# Лекция «Объектно-ориентированный подход в интеграции информационных систем» (часть 4)

Овчинников П.Е.
МГТУ «СТАНКИН»,
ст.преподаватель кафедры ИС

# Информационная безопасность

**ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология**

Информационная безопасность включает в себя три основных измерения:
- **конфиденциальность**,
- **доступность** и
- **целостность**.

С целью обеспечения длительного непрерывного успеха в бизнесе и уменьшения нежелательных воздействий информационная безопасность предусматривает применение соответствующих мер безопасности, которые включают в себя рассмотрение широкого диапазона угроз, а также управление этими мерами.

Информационная безопасность достигается посредством применения соответствующего набора средств управления, определенного с помощью **процесса управления рисками** и управляемого с использованием СМИБ, включая политику, процессы, процедуры, организационные структуры, программное и аппаратное обеспечение, чтобы защитить идентифицированные информационные активы.

*Стандарты в области ИБ*
*http://docs.cntd.ru/document/1200102762*

# Информационная безопасность

**ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология**

2.19 **информационная безопасность (information security):** сохранение конфиденциальности (2.9), целостности (2.25) и доступности (2.7) информации.
*Примечание - Также сюда могут быть включены другие свойства, такие как подлинность (2.6), подотчетность (2.2), неотказуемость (2.27) и достоверность (2.33).*

2.9 **конфиденциальность (confidentiality):** Свойство информации быть недоступной или закрытой для неавторизованных лиц, сущностей или процессов (2.31).
2.25 **целостность (integrity):** Свойство сохранения правильности и полноты активов (2.3).
2.7 **доступность (availability):** Свойство быть доступным и готовым к использованию по запросу авторизованного субъекта.
2.6 **подлинность (authenticity):** Свойство, гарантирующее, что субъект или ресурс идентичен заявленному.
2.2 **подотчетность (accountability):** Ответственность субъекта за его действия и решения.
2.27 **неотказуемость (non-repudiation):** Способность удостоверять имевшее место событие (2.15) или действие и их субъекты так, чтобы это событие (2.15) или действие и субъекты, имеющие к нему отношение, не могли быть поставлены под сомнение.
2.33 **достоверность (reliability):** Свойство соответствия предусмотренному поведению и результатам.

*Стандарты в области ИБ*
*http://docs.cntd.ru/document/1200102762*

# Кибербезопасность

**ГОСТ Р МЭК 62443-2-1-2015 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 2-1. Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики**

Организации, применяющие IACS (системы промышленной автоматики и контроля), начали применять готовые коммерческие технологии (COTS), разработанные для бизнес-систем, используемых в их повседневных процессах, в результате чего возрос риск кибератак, направленных на оборудование IACS. Как правило, такие системы в среде IACS по многим причинам не настолько робастны, как системы, специально спроектированные как IACS для подавления кибератак. Подобные недостатки могут привести к последствиям, которые отразятся на уровне охраны труда, промышленной безопасности и охраны окружающей среды (HSE).

3.1.13 **система управления кибербезопасностью** (cyber security management system): Программа, разработанная организацией для поддержания кибербезопасности всех имущественных объектов данной организации на заданном уровне конфиденциальности, целостности и доступности, независимо от того, относятся ли данные объекты к бизнес-процессам или системам IACS организации.



http://docs.cntd.ru/document/1200102762

# Аутентификация

**ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология**

2.5 **аутентификация (authentication):** Обеспечение гарантии того, что заявленные характеристики объекта правильны.

**Р 50.1.056-2005 Техническая защита информации. Основные термины и определения**

3.5.11 **аутентификация (подлинности субъекта доступа):** Действия по проверке подлинности субъекта доступа в информационной системе

**ГОСТ Р 52633.0-2006 Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации**

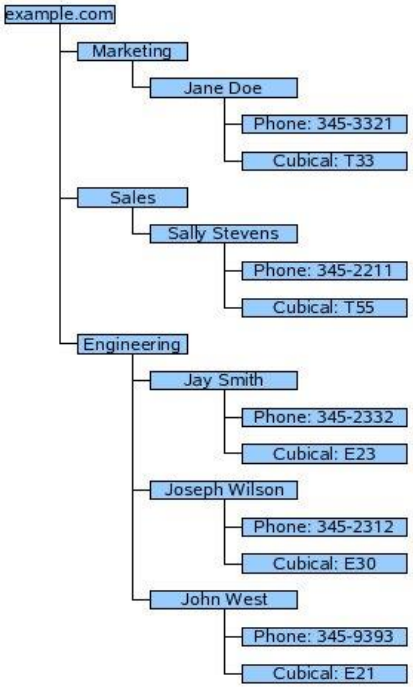
3.6 **биометрическая идентификация:** Преобразование совокупности примеров биометрических образов человека, позволяющее описать их стационарную и случайную составляющие, например, в виде математического ожидания и дисперсий контролируемых параметров или, например, в виде параметров обученной сети искусственных нейронов

