Д. А. Мельников, В. Р. Петров, Е. В. Дириенко, А. А. Абрамов, И. А. Корсаков, С. С. Кузьминов

МОДЕЛЬ КОМПЬЮТЕРНОГО ШПИОНАЖА СИСТЕМЫ СЕТЕВОГО ВРЕМЕНИ (СИНХРОНИЗАЦИИ) И ЕГО ВОЗМОЖНЫЕ ПОСЛЕДСТВИЯ[1]

Система синхронизации времени в информационно-технологических сетях (ИТС) — обязательная и чрезвычайно важная подсистема, которая влияет на функционирование практически каждого сетевого компонента и ресурса [1, 2]. Точность сетевого времени (синхронизации) не только имеет технологическое значение, но и становится фактором, влияющим на надежность и качество проведения разного рода юридически значимого электронного документооборота, основанного на применении меток времени, и выполнение криптографических функций и вычислений. Вместе с тем поддержание качественной синхронизации сетевого времени зависит от надежности (корректности) функционирования:

1) программно-аппаратных модулей времени, имеющихся в операционной системе (ОС) каждого компьютера, сервера и сетевого устройства. Последнее напрямую зависит от надежности (корректности) функционирования ОС;

2) подсети синхронизации (инфраструктура сетевого времени), которая реализована на основе протокола сетевого времени (Network Time Protocol 4 version — NTPv4-протокол) [1, 3].

Компрометация одного из перечисленных компонентов (модулей времени, ОС и подсети синхронизации или ее сегментов) приводит к дискредитации целых прикладных систем и служб.

Система формирования меток времени в программно-аппаратном комплексе

В любом программно-аппаратном комплексе (ПАК) (компьютере, коммутаторе и др.) имеется генератор тактовой частоты, который является основой формирования времени и частоты синхронизации. Блок-схема формирования системного времени, используемого в метке времени, представлена на рис. 1.

В современных ПАК системное время формируется на основе генератора тактовых импульсов и двух счетчиков секунд (основного и дублера). Другими словами, дата (число, месяц и год) и время (часы, минуты и секунды) описываются определенным количеством секунд (как степень числа 2), а точность текущего времени определяется дробной частью, которая описывает доли секунды (рис. 2а, 2б, 2в) [3].

[1] Данная работа выполнена в НИЯУ МИФИ при финансовой поддержке Министерства образования и науки Российской Федерации в рамках проекта «Создание инженерно-технических решений для высокотехнологичного производства инновационных программно-аппаратных средств защиты информации на базе перспективных высокоскоростных интерфейсов информационного взаимодействия», выполняемого совместно с ООО «ОКБ САПР» по договору № 02.G25.31.0050.

