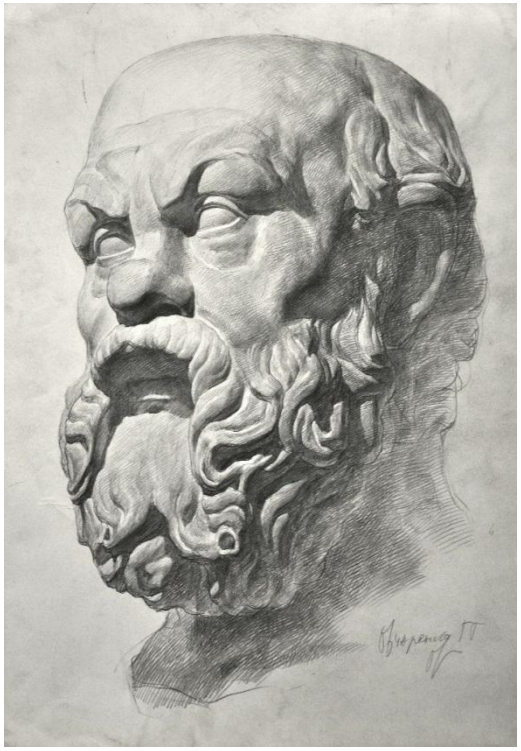
Комплексное противодействие атакам на информационные и материальные ресурсы бизнеса



Сократ, мудрец

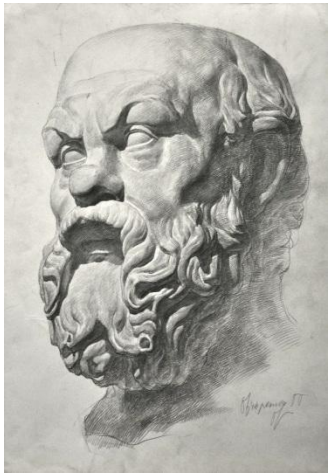
Тема № 7

Превентивная защита информации на АРМ, в сетях и БД, в системе ЭФ

Лекция, 2 часа

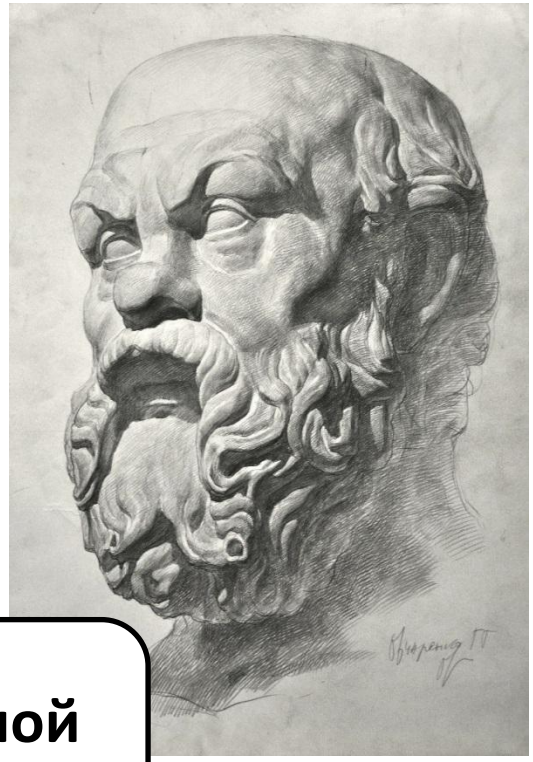
Информационная безопасность

Оглавление



1. Концепция обеспечения информационной безопасности бизнеса
2. Политики информационной безопасности
3. Модели безопасности
4. Выбор средств защиты системы информационной безопасности
5. Криптографическая защита информации
6. Антивирусные программы
7. Средства защиты АСУ ТП
8. Защита электронных финансов
9. Библиография

Концепция обеспечения информационной безопасности бизнеса



Сократ, мудрец

ДВЕ КРАЙНОСТИ ПРИ ПОСТРОЕНИИ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Бумажки для отмашки от проверяющих

Бездумно внедренные всевозможные средства защиты

МОДЕЛЬ ПОСТРОЕНИЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ISO/IEC 15408 **«Общие критерии безопасности информационных технологий»**

ISO 17799 **«Информационные технологии — Технологии безопасности — Практические правила менеджмента информационной безопасности»**

ISO/IEC 15408 **«Информационная технология - методы защиты - критерии оценки информационной безопасности»**

ISO/IEC 17799 **«Управление информационной безопасностью»**

РАССМАТРИВАЮТСЯ СЛЕДУЮЩИЕ ОБЪЕКТИВНЫЕ ФАКТОРЫ:

- ***угрозы информационной безопасности, характеризующиеся вероятностью возникновения и вероятностью реализации;***
- ***уязвимости системы информационной безопасности, влияющие на вероятность реализации угрозы;***
- ***риск - фактор, отражающий возможный ущерб организации в результате реализации угрозы информационной безопасности: утечки информации и ее неправомерного использования (риск в конечном итоге отражает вероятные финансовые потери - прямые или косвенные).***

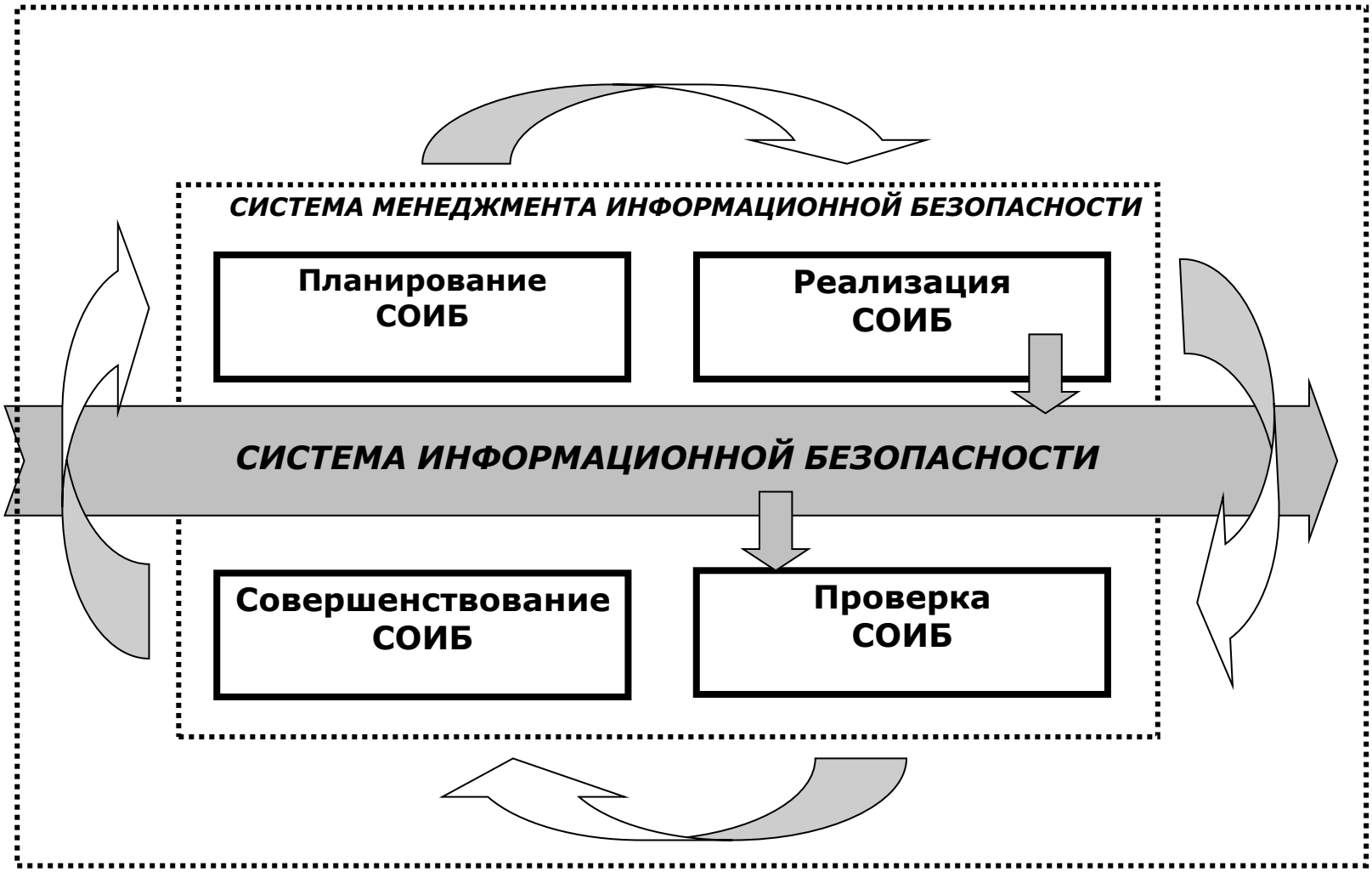
МОДЕЛЬ PDCA ДЛЯ УПРАВЛЕНИЯ ИБ

Принцип Деминга - Шухарта