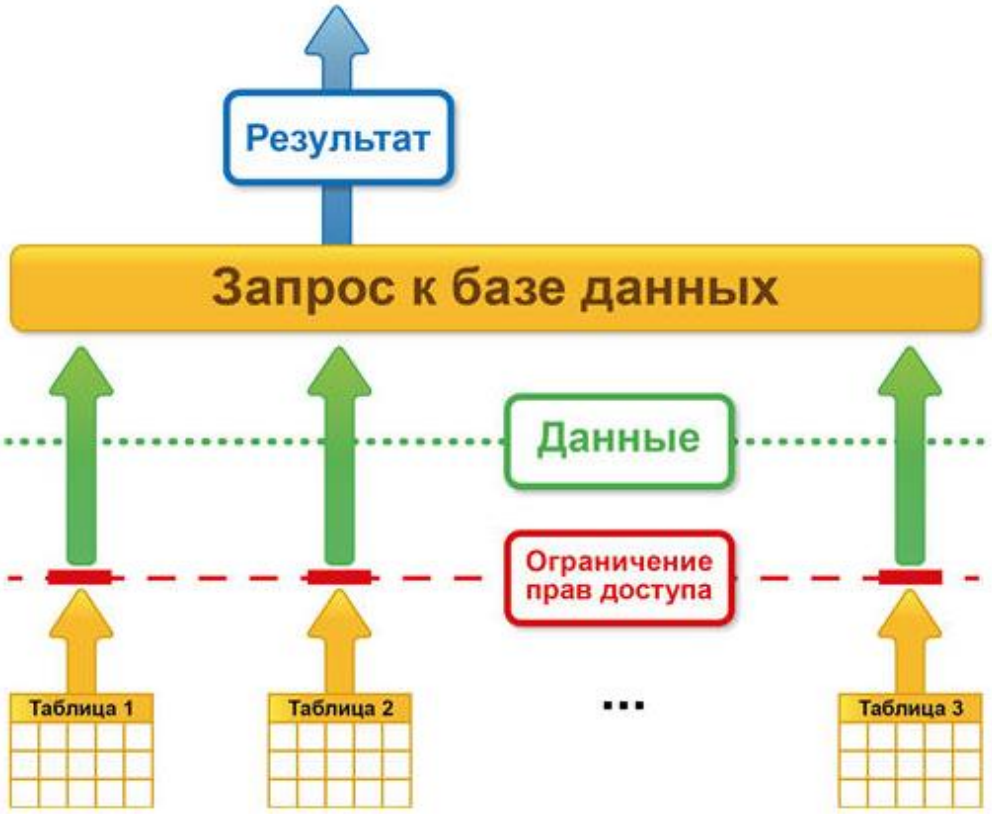
*http://docs.cntd.ru/document/1200102762*
*http://docs.cntd.ru/document/1200048922*
*Биометрическая аутентификация*

# Авторизация

**Р 50.1.056-2005 Техническая защита информации. Основные термины и определения**

3.5.10 **санкционирование доступа; *авторизация*:** Предоставление субъекту прав на доступ, а также предоставление доступа в соответствии с установленными правами на доступ




http://docs.cntd.ru/document/1200044768
http://v8.1c.ru/overview/Term_000000579.htm
https://ru.wikipedia.org/wiki/Active_Directory

# Угрозы

**ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология**

2.45 **угроза** (threat): Возможная причина нежелательного инцидента, который может нанести ущерб системе или организации.

2.4 **атака** (attack): Попытка уничтожения, раскрытия, изменения, блокирования, кражи, получения несанкционированного доступа к **активу** (2.3) или его несанкционированного использования.

**Cross-site scripting (XSS)** - название **атаки**.

В общем виде являются атакой на клиента, именно клиентские учетные данные атакующий может украсть.

- В некоторых случаях атака на систему, к примеру, если клиент администратор системы – атака на систему (деление атак условное и зависит от ситуации).

Соответствующий атаке **недостаток**: возможность внедрения **кода интерпретируемого на клиенте**.

