Модель целостности информации в длительном периоде времени ($t >> t_ж$)

Профессор кафедры БИТ НИУ «МЭИ»
д.т.н., проф. Минзов Анатолий Степанович
MinzovAS@mpei.ru

Содержание

1. Понятие «целостность информации» и механизмы её достижения в современных представлениях.
2. Постановка задачи обеспечения целостности в продолжительном периоде времени.
3. Некоторые выводы и оценки.

1.Понятие «целостность информации» и механизмы её достижения в современных представлениях

Механизмы обеспечения информационной безопасности

Понятие «целостность информации»

- **Целостность информации** –это состояние информации, при котором отсутствует любое её изменение, а любое изменение осуществляется только преднамеренно субъектами, имеющими на это право (**ГОСТ Р 50922-2006)**.
- Основные процессы, которые должны обеспечиваться в механизмах целостности: передача, изменение, хранение и отображение информации.
- Контроль целостности цифровой информации обеспечивается, как правило, вычислительной процедурой с использованием Хэш-функции h(T)

если $h(T)=h(To)$, то $T = To$,

где T – исходная информация

To – переданная информация.

Почему сегодня возрастает интерес к обеспечению целостности информации ?

1. Необходимость хранения личной информации (пин-коды, пароли от различных информационных систем, электронных кошельков и т.д.) за последние 10 лет возросла в десятки раз.
2. Интенсивное развитие информационных технологий, к сожалению, резко увеличило «летучесть» данных.
3. Появление новых механизмов создания доверенной по конфиденциальности и целостности среды на основе технологий блокчейн.

Угрозы целостности информации

- Модификация.
- Имитация источника.
- Повторная передача информации.
- Отказ от сообщения.
- …

База данных угроз целостности информации содержит 124 угрозы (http:fstec.ru). Это ~60% от всех угроз.

Пример описания угроз целостности

УБИ.027: Угроза искажения вводимой и выводимой на периферийные устройства информации

- **Описание угрозы** Угроза заключается в возможности подмены или искажения информации, выводимой на принтер, дисплей оператора или на другие периферийные устройства.
- **Данная угроза обусловлена** слабостями мер антивирусной защиты и контроля достоверности входных и выходных данных.
- **Реализация данной угрозы возможна** при условии наличия в дискредитируемой информационной системе вредоносного программного или аппаратных закладок
- **Источники угрозы**

  Внутренний нарушитель с низким потенциалом

  Внешний нарушитель с высоким потенциалом

Модели целостности информации

Модель целостности Кларка-Вилсона

Обозначения

S *– множество субъектов;*

D *– множество данных в автоматизированной системе (множество объектов);*

CDI *(Constrained Data Items) – данные, целостность которых контролируется;*

UDI *(Unconstrained Data Items) – данные, целостность которых не контролируется;*

TP *(Transformation Procedure) – процедура преобразования;*

IVP *(Integrity Verification Procedure) – процедура проверки целостности CDI.*

Модель

1. ***D = CDI ∪ UDI , CDI ∩ UDI =∅***
2. Элементарные операций над объектами выполняются процедурами преобразования ***TP*** и контроля целостности ***Ivp***
3. Процедуры ***TP,*** прошедшие проверки целостности ***Ivp*** называются «*корректно сформированными транзакциями*».

Правила

1. Наличие процедур ***Ivp***; неизменяемость ***Cdi*** при преобразованиях; допустимости применения ***Tp*** к ***Cdi***;
2. Строгое определение отношений между ***S, D, Tp***. Эти отношения определяются политикой.
3. Учет всех применений ***Tp*** (ведение журнала регистрации без прав изменения записей) .
4. Наличие специальных процедур ***Tp*** для преобразования ***Udi*** в ***Cdi*** и распознавания субъектов пытающихся применить ***Tp***.

Достоинства и недостатки модели целостности Кларка-Вильсона

Достоинства:

- Основана на реальной модели целостности бумажного документооборота.
- Проблема целостности электронного документооборота решается только как бинарная задача.

Недостатки:

- Основана на реальной модели целостности бумажного документооборота.
- Отсутствие формализации.

Модель целостности Кена Биба

Мандатная модель целостности Биба определяется в виде правил для новых типов уровней безопасности **– *уровней целостности (достоверности)***:

1.*NRD: $\forall s \in S, o \in O$:*

разрешить (s, o, чтение) если и только если уровень(o) *преобладает* уровень(s)

2.*NWU: $\forall s \in S, o \in O$:*

разрешить (s, o, запись) если и только если уровень (s) преобладает уровень(o).

