ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ В РАСПРЕДЕЛЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМАХ В ПРОДОЛЖИТЕЛЬНОМ ПЕРИОДЕ ВРЕМЕНИ

ENSURING THE INTEGRITY OF INFORMATION IN DISTRIBUTED COMPUTING SYSTEMS IN A LONG PERIOD OF TIME

A. Mingzov

Summary. The article discusses issues of ensuring the integrity of information over a long period of time. This task was not raised earlier. However, experience shows that in the long periods of time in electronic archives there can be an uncontrolled change in information and even its disappearance. Attacks on the integrity of electronic archives can be targeted. This requires the creation of information technology to ensure the integrity of archives. The work is devoted to the mechanism of the integrity of information in the electronic archive by creating a distributed managed trusted environment. This allows you to track the processes, data, user actions and make decisions about the choice of the owners of the archive, restore the archive with a partial loss of information in it and meet attacks on the integrity of the archive.

Keywords: information integrity, electronic archive, long period of time, attack.

Минзов Анатолий Степанович
Д.т.н., профессор, Государственный университет «Дубна», Дубна, Российская Федерация
983083@rambler.ru

Аннотация. В статье рассматриваются вопросы обеспечения целостности информации в длительных периодах времени. Такая задача ранее не ставилась. Однако опыт показывает, что в длительных периодах времени в электронных архивах может происходить не контролируемое изменение информации и даже её исчезновение. Атаки на целостность электронных архивов могут носить целенаправленный характер. Это вызывает необходимость создания информационных технологий по обеспечению целостности архивов. В работе рассматривается механизм работы системы обеспечения целостности информации в электронном архиве путем создания распределенной управляемой доверенной среды. Это позволяет контролировать процессы, данные, действия пользователей и принимать решения по выбору владельцев архива, восстанавливать архив при частичной потере информации в нем и противодействовать атакам на целостность архива.

Ключевые слова: целостность информации, электронный архив, длительный период времени, атака.

Введение

Прогрессирующее развитие информационных технологий с новыми возможностями создания виртуальных сред и распределенных вычислительных систем заставляет нас несколько по-другому взглянуть на проблемы обеспечения безопасности информации в этих системах. Появилась тенденция встраивания систем защиты информации в распределенные вычислительные системы, что нашло отражение и в нормативных документах [1–6]. Стало более заметным и отсутствие в этих условиях новых подходов к обеспечению механизмов конфиденциальности, целостности и доступности информации. Сегодня все решения по проектировании систем информационной безопасности имеют ограниченные жизненные циклы управления, а нормативные документы включают в себя рекомендации по выводу элементов систем защиты информации из эксплуатации. Реально длительность жизненного цикла систем безопасности существенно зависит от морального старения элементов этих систем и составляет сегодня менее 10 лет.

Есть и еще одна тенденция, которая вплотную приближается к рассматриваемой проблеме. Это необходимость хранения личной цифровой информации в длительном периоде времени, значительно превышающем время жизни человека. До сих пор считается, что самой надежной формой хранения информации является бумага. Известно выражение, что «рукописи не горят», однако, это далеко не так. Интенсивная урбанизация населения, повышение плотности застройки городов создают проблемы для хранения информации на бумажных и других носителях от пожаров и других угроз. С другой стороны, интенсивный переход к цифровым технологиям привёл нас к тому, что время жизни носителей информации в электронном виде не существенно отличается от времени жизни бумажных документов. Отсюда возникает главное противоречие: с одной стороны, идет резкая интенсификация технологий обработки и обмена информацией, а с другой стороны мы совершенно не заботимся о том, как, где, сколько времени и в каких формах хранится эта информация. Есть ещё одна тенденция, связанная с нарастанием значительных объемов данных, которые требуются нам для запоминания. Причём

эта информация имеет, как правило, смысл, но лишена некоей логической последовательности. К ней относятся: логины и пароли от различных информационных систем, социальных сетей, почтовых служб; пароли от электронных кошельков денежных информационных систем и дистанционного банковского обслуживания; пароли доверенной загрузки и систем электронной подписи; пин-коды платежных банковских карт; информация, относящаяся к личной и семейной тайнам и другая. Часть этой информации передается другим лицам с разным уровнем доступа, а личная информация может передаваться по наследству. Таким образом, сегодня возникает противоречие между увеличивающимися возможностями информационных систем, средств связи и телекоммуникаций и устаревшими подходами к обеспечению целостности информации в этих системах в длительных периодах времени.