**Cross-site request forgery (CSRF)** - название **атаки**.

http://docs.cntd.ru/document/1200102762

# Уязвимости

**ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология**

2.46 **уязвимость** (vulnerability): Слабое место **актива** (2.3) или **меры и средства контроля и управления** (2.10), которое может быть использовано **угрозой** (2.45).


http://docs.cntd.ru/document/1200102762

# Нарушители

**Модель нарушителя — (в информатике) абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа.**

Модель нарушителя определяет:
• **категории** (типы) нарушителей, которые могут воздействовать на объект
• **цели**, которые могут преследовать нарушители каждой категории, возможный количественный состав, используемые инструменты, принадлежности, оснащение, оружие и проч.
•типовые **сценарии** возможных действий нарушителей, описывающие последовательность (алгоритм) и способы действий групп и отдельных нарушителей

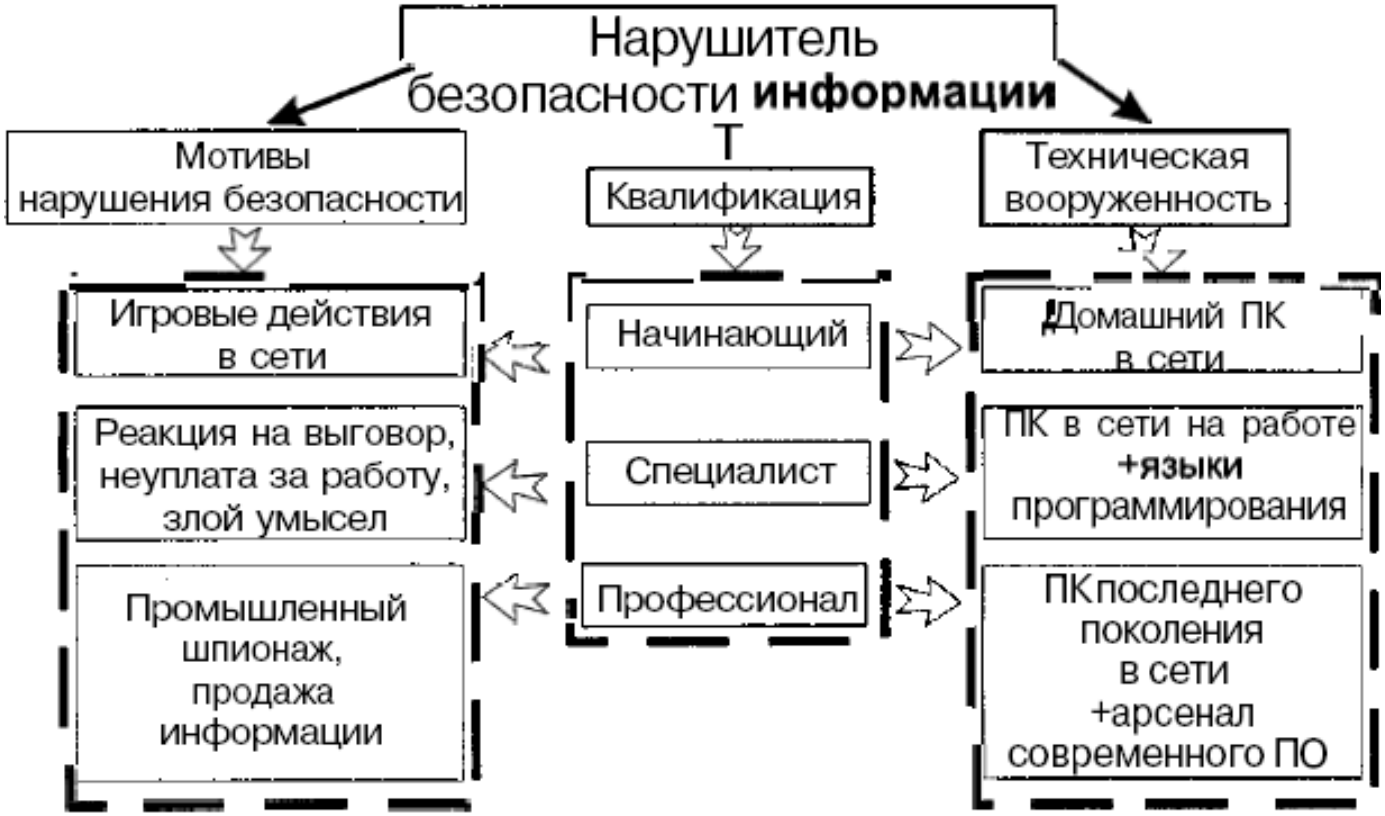
Модель нарушителей может иметь разную степень детализации.
• **Содержательная модель** нарушителей отражает систему принятых руководством объекта, ведомства взглядов на контингент потенциальных нарушителей, причины и мотивацию их действий, преследуемые цели и общий характер действий в процессе подготовки и совершения акций воздействия.
• **Сценарии воздействия** нарушителей определяют классифицированные типы совершаемых нарушителями акций с конкретизацией алгоритмов и этапов, а также способов действия на каждом этапе.
• **Математическая модель воздействия** нарушителей представляет собой формализованное описание сценариев в виде логико-алгоритмической последовательности действий нарушителей

# Нарушители

С точки зрения наличия права постоянного или разового доступа в контролируемую зону нарушители могут подразделяться на два типа:

• нарушители, не имеющие права доступа в контролируемую зону территории (помещения) — **внешние нарушители**

• нарушители, имеющие право доступа в контролируемую зону территории (помещения) — **внутренние нарушители**