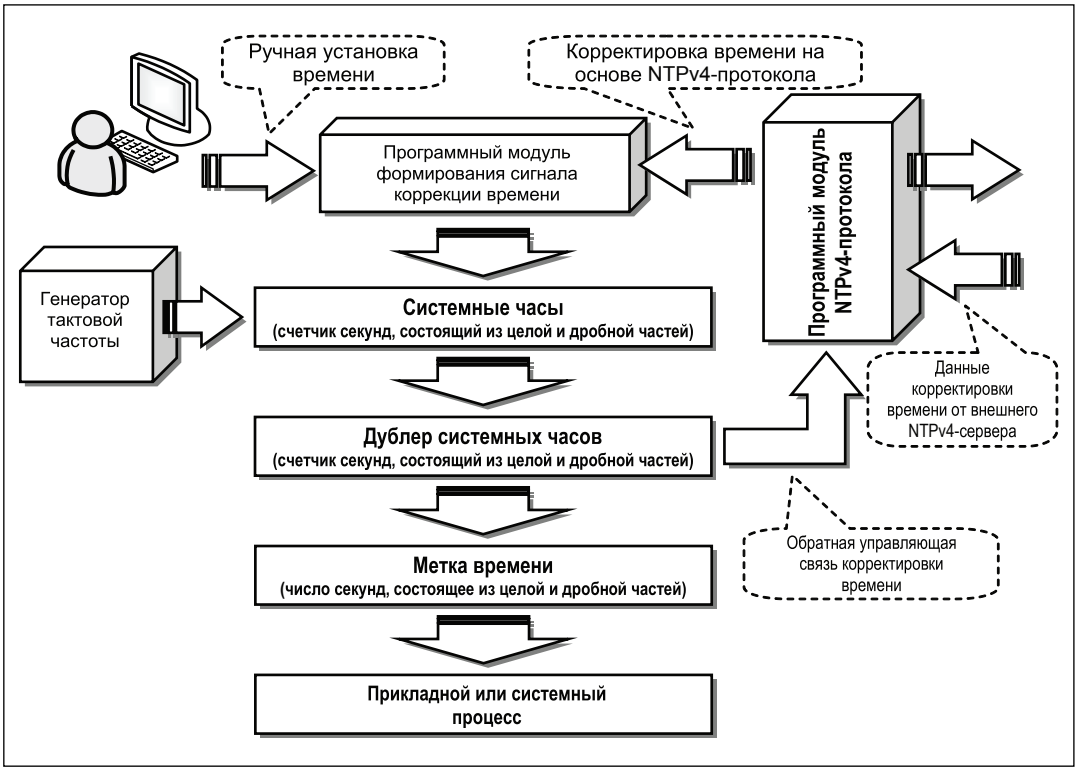

Рис. 1. Блок-схема формирования системного времени

0 15	*16 31*
Секунды	Доли секунды

Рис. 2а. 32-битовый укороченный формат NTP-времени

0 31
Секунды
Доли секунды

Рис. 2б. 64-битовый формат метки времени

0 31	
Номер эпохи	} Секунды
Сдвиг относительно точки отсчета эпохи	
Доли секунды	

Рис. 2в. 128-битовый формат даты

Основной счетчик времени функционирует постоянно, прерываясь только на корректировку значения текущего времени, при этом учитывается необходимый интервал времени, затраченный на корректировку. Счетчик-дублер полностью повторяет значение времени, показываемое основным счетчиком, и используется для считывания текущего времени в интересах системных и прикладных процессов, а также для формирования корректирующего значения времени NTPv4-протоколом (в определенные интервалы).

В некоторых ОС дробная часть дублирующего счетчика секунд используется в качестве генератора случайных чисел. В реальной ситуации момент считывания текущего значения времени

является случайным событием, и поэтому дробная часть секунды может восприниматься как случайное двоичное число. Действительно, практически невозможно предугадать прошедшее число миллисекунд, микросекунд и тем более наносекунд с момента целого числа секунд.

Модель КШ по модификации системного времени в ПАК

Одним из требований (условий) обеспечения высокого уровня информационной безопасности является *надежность (гарантированность) функционирования* ПАК, обеспечивающих, в свою очередь, функционирование средств защиты данных [2]. Любая процедура, напрямую обеспечивающая реализацию способа безопасности или доступ к услуге по обеспечению безопасности, должна заслуживать доверия.

В настоящее время буквально повсеместно используются ОС, которые не отвечают указанному требованию и являются недоверенными (ненадежными). Другими словами, такие ОС весьма трудно проверить на корректность функционирования тех или иных системных и прикладных процессов. К сожалению, «жизнь» подтверждает парадигму Министерства обороны США: «компьютерам, в принципе, доверять нельзя» (это относится к массовым коммерческим компьютерам) [1].

Рассмотрим следующую возможную атаку (модель компьютерного шпионажа, КШ) на систему формирования текущего времени в программно-аппаратном комплексе (рис. 3) [1].