3.Модель понижения уровня целостности субъекта до уровня целостности объекта при чтении.

4.Модель понижения уровня целостности объекта до уровня субъекта при записи (не всегда возможна).

Современные проблемы целостности информации

1. Все решения по целостности сводятся только к правилам взаимоотношений субъектов, объектов и процедур преобразования информации в текущий момент времени. При этом история изменения документа развита слабо, не формализована и не используется при управлении целостностью электронных архивов.
2. Управление целостностью информации в длительных периодах времени должно быть построено на доказательной базе контроля целостности при каждом изменении информации в электронном документе. Сегодня этого практически нет.
3. Вопросы изменения целостности в длительном периоде времени при хранении, передаче, отображении информации, модернизации оборудования, форматов хранения информации и ПО не рассматриваются.
4. Механизмы оценки уровня целостности (достоверности) четко не определены и являются самостоятельной очень сложной задачей.
5. Процедуры восстановления целостности информации при частичной её потере в электронных архивах в моделях не рассматриваются.
6. Риски передачи электронных архивов новому поколению владельцев (администраторов) не обсуждаются, а механизмы сохранения целостности для этой ситуации не разработаны.
7. Возможность потери архивов в результате случайного или умышленного воздействия на него его владельца или пользователей с высокими правами не рассматриваются.

2. Постановка задачи обеспечения целостности информации в длительных периодах времени

Наименование проекта:

Система обеспечения целостности электронного 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.

Модель документа в архиве

1. Все документы архива состоят из начального документа (d_o) и отдельных блоков, состоящих из транзакций модификаций предыдущего состояния документа $d=\{d_o, d_1, d_2, \ldots, d_n\}$
2. Каждая транзакция связана с изменением документа и условиями его проведения: временем (t), содержанием изменений (Δd), субъектом проводившим изменения (s), уровнем безопасности транзакции (c), функцией контроля целостности транзакции $h(t)$.
3. Уровень безопасности документа определяется из условия:
   $max\ \{c_i\}.$
4. Доступ к документу субъекта (s) возможен только в том случае, если уровень безопасности (s) преобладает уровень документа (d).
5. Такая модель документа может восстановить его состояние на любой момент времени с использованием специальной процедуры $F(d,t)$ и доказать его целостность, при условии, что обратные действия по отношению к транзакциям будут запрещены.

Ограничения и допущения (1)

1. Общая сеть (Интернет) будет модернизироваться ***эволюционно*** с сохранением преемственности протоколов передачи информации.
2. Операционные системы также остаются консервативными в отношении поддержки сервисов выполнения команд. 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.