# Защита

**ГОСТ Р 50922-2006 Защита информации. Основные термины и определения**

**защита информации; ЗИ:** Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию

• **правовая защита информации:** Защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением

• **техническая защита информации;** ТЗИ: Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств

• **криптографическая защита информации:** Защита информации с помощью ее криптографического преобразования

• **физическая защита информации:** Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты

http://docs.cntd.ru/document/1200058320

# Парирование

**ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения**

3.6.1 **обеспечение информационной безопасности** организации; обеспечение ИБ организации: Деятельность, направленная на **устранение (нейтрализацию, парирование)** внутренних и внешних угроз информационной безопасности организации или на минимизацию ущерба от возможной реализации таких угроз.

3.1.15 **критически важная система информационной инфраструктуры;** *ключевая система информационной инфраструктуры*; КСИИ: Информационно-управляющая или информационно-телекоммуникационная система, которая осуществляет управление или информационное обеспечение критическим объектом или процессом, или используется для официального информирования общества и граждан, нарушение или прерывание функционирования которой (в результате деструктивных информационных воздействий, а также сбоев или отказов) может привести к чрезвычайной ситуации со значительными негативными последствиями.

3.1.16 **критический объект:** Объект или процесс, нарушение непрерывности функционирования которого может нанести значительный ущерб.

http://docs.cntd.ru/document/1200075565
http://cyberrus.com/wp-content/uploads/2015/01/vkb_05_01.pdf

# Доверенная среда

**ГОСТ Р 54583-2011 Информационная технология. МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Основы доверия к безопасности информационных технологий. Часть 3 Анализ методов доверия**

2.4 **орган обеспечения доверия** (assurance authority): Лицо или организация, уполномоченные принимать решения (например, по выбору, спецификации, принятию, контролю за исполнением), связанные с обеспечением доверия к объекту, что однозначно приводит к формированию уверенности в безопасности объекта.

2.9 **среда** (environment): Условия, в которых выполняются процессы жизненного цикла (то есть люди, оборудование и другие ресурсы), и связанные с этими условиями характеристики доверия (например, репутация, сертификация).

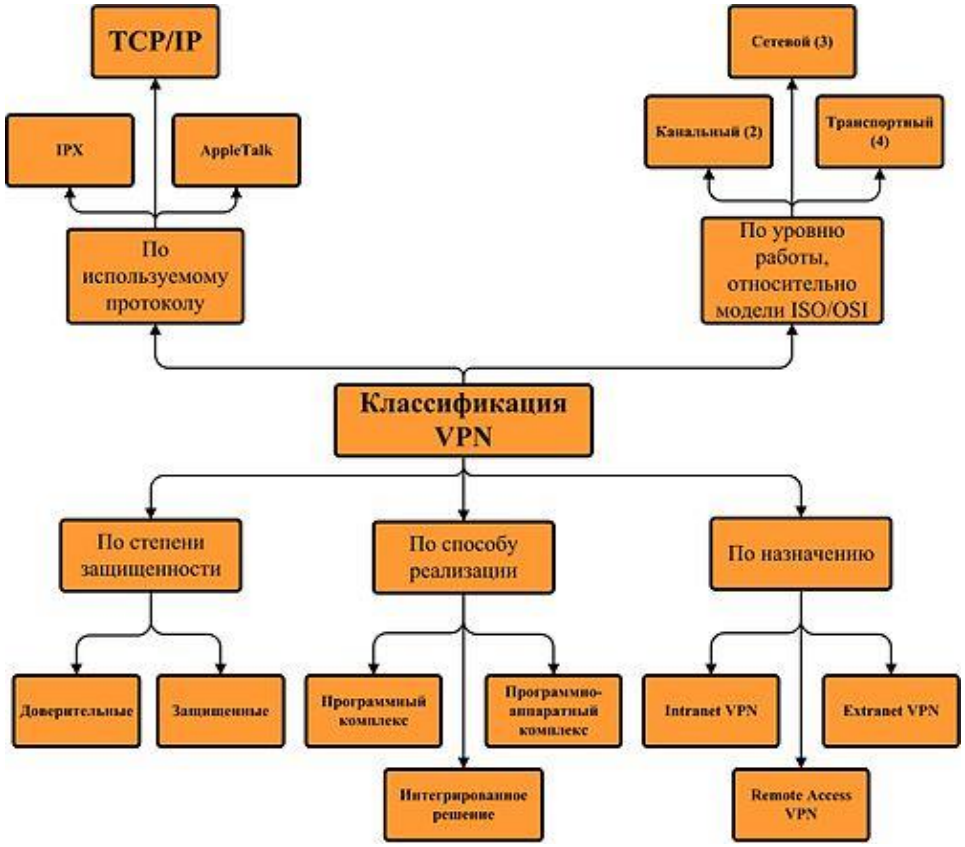
Примечание - В настоящем стандарте "доверие к среде" означает то же, что "доверие к продукту" и "доверие к процессу".

http://docs.cntd.ru/document/gost-r-54583-2011

# Шлюзы

**VPN (англ. *Virtual Private Network* — виртуальная частная сеть) — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет)**

Несмотря на то, что коммуникации осуществляются по сетям с меньшим или неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений, передаваемых по логической сети сообщений).
В зависимости от применяемых протоколов и назначения, VPN может обеспечивать соединения трёх видов: *узел-узел*, *узел-сеть* и *сеть-сеть*.

