Получение достоверных значений показателей надежности МПЦ затруднено ввиду сложности систем, отсутствия адекватных математических моделей и методов анализа надежности, отсутствия достоверной информации о надежности используемой элементной базы и ПО. Имеющиеся статистические оценки показателей надежности МПЦ также недостаточно точны, т. к. получены по ограниченному статистическому материалу, предоставляются, зачастую, лишь для служебного пользования, не являются устойчивыми, в следствии постоянной модернизации систем, используемой элементной базы и ПО. Большинство существующих математических моделей и методов являются недостаточно адекватными при исследовании высоконадежных МПЦ. Вместе с тем они вполне применимы для сравнения нескольких систем (что актуально при внедрении одной из нескольких существующих МПЦ, аналогичных по функциональности и стоимости) или нескольких вариантов ее организации (при разработке новых МПЦ).

Методы обеспечения безотказности функционирования современных МПЦ связаны в той или иной степени со следующими подходами: использование высоконадежной элементной базы, а также использование элементной базы с несимметричными отказами и специальных методов построения безопасных схем; использование аппаратного (пространственного) и информационного (временного) резервирования; использование диверситетного программного и аппаратного обеспечения.

Выполнены расчеты безотказности таких современных систем МПЦ, как «Ebilock-950», «Alister» (Швеция), «SIMIS» (Германия), «ESA-11» (Чехия), «ЭЦ-ЕМ» (Россия) и «іпуть» (Белоруссия). Сравнение структур построения современных МПЦ, а также расчеты их безотказности и безопасности функционирования показывают:

– невозможно констатировать безусловное преимущество одной структуры МПЦ над другой, поскольку большое значение в этом вопросе, наряду с указанными выше, имеют используемые подходы обеспечения безопасности функционирования системы (информационное и временное резервирование; диверситетное аппаратное и программное обеспечение);

– для МПЦ западной Европы характерно использование бесконтактных схем увязки с объектами управления, которые входят в структуру самой МПЦ. Для МПЦ производства стран восточной Европы и США характерно использование релейных схем увязки, которые накладывают определенные ограничения на быстродействие и долговечность данной подсистемы, поскольку нуждаются в мероприятиях по поддержанию ресурса;

– для обеспечения заданных нормативных значений показателей надежности МПЦ целесообразно резервирование как можно большего количества подсистем, включая некоторые подсистемы исполнительного уровня.

УДК 621.38

# ЭФФЕКТИВНОСТЬ БИОМЕТРИЧЕСКИХ СРЕДСТВ АУТЕНТИФИКАЦИИ В СИСТЕМАХ УПРАВЛЕНИЯ НА ТРАНСПОРТЕ

*П. М. БУЙ*

*Белорусский государственный университет транспорта, г. Гомель*

Реализация процедур опознания, которые включают в себя идентификацию и аутентификацию, является общей проблемой для любых управляющих систем, в которых требуется обеспечивать разграничение доступа к обрабатываемой информации. Особенно актуален этот вопрос для систем, управляющих стратегическими процессами в транспортных отраслях народного хозяйства.

Функционирование всех механизмов разграничения доступа, использующих аппаратные или программные средства, основано на предположении, что любой субъект системы представляет собой конкретное лицо. Следовательно, существует некоторый механизм, обеспечивающий установление подлинности субъекта, обращающегося к системе. Идентификация – это процесс распознавания субъекта с помощью заранее присвоенного идентификатора. Аутентификация – это процесс, заключающийся в проверке подлинности субъекта.

Средство аутентификации – это программный модуль или аппаратно-программное устройство, которое обеспечивает проверку подлинности субъекта, т. е. устанавливает, является ли он тем, за кого себя выдает.

В общем случае существуют три класса опознания, на основании которых строятся все средства аутентификации. Эти классы базируются [1]:

а) на условных, заранее присваиваемых признаках (сведениях), известных субъекту (парольные средства аутентификации);

б) физических средствах, действующих аналогично физическому ключу (средства аутентификации с использованием смарт-карт или электронных ключей);

в) индивидуальных характеристиках субъекта, его физических данных, позволяющих выделить его среди других лиц (биометрические средства аутентификации).