1. Целостность информации и механизмы её обеспечения и контроля

Термин «целостность» используется в различных областях знаний: информационная безопасность, компьютерная безопасность, защита компьютерных сетей и информационных систем. Но практически везде он имеет одинаковый смысл:

1. ***Целостность информации (ресурсов автоматизированной информационной системы)*** — состояние информации (ресурсов автоматизированной информационной системы), при котором ее (их) изменение осуществляется только преднамеренно субъектами, имеющими на него право [4].
2. ***Целостность информации*** — состояние информации, при котором отсутствует любое ее изменение, либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.
3. ***Целостность ресурсов информационной системы*** — состояние ресурсов информационной системы, при котором их изменение осуществляется только преднамеренно субъектами, имеющими на него право, при этом сохраняются их состав, содержание и организация взаимодействия.
4. ***Целостность информации*** — это состояние информации, при котором отсутствует любое её изменение субъектами, не имеющими на это права. Основные процессы, которые должны обеспечиваться в механизмах целостности: хранение, *передача и отображение* информации.

Таким образом, в широком смысле этого слова термин целостность имеет отношения не только непосредственно к самой информации, но также и к тем субъектам, которые имеют отношение к хранению, передаче и отображению информации.

Все угрозы нарушения целостности информации относятся к любым формам несанкционированного воздействия на информацию, приводящие к её изменению, нарушению логической последовательности или исчезновению. В ответственных информационных системах, например критических информационных инфраструктурах, механизм целостности может быть более сложным и включать защиту информации от субъектов, имеющих права на её изменение, но действия которых могут привести к её разрушению или уничтожению[1].

Основными механизмами обеспечения целостности информации (данных) в информационных системах являются:

1. Обеспечение отказоустойчивости (***надежности***) хранения информации. Это достигается многократным дублированием информации на различных носителях и в виртуальных средах. Показатели надежности могут быть рассчитаны при известных вероятностях безотказной работы отдельного устройства или облачного сервиса.
2. Обеспечение безопасного ***восстановления*** информации при её хранении. Такая задача возникает в том случае, когда информация представляет собой архивы документов, копии которых отличаются по контролю целостности.
3. Обеспечение требований по целостности информации ***при передаче её по линиям связи*** путем помехоустойчивого кодирования, хэширования, шифрования, использования имитовставки и применения электронной подписи документов.
4. Выполнение требований по ***доступности и целостности*** информации путем выполнения требований по резервированию каналов связи, оборудования и проведения других мероприятий по обеспечению непрерывности бизнеса [2].
5. Выполнение требований по ***конфиденциальности*** к информации, содержащейся информационных системах, и к информационным технологиям обеспечения целостности информации и её контроля.

Практическая реализация контроля целостности обеспечивается в механизме инкапсуляции при проектировании классов в объектно-ориентированном программировании. При этом необходимо ориентироваться на требования стандарта [4–6] (*Common Criteria*),

[1] В настоящее время этот вопрос вообще не рассматривается в нормативной документации. Однако при обеспечении целостности на длительный период времени он должен быть обязательно решен (***авт.***).

который описывает инфраструктуру требований по свойствам безопасности отдельных её компонентов. Для этого в этом стандарте предусматриваются функции безопасности в форме семейства ***FDP_UIT***, которые определяют требования по обеспечению целостности данных пользователя при их передаче между объектом и другим доверенным продуктом информационной технологии, а также возможность их восстановления при обнаружении ошибок.

К сожалению, вопросы обеспечения целостности информации при её отображении в настоящее время не рассматриваются. Однако в будущих информационных системах и особенно в критических информационных инфраструктурах это требование может появиться.

Есть ещё один важный аспект этой проблемы. В длительных периодах времени будет происходить не только контролируемое изменение информации в архивах документов, но и смена владельцев этих архивов. Для этого необходима разработка механизмов безопасной реализации этих процессов. Существуют и технические аспекты этой проблемы, связанные с управлением архивом, его расширением и переходом на новые форматы и технологические платформы.

Остается актуальной и другая задача — создание доверенной среды всех субъектов, имеющих отношение к архиву.

Таким образом, механизмов обеспечения целостности информации на длительный период времени сегодня не существует, а процессы управления архивами с позиций обеспечения их целостности не рассматривались.

2. Постановка задачи обеспечения целостности информации в длительных периодах времени

Наименование проекта:

Система обеспечения целостности архива в продолжительных интервалах времени (СОЦ)

Цель проекта:

Разработка механизма управления архивом информации с передачей прав его наследования очередному владельцу при заданном уровне надежности хранения криптографически защищенной информации.