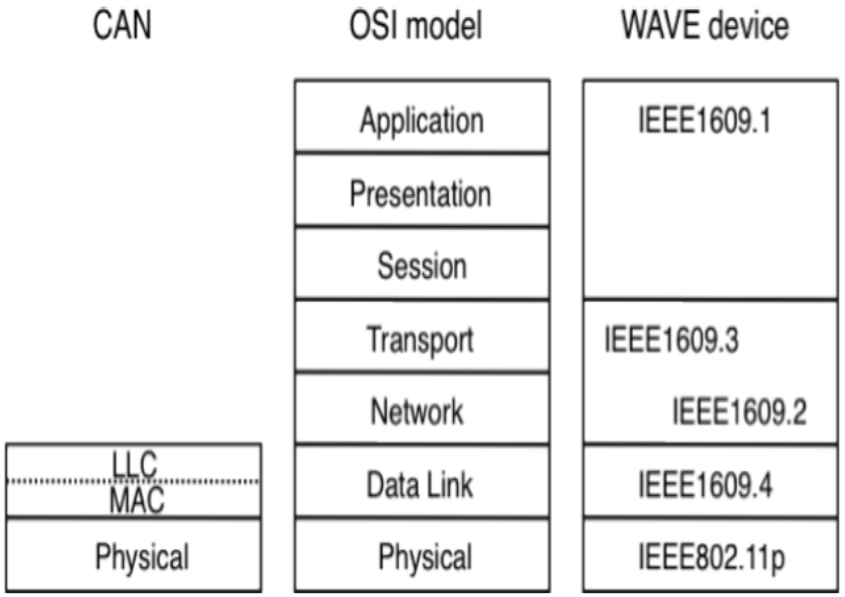



https://ru.wikipedia.org/wiki/VPN

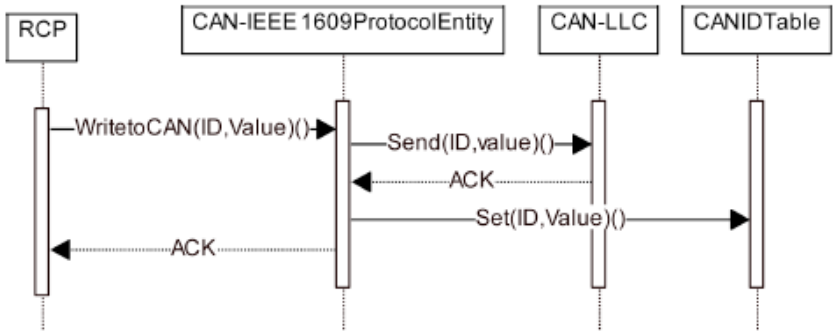
# Шлюзы

**Сетевой шлюз (англ. *gateway*) — аппаратный маршрутизатор или программное обеспечение для сопряжения *компьютерных сетей*, использующих разные *протоколы* (например, локальной и глобальной)**

В крупных сетях сервер, работающий как сетевой шлюз, обычно интегрирован с прокси-сервером и межсетевым экраном. Сетевой шлюз часто объединен с роутером, который управляет распределением и конвертацией пакетов в сети.




Internet of Things ecosystem today there are two dominant architectures for data exchange protocols: bus-based (DDS, REST, XMPP) and broker based (AMPQ, CoAP, MQTT, JMI). The protocols that support the information exchange between interoperability domains can also be classified to message-centric (AMQP, MQTT, JMS, REST) and data-centric (DDS, CoAP, XMPP).