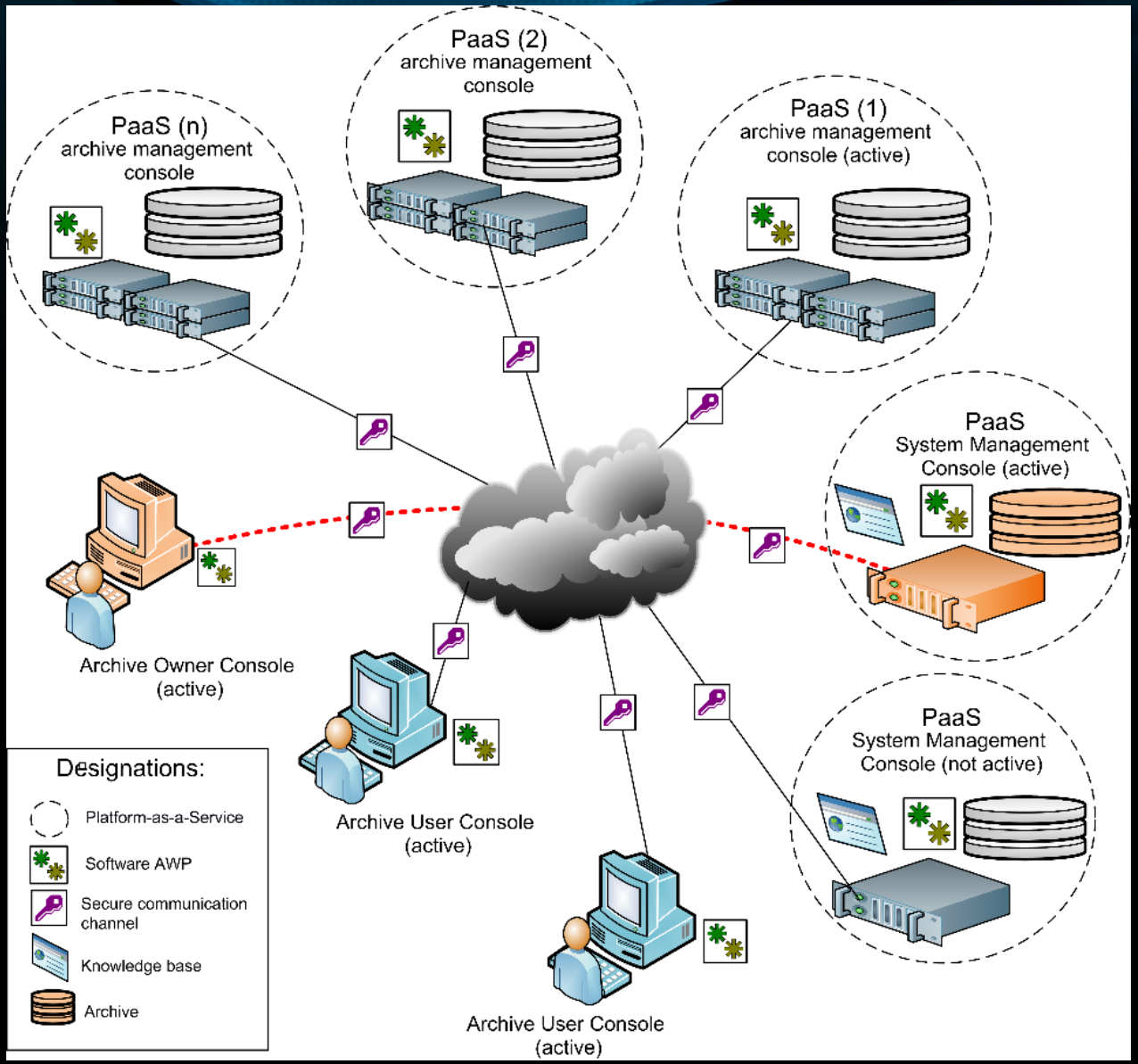
Ограничения и допущения (2)

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, реализованное 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 проводится под управлением владельца архива по ***процедуре, исключающей возможность его модификации, а также полного или частичного его разрушения или исчезновения.***
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.

Сфера применения

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

Структура системы



Функции Sistem Management Console (SMC)

1. Принятие решения на передачу прав доступа к архиву очередному его владельцу или администратору (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 (администратора) архива

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.

Расширенные функции СОЦ

1. Поиск наследников владельцев архива.
2. Оценка рисков целостности и доступности и уведомление владельца о расширении числа копий архива.
3. Перенос виртуальных копий на материальные носители.
4. Поиск новых виртуальных средств для хранения копий.
5. Нахождение компромиссов при нарушениях целостности отдельных копий архива.
6. Многопользовательская работа с архивом.
7. Применение разных механизмов наследования для владельцев архива.
8. Процедуры активного противодействия атакам на архив.
9. …

Заключение

Механизм работы Системы Обеспечения Целостности основан на создании распределенной управляемой доверенной среды, позволяющей контролировать процессы, данные, действия пользователей и принимать в отдельных случаях решения по выбору владельцев архива, поиску компромиссов при частичной потере информации в нем и выбору главной консоли управления СОЦ.

Проблемы целостности электронных архивов, которые требуют решений

1. Как восстанавливать целостность частично разрушенного архива, когда нет ни одной полностью не поврежденной его копии ?
2. Как разрешать конфликты в системе управления электронным архивом между его подсистемами ?
3. Содержание архива потребует определенных затрат на коммуникации, виртуальные среды, обновления ПО и т.д. Как обеспечить его финансирование или самофинансирование в длительном периоде ?
4. Какие функции и механизмы управления электронным архивом необходимо развивать дальше ?
5. В КФС защита информации строится на различных отношениях К,Ц,Д. Это экономически оправдано, но могут ли сегодня быть применимы существующие модели К,Ц,Д и в какой степени ?
6. Как будут использоваться в КФС другие модели защиты информации: неотказуемость, неизменяемость, подконтрольность, подотчетность ?

Минзов Анатолий Степанович, НИУ «МЭИ», Москва