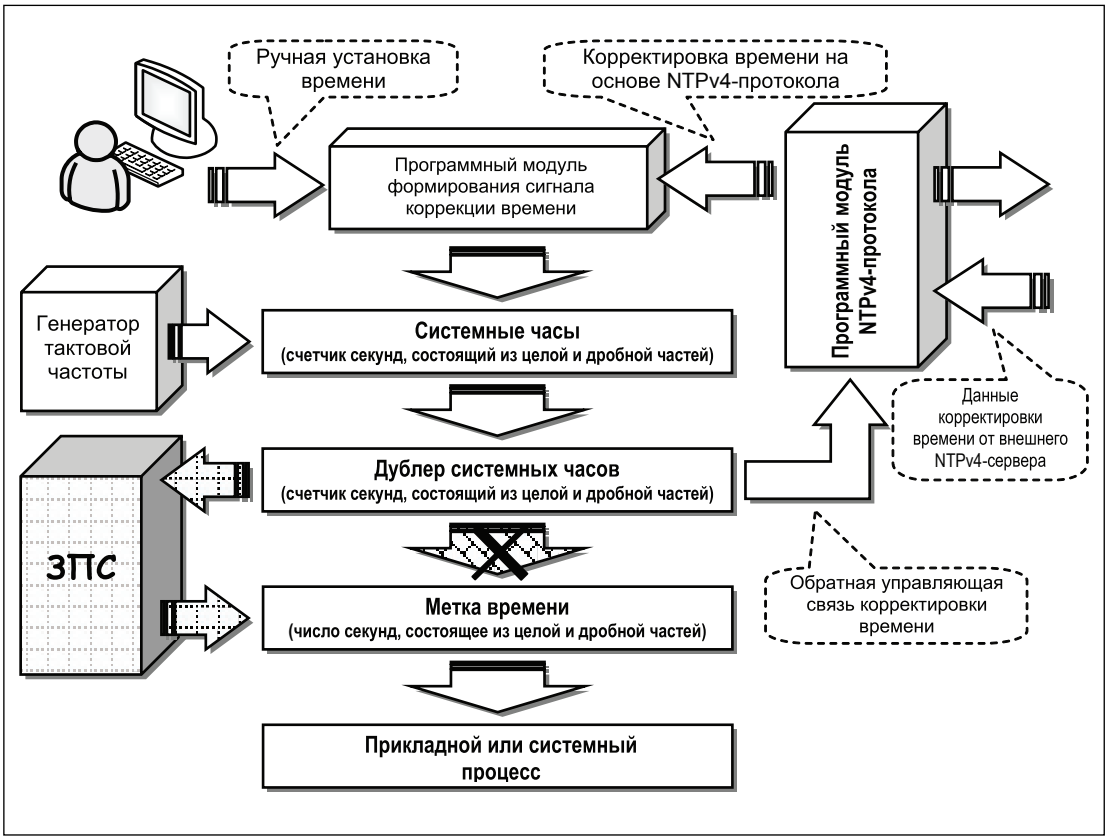

Рис. 3. Модель КШ на основе внедрения ЗПС в целях модификации текущего значения времени

В основе этой атаки лежит внедрение закладного программного средства (ЗПС) в недоверенную ОС для модификации текущего значения времени. Сущность функционирования ЗПС заключается в изменении по заранее известному алгоритму дробной части (долей секунд)

системного времени. Например, алгоритм формирования дробной части может быть основан на определенной процедуре преобразования целой части значения текущего времени, то есть дробная часть текущего времени будет напрямую зависеть (будет функцией) целой части текущего времени. Сформированная таким образом метка времени будет состоять из реальной (истинной) целой части текущего времени и модифицированной дробной части (не случайной, а псевдослучайной).