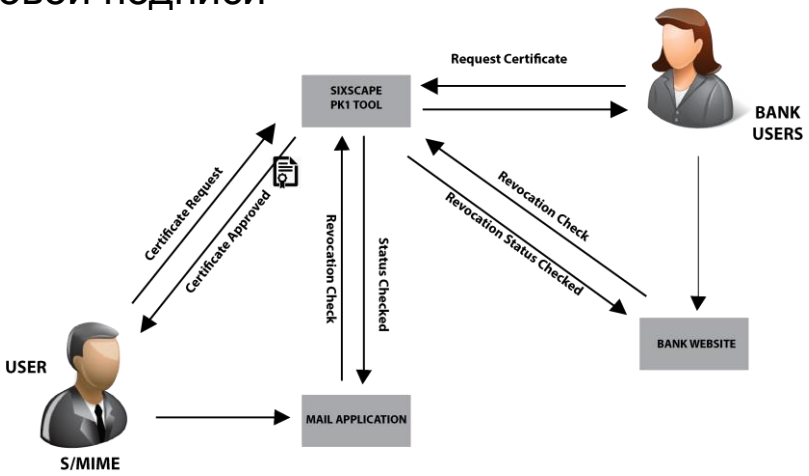

*Сетевой шлюз*

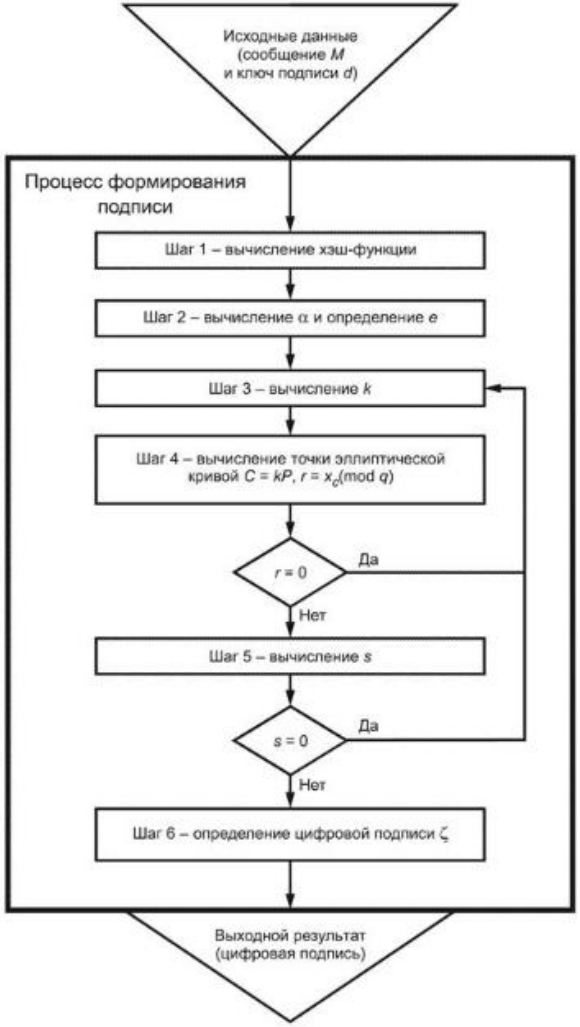
# Криптография

**ГОСТ Р 34.10-2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи**

**ключ подписи** (signature key): Элемент секретных данных, специфичный для субъекта и используемый только данным субъектом в процессе формирования цифровой подписи

**ключ проверки подписи** (verification key): Элемент данных, математически связанный с ключом подписи и используемый проверяющей стороной в процессе проверки цифровой подписи

