. ТИХАНОВИЧ, П.В. ЛУЧЕНОК

Рассмотрены системы, описываемые нелинейными отображениями фрактального типа, обеспечивающие прямое и обратное преобразование сообщений в каналах с защитой информации:

$$x_{n+1} = k_1 F(x_n) + y_n$$

$$x_n = k_2 F(x_{n-1})$$

где x_n – преобразованное сообщение, $F(...)$ – нелинейная функция, y_n – сообщение.

Возможны два режима работы системы: генерация хаотических колебаний и нелинейное преобразование сообщения.

Выявлены условия, при которых возникает режим хаотических движений в системе. Показана возможность восстановления сообщений в случае действия аддитивных помех в канале передачи.

Обсуждаются вопросы синхронизации генераторов хаотических колебаний на передающей и приёмной сторонах, влияние канальных помех на качество синхронизации.

За счёт включения линейного фильтра с оптимальными характеристиками на выходе обратного преобразователя снижается вероятность ошибочного воспроизведения информационных символов y_n.

Приведены результаты моделирования системы. Приводятся трёхмерные отображения состояний системы при различных параметрах преобразований.

Показана возможность повышения качества криптозащиты информации за счёт использования комбинационного построения генераторов хаотических последовательностей.

ШИРОКОПОЛОСНАЯ СИСТЕМА СВЯЗИ С ЗАЩИТОЙ ИНФОРМАЦИИ

Д.А. ГОЛОВАЧ, Н.А. ДЕЕВ

Рассмотрена система передачи сообщений, использующая скремблированный ЧМ-сигнал $s(t)$ в качестве скремблирующих последовательностей, обеспечивающих расширение спектра ЧМ-сигнала, используется двоичная $\{\pm 1\}$ случайная последовательность (ДСП) $g(t)$ с тактовой частотой $f(t)$. Последовательностью $g(t)$ осуществляется фазовая манипуляция ЧМ-сигнала. Для обеспечения