Нарушитель, который внедрил ЗПС в недоверенную ОС, знает алгоритм преобразования целой части текущего времени в его дробную часть. Следовательно, нарушителю необязательно знать географическое место скомпрометированного ПАК, ему достаточно знать часовой пояс, в котором находится указанный комплекс. С точки зрения обнаружения такого ЗПС выявить модификацию дробной части текущего времени будет чрезвычайно трудно по следующим причинам:

1) весьма трудно только по каким-либо внешним признакам отличить случайную дробную часть текущего значения времени от псевдослучайной, учитывая, что дробная часть состоит из миллисекунд, микросекунд и даже наносекунд, например, при использовании дробной части в качестве основы при формировании случайного числа;

2) даже если вести определенную статистику формируемых меток текущего времени, вряд ли удастся вскрыть алгоритм преобразования целой части в дробную при условии, что нарушитель использовал в ЗПС криптографически сложную функцию;

3) если в течение одной секунды будет востребовано несколько меток времени, то тогда в ЗПС можно добавить соответствующие коэффициенты усложнения, которые будут вносить различие между дробными частями меток времени при модификации одного и того же целого числа секунд. Число таких коэффициентов усложнения зависит от быстродействия скомпрометированного программно-аппаратного комплекса;

4) при такой модели КШ функционирование ЗПС не влияет на работу других компонентов программно-аппаратного комплекса, а также на процедуры, осуществляемые программным NTPv4-модулем. Другими словами, корректно встроенное ЗПС «не позволит себя обнаружить» через какие-либо системные или прикладные процессы.

При реализации рассмотренной модели КШ (на основе встраивания ЗПС) последующие мероприятия нарушителя могут привести к чрезвычайно «тяжелым» последствиям.

Возможные последствия КШ на основе модификации системного времени в ПАК

Основная цель модификации системного времени — это вскрытие секретного (закрытого) ключа объекта КШ на основе знания метки времени и перехвата его ЭЦП в инфраструктуре открытых ключей (Public Key Infrastructure — PKI) [4]. С точки зрения компрометации ИБ внедрение ЗПС обеспечивает «практически» безграничный несанкционированный доступ к защищаемой информации.

Содержание мероприятий КШ[2] после внедрения ЗПС может быть следующим:

1) перехват ЭЦП объекта КШ (владельца скомпрометированного компьютера);

2) регенерация метки времени в ЭЦП. Количество вариантов метки времени зависит от выбранного интервала анализа времени, но не более 5 минут, числа секунд в минуте (60 секунд) и числа коэффициентов усложнения. Общее количество вариантов не будет превышать 3000;

3) зная месторасположение метки времени в ЭЦП, можно получить последовательность «чистой шифргаммы» (точнее 3000 ее вариантов) и провести целенаправленный криптоанализ. Длина «шифргаммы» зависит от используемой метки времени и может составлять 128 бит. В результате дешифровки можно вскрыть секретный (закрытый) ключ объекта КШ (в том случае, если ЗПС внедрено в его компьютер);

[2] В данном случае речь идет о криптоаналитической атаке «подбор открытого текста». В этой атаке в качестве «подобранного открытого текста» выступает фальсифицированная метка времени.

4) если же объект КШ ведет информационный обмен с владельцем скомпрометированного компьютера, то, используя вскрытый секретный (закрытый) ключ последнего, можно вскрыть ключ объекта КШ;

5) в дальнейшем поэтапно можно вскрыть секретные ключи всех пользователей, которые осуществляют защищенный информационный обмен с владельцем скомпрометированного компьютера.

Более детальный анализ показывает, что компрометация нескольких программно-аппаратных комплексов может привести к компрометации всей системы открытых ключей (PKI-инфраструктуры). Естественно, компрометация не произойдет в один момент, это будет целый комплекс целенаправленных и последовательных мероприятий КШ. Но конечный результат очевиден.

Аналогичная ситуация может сложиться с протоколом «Kerberos» [5, 6], который уязвим к атакам на системы сетевой синхронизации и меток времени. Системы с одноразовыми паролями также «бессильны» перед КШ на основе модификации системного времени в ПАК [7].

Другие модели КШ системы сетевой синхронизации

Рассмотренная ранее модель КШ системы сетевой синхронизации на основе внедрения ЗПС относится к группе мероприятий КШ, при реализации которых эту систему рассматривают как источник КШ. Однако такая система становится источником только после внедрения ЗПС, а при проведении комплекса мероприятий КШ по внедрению «закладки» система сетевой синхронизации рассматривается как объект КШ.