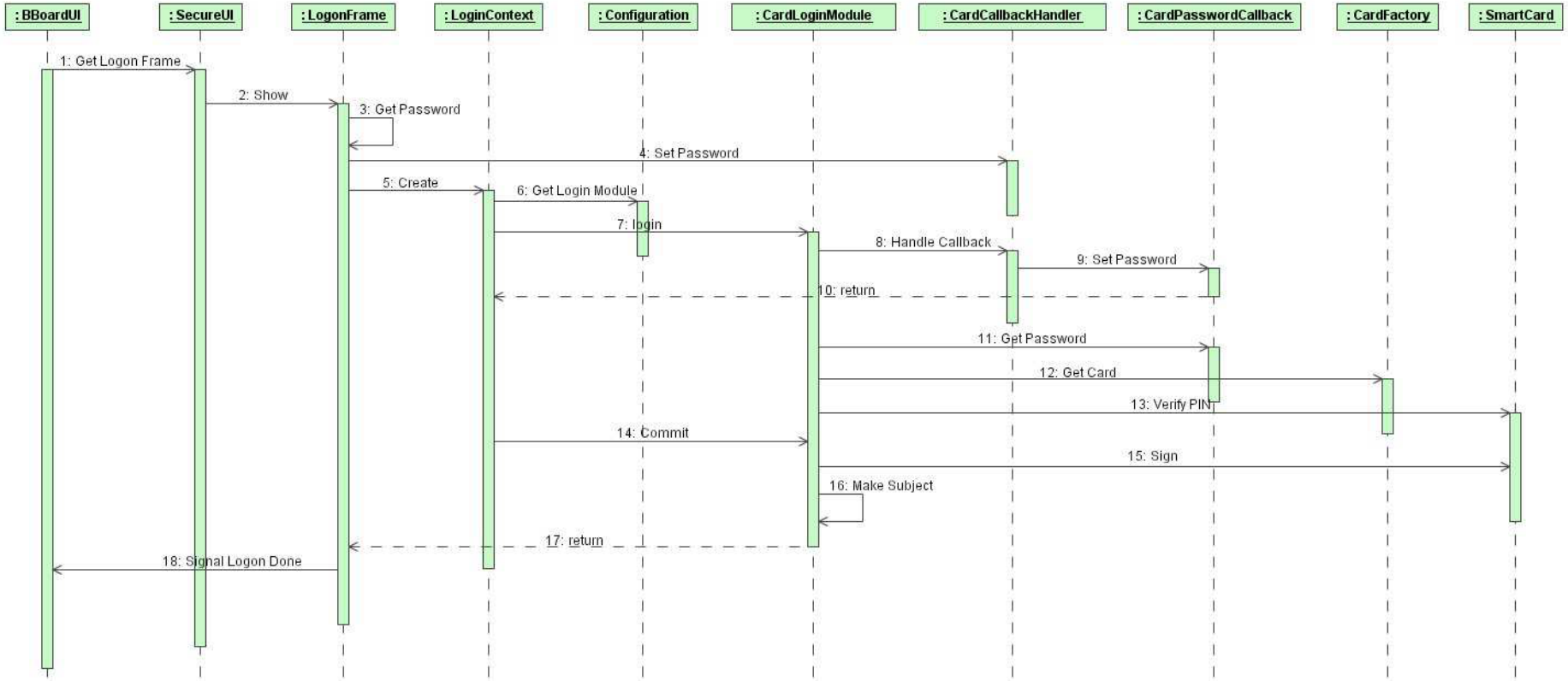



http://docs.cntd.ru/document/1200095034

PKI

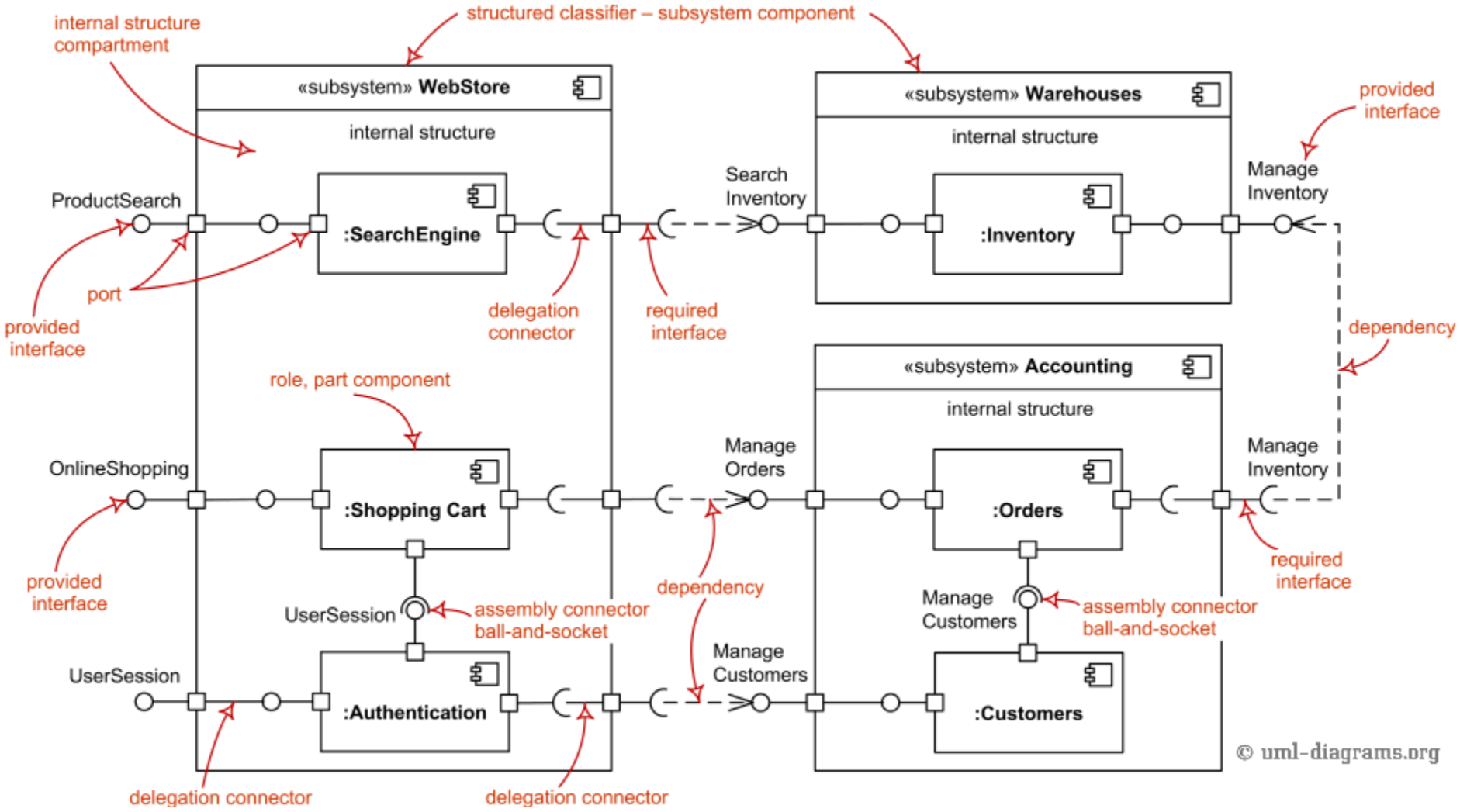
# Прогресс в UML






http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.136.3430&rep=rep1&type=pdf