Ограничения и допущения:

1. Общая сеть (Интернет) будет модернизироваться эволюционно с сохранением преемственности протоколов передачи информации.
2. Операционные системы также остаются консервативными в отношении поддержки команд исполняемых файлов. Направление их развития идет в сторону повышения надежности, производительности, безопасности и расширения интерфейсов взаимодействия с оборудованием и приложениями.
3. Форматы хранения информации консервативны и будут изменяться в сторону обеспечения их безопасности и надежности при условии совмещения их разных версий.
4. Виртуальные среды будут все более доступны для архивов и процессов.
5. Права владельца архива и других его пользователей контролируются системой (*System Management Console*), размещенной в виртуальной среде на одной из платформ *PaaS* (*Platform-as-a-Service*). Любые их действия, направленные на расширение своих прав, приводят к блокированию у них консоли управления (*Archive User Console*).
6. Все действия с архивом протоколируются и могут быть восстановлены пользователями, имеющими на это права. Изменения истории архива недопустимы, даже владельцем документа. Все изменения проводятся только относящиеся к текущему времени.
7. Смена владельца архива проводится по процедуре, организованной *System Management Console* на основании списка очередных владельцев архива. Условием запуска этой процедуры может быть потеря активности владельца архива в течении определенного промежутка времени, либо желание его владельца через его консоль (*Archive Owner Console)*.
8. Решение на включение нового пользователя архива и его права принимает владелец архива. Решения по доступу пользователей к общей публичной информации принимает *System Management Console* по заданным критериям.
9. Аутентификация пользователей архива и процессов осуществляется на основе архитектуры открытых ключей. Эта процедура запускается при входе в архив.
10. Ограничения на время работы СОЦ нет. Переход на другие технологические платформы осуществляется без изменения программной среды приложений и проводятся под управлением владельца архива по процедуре, исключающей возможность его модификации, также полного или частичного исчезновения (нарушения целостности).
11. Все элементы системы (процессы и данные) многократно дублируются, синхронизируются при изменениях и контролируются на целостность.
12. Восстановление архива проводится по процедуре установления консенсуса для его отдельных элементов.