Основным показателем эффективности средства аутентификации является вероятность пропуска «чужого» субъекта данным средством с первой попытки – вероятность такого события, когда «чужой» субъект в результате однократного представления аутентификатора будет опознан в качестве «своего».

В настоящее время в системах управления на транспорте используются в основном средства аутентификации первых двух классов.

Для этих средств аутентификации опознание субъекта считается успешным при абсолютном совпадении всех сравниваемых признаков входного воздействия, предоставленного этим субъектом, и эталонного, хранящегося в памяти средства аутентификации. Это обусловлено тем, что результат преобразования признаков, предоставляемых одним и тем же субъектом, в понятный средству аутентификации вид всегда имеет одинаковые значения. В связи с этим вероятность пропуска «чужого» субъекта (подбора аутентификатора) средством аутентификации с первой попытки определяется известной формулой [2]:

$$P_{\text{ПА1}} = \frac{1}{A^n}, \qquad (1)$$

где $A$ – алфавит пароля, PIN-кода или серийного номера электронного ключа или смарт-карты; $n$ – количество символов пароля, PIN-кода или серийного номера электронного ключа или смарт-карты.

Биометрические средства аутентификации – это устройства, основанные на опознании субъекта по его индивидуальным характеристикам, физическим данным, позволяющим выделить его среди других субъектов. В таких средствах аутентификации проверка подлинности субъекта осуществляется на основании предоставляемого им биометрического признака, в качестве которого может использоваться отпечаток пальца, сетчатка или радужная оболочка глаза, форма или термограмма лица, почерк, голос и т. п.

Отличие биометрических средств аутентификации от средств первых двух классов заключается в том, что для принятия решения об аутентичности субъекта в биометрических средствах аутентификации используется понятие порога меры близости. Порог меры близости – это такое значение меры близости предоставляемого субъектом признака с эталонным, при не превышении которого субъект считается «своим», а при превышении – «чужим». Использование порога меры близости связано с тем, что невозможно достичь абсолютной идентичности предоставляемого субъектом признака с эталонным.

Поэтому при определении вероятности пропуска «чужого» субъекта биометрическим средством аутентификации с первой попытки необходимо использовать следующие подходы:

– дискретизация исследуемого биометрического образа, которая заключается в его оцифровке и последующей обработке;

– нормирование оцифрованного биометрического образа и заданного порога его меры близости с эталонным;

– параметрическое сравнение нормированного оцифрованного биометрического образа с эталонным.

Для каждого биометрического средства аутентификации данные трех подходов реализуются индивидуально, но для вывода аналитических выражений для определения вероятности пропуска «чужого» субъекта с первой попытки необходимо выполнить все указанные подходы строго в заданной последовательности.

Используя данную методику, были получены аналитические выражения для оценки эффективности реальных биометрических средств аутентификации по отпечатку пальца, образцу голоса и радужной оболочке глаза [3, 4]. В дальнейшем планируется проведение исследований с биометрическими средствами аутентификации по геометрии руки, сетчатке глаза и пр.

Результаты оценки эффективности исследованных средств аутентификации (таблица 1) показывают, что при различных значениях порога меры близости, а также ряда других переменных параметров, индивидуальных для каждого средства аутентификации, вероятность подбора биометрического аутентификатора с первой попытки варьируется от $10^{-3}$ до $10^{-9}$. Что соответствует вероятности подбора цифрового пароля из трех–девяти символов. При дальнейшем уменьшении порога меры близости вероятность подбора аутентификатора также уменьшается, однако работа средства аутентификации с такими параметрами приводит к возрастанию вероятности блокировки «своего» субъекта, что уменьшает доступность средства аутентификации законному пользователю.