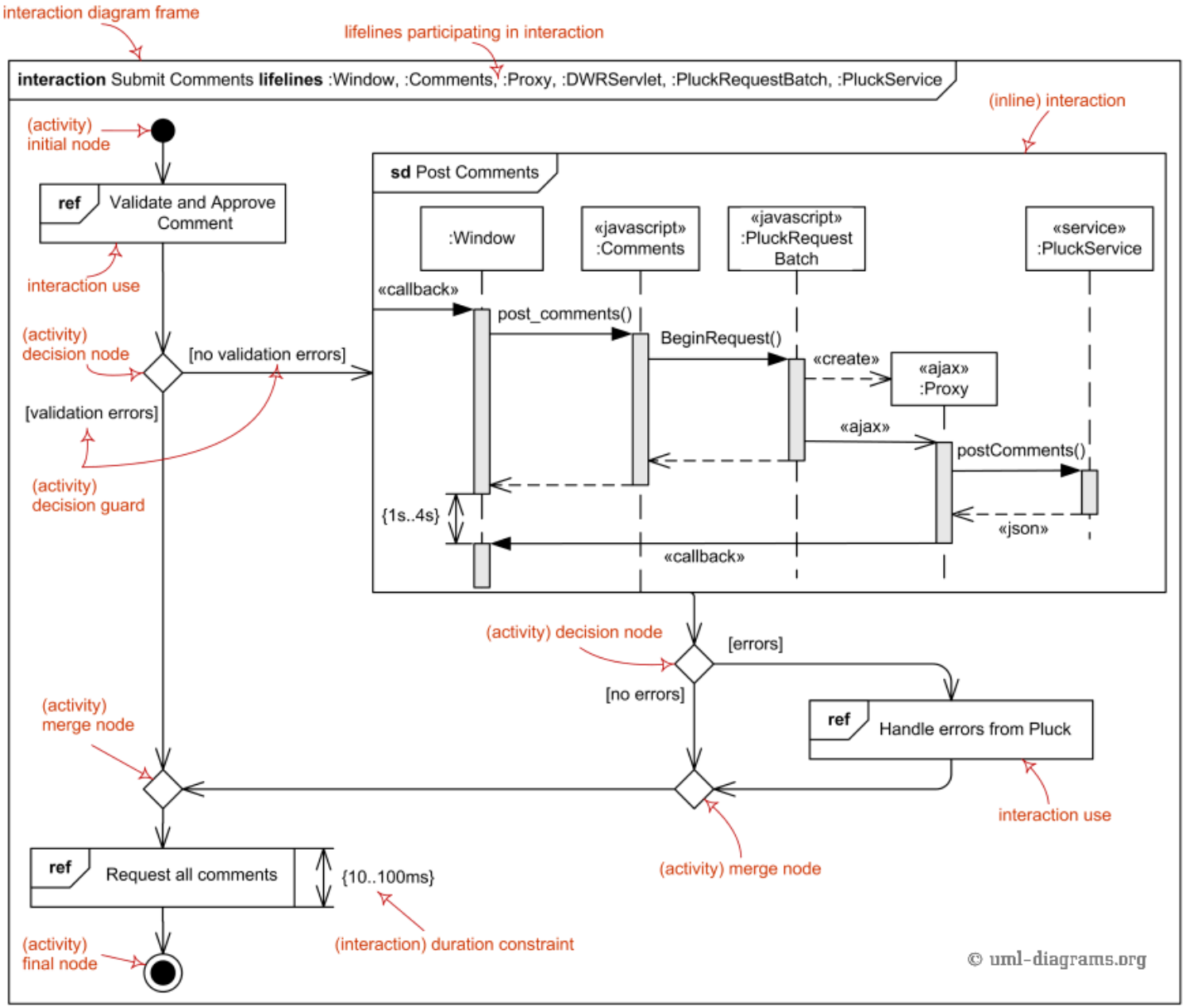
# Прогресс в UML






http://www.uml-diagrams.org/component-diagrams.html

# Прогресс в UML






http://www.uml-diagrams.org/interaction-overview-diagrams.html