Инфраструктура сетевой синхронизации на основе NTPv4-протокола может выступать в двух аспектах:

1) вспомогательный, как источник и/или средство проведения КШ против выбранного объекта;

2) целевой, как объект КШ.

С точки зрения функциональных мероприятий КШ инфраструктуры сетевого времени включает:

- комплекс пассивных мероприятий;
- комплекс активных мероприятий.

Конкретные мероприятия [1], входящие в указанные комплексы, представлены на рис. 4.

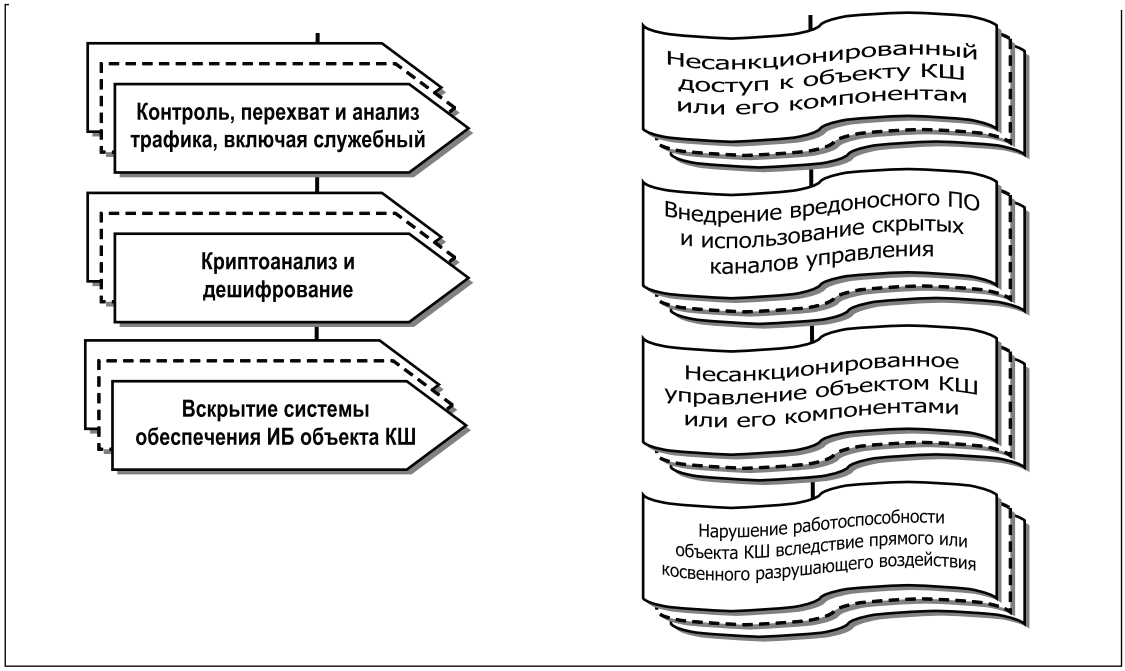

Рис. 4. Модель КШ ИТС

СПИСОК ЛИТЕРАТУРЫ:

1. *Мельников Д. А.* Организация и обеспечение безопасности информационно-технологических сетей и систем: Учебник. М.: Университетская книга, 2012.
2. *Мельников Д. А.* Информационная безопасность открытых систем: Учебник. М.: ФЛИНТА, Наука, 2013.
3. *Mills D.* Network Time Protocol Version 4: Protocol and Algorithms Specification. RFC-5905, June 2010.
4. *Cooper D.* Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC-5280, May 2008.
5. *Kohl J., Neuman C.* The Kerberos Network Authentication Service (V5). RFC-4120 (RFC-4537), July 2005.
6. *McNamara J.* Secrets of Computer Espionage: Tactics and Countermeasures. New York: John Wiley & Sons, Inc., 2003.
7. *Haller N., ed.* A One-Time Password System. RFC-2289, February 1998.