*Таблица 1*

| Средство аутентификации | Порог меры близости | $P_{ПА1}$ | Средство аутентификации | Порог меры близости | $P_{ПА1}$ |
|---|---|---|---|---|---|
| По отпечатку пальца | 0,55 | $1{,}461 \cdot 10^{-7}$ | По радужной оболочке глаза | 0,4 | 1 |
| | 0,6 | $1{,}461 \cdot 10^{-7}$ | | 0,45 | 0,999 |
| | 0,65 | $1{,}972 \cdot 10^{-8}$ | | 0,5 | 0,5 |
| | 0,7 | $1{,}972 \cdot 10^{-8}$ | | 0,55 | $7{,}175 \cdot 10^{-4}$ |
| | 0,75 | $1{,}972 \cdot 10^{-8}$ | | 0,6 | $9{,}148 \cdot 10^{-11}$ |
| | 0,8 | $1{,}972 \cdot 10^{-8}$ | По образцу голоса | 0,85 | $0{,}501 \cdot 10^{-3}$ |
| | 0,85 | $2{,}381 \cdot 10^{-9}$ | | 0,9 | $2{,}523 \cdot 10^{-5}$ |
| | 0,9 | $2{,}381 \cdot 10^{-9}$ | | 0,95 | $2{,}391 \cdot 10^{-8}$ |

**СПИСОК ЛИТЕРАТУРЫ**


1 *Бобов, М. Н.* Обеспечение безопасности информации в телекоммуникационных системах / М. Н. Бобов, В. К. Конопелько. – М.: БГУИР, 2002. – 164 с.

2 *Смит, Ричард Э.* Аутентификация: от паролей до открытых ключей / Ричард Э. Смит. – М.: Издательский дом "Вильямс", 2002. – 432 с.

3 *Бобов, М. Н.* Оценка уровня защищенности средства аутентификации по отпечатку пальца / М. Н. Бобов, П. М. Буй // Управление защитой информации. – 2008. – № 1. – С. 58–64.

4 *Бобов, М. Н.* Оценка уровня защищенности голосового средства аутентификации / М. Н. Бобов, П. М. Буй // Информатика. – 2008. – № 1(17). – С. 31–37.



УДК 621.3.


# ФОРМИРОВАНИЕ ТРЕБОВАНИЙ К СРЕДСТВАМ ВСТРОЕННОЙ ДИАГНОСТИКИ ИСТОЧНИКОВ СИНХРОСИГНАЛОВ В СЕТИ ТАКТОВОЙ СЕТЕВОЙ СИНХРОНИЗАЦИИ


*А. К. КАНАЕВ, В. В. КРЕНЕВ, Е. В. ОПАРИН*

*Петербургский государственный университет путей сообщения, Российская Федерация*

*А. С. ВАНЧИКОВ*

*«ГИПРОТРАНССИГНАЛСВЯЗЬ» — филиал ОАО «Росжелдорпроект»*


Выявленная в результате моделирования вероятностно-временная взаимосвязь показателей диагностирования, частных показателей эффективности приведения в готовность элементов сети тактовой сетевой синхронизации (ТСС), их целевого применения и восстановления позволяет решить задачу формирования требований к количественной и качественной составляющим метрологического ресурса, для чего следует определить влияние количественных и качественных характеристик метрологического ресурса элементов на показатели восстанавливаемости сети ТСС с учетом обеспечения требований к значению показателя надежности, задаваемому нормативными документами.

Это связанно с тем, что при введении в объект диагностирования дополнительных элементов, сознательно идут на некоторое приемлемое снижение безотказности объекта в целом для обеспечения выполнения требований к их ремонтопригодности.

Приемлемое снижение безотказности объекта достигается незначительным увеличением общего количества элементов за счет введения в состав элементов сети ТСС встроенных средств диагностирования, обеспечивающих повышение достоверности определения их состояния. В соответствии с четырьмя уровнями иерархии в сети ТСС присутствуют различные источники сигналов синхронизации