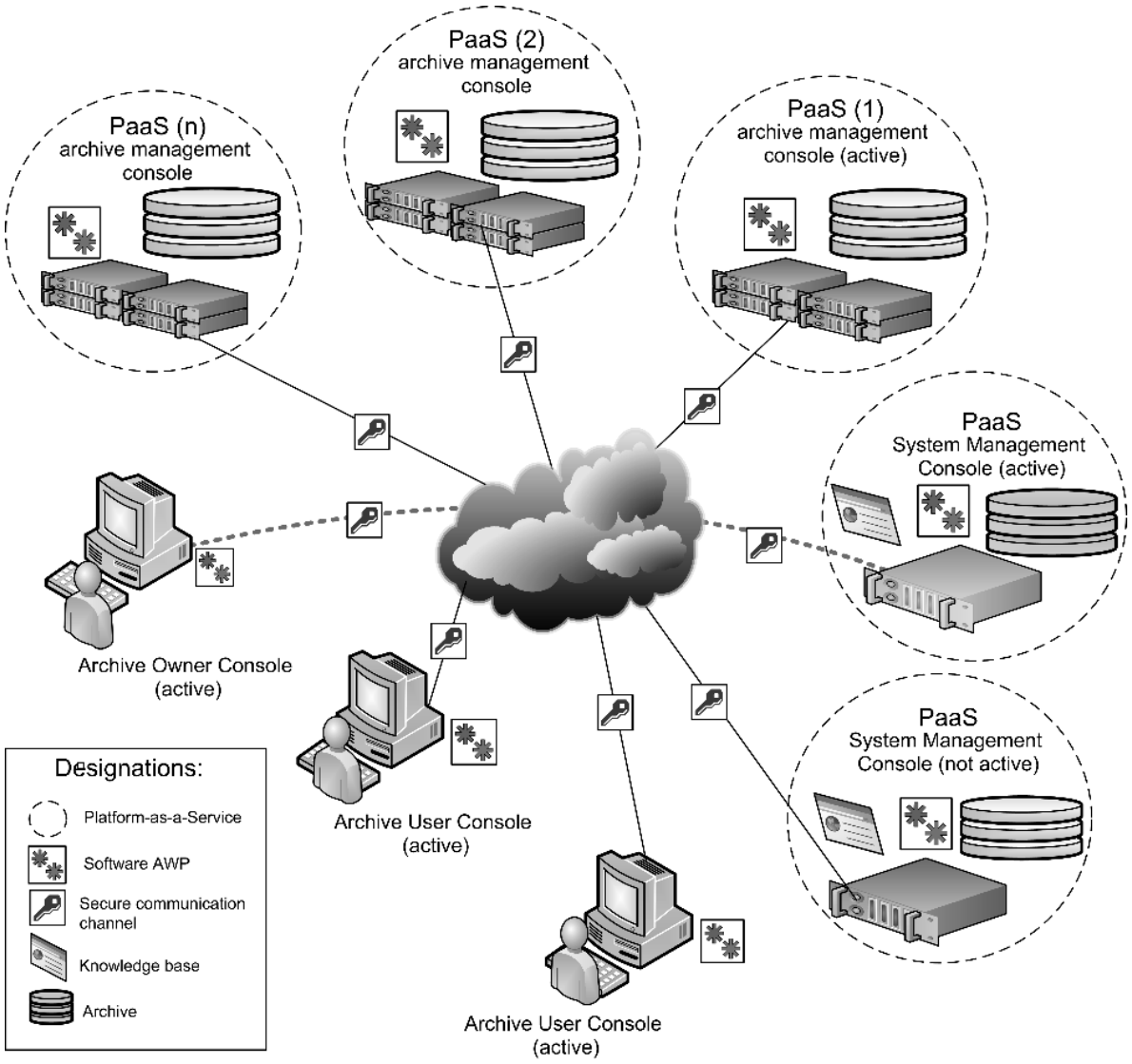

Рис. 1. Структура системы обеспечения целостности архивов

Сфера применения

Физические или юридические лица, желающие гарантировано передать информацию архива очередному его владельцу (наследнику) в неограниченном периоде времени.

3.Структура системы обеспечения целостности информации и её основные функции

Структура системы представлена на рис. 1. Вся организация работы архива в длительном периоде времени осуществляется в четырех взаимосвязанных структурах (рис. 1):

1. Управления архивом (*AMC — Archive Management Console*).
2. Управления системой (*SMC — System Management Console).*
3. Система управления владельца архива *(AOC — Archive Owner Console).*
4. Система доступа пользователя архива *(AUC — Archive User Console).*

Управление архивом осуществляется автономно на одной из активных платформ. Хранение архива осуществляется в несколько десятках копий в различных виртуальных средах на платформах PaaS. Передача управления на архив и синхронизация всех изменений с другими копиями архива осуществляется с SMC. Формат хранения архива настраивается при запуске системы и представляет собой логически связанную структуру документов, которые классифицируются при вводе в архив по определенным признакам. Определяющим фактором является дата документа, занесенного в архив, но реестр документов позволяет отображать содержание архива во всех возможных сочетаниях описания

признаков документов. Все документы архива зашифрованы и передаются пользователю архива после проверки возможности его доступа и полномочий.

Наиболее сложным элементом систем обеспечения целостности является SMC. Именно её функции определяют длительность обеспечения целостности архива и включают:

1. Принятие решения на передачу прав доступа к архиву очередному владельцу (при определенных условиях). Применение разных механизмов наследования архива.
2. Организация взаимодействия с пользователями активного архива и установление им прав доступа.
3. Контроль работы всех пользователей архива и подготовка отчетов.
4. Синхронизация изменений архива во всех его копиях и информации управления.
5. Контроль целостности процессов консолей управления AMC, SMC, AOC, AUC и данных.
6. Генерация ключей и их сертификатов. Содержание архива ключей.
7. Шифрование архива. Синхронизация службы времени консолей управления.
8. Перенос архива на новые платформы и среды.
9. Восстановление целостности архива по отдельным его элементам с использованием процедуры консенсуса.
10. Оценка рисков нарушения целостности архива со стороны пользователей и уведомление об этом владельца архива.
11. Перенос виртуальных копий на материальные носители.
12. Поиск новых виртуальных средств для хранения копий.
13. Выявление признаков атак на активный архив и смена активного архива.

Функции очередного владельца архива включают:

1. Установление на своём хосте консоли владельца архива и получение от SMC права на его управление.
2. Пополнение списка очередных владельцев архива определение способов связи SMC с ним.
3. Определение мест хранения архива в современных виртуальных средах.
4. Определение прав и условий доступа к архиву очередных участников и других пользователей.
5. Изменение содержания архива в пределах времени его владения и доступных ему документов.
6. Изменение доступных ему настроек управления архивом.
7. Определение форматов хранимой информации.
8. Запуск процессов переноса архива в другие виртуальные среды и устройства.
9. Принятие решения на передачу прав доступа к архиву очередному владельцу.

Заключение

Механизм работы СОЦ основан на создании распределенной управляемой доверенной среды, позволяющей контролировать процессы, данные, действия пользователей и принимать в отдельных случаях решения по выбору владельцев архива, управлять работой архива, восстанавливать архив при частичной потере информации в нем и противодействовать атакам на целостность архива.

ЛИТЕРАТУРА

1. ISO/IEC27001:2005 Information technology — Security techniques — Information security management systems — Requirements.
2. ISO/IEC27002:2013 Information technology — Security techniques — Code of practice for information security controls.
3. ISO/IEC27003:2017 Information technology — Security techniques — Information security management systems — Guidance.
4. ISO/IEC27005:2008 Information technology — Security techniques — Information security risk management.
5. ISO/IEC15408–1:2009 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model.
6. ISO/IEC CD15408–2 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components.
7. ISO/IEC CD15408–3 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components.

Журнал «Современная наука: актуальные проблемы теории и практики»