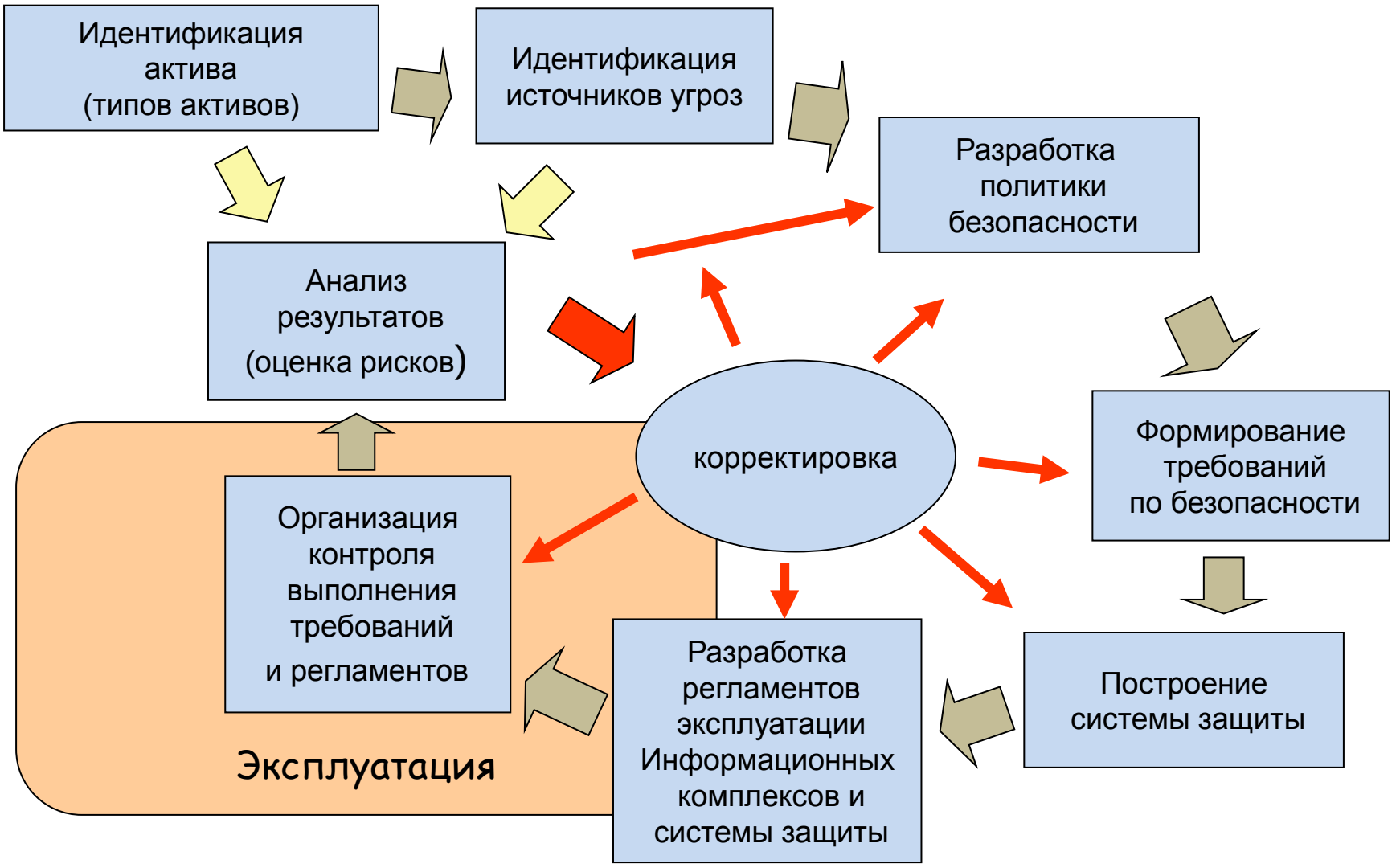
ПРОБЛЕМЫ С МОДЕЛЬЮ PDCA ДЛЯ УПРАВЛЕНИЯ ИБ

- **Нелинейность информационной безопасности**
- **Информационная безопасность в отличие от системы качества требует учета “интересов” злоумышленников, которые могут разбить все благие намерения по линейному циклу обеспечения управления ИБ**
- **Попытка все самое сложное вместить на первый шаг**
- **Планирование сильно зажимает вас в пространстве линейных и пошаговых моделей**
- **Нельзя постоянно совершенствоваться и менять ISO/IEC 27001 — международный стандарт по информационной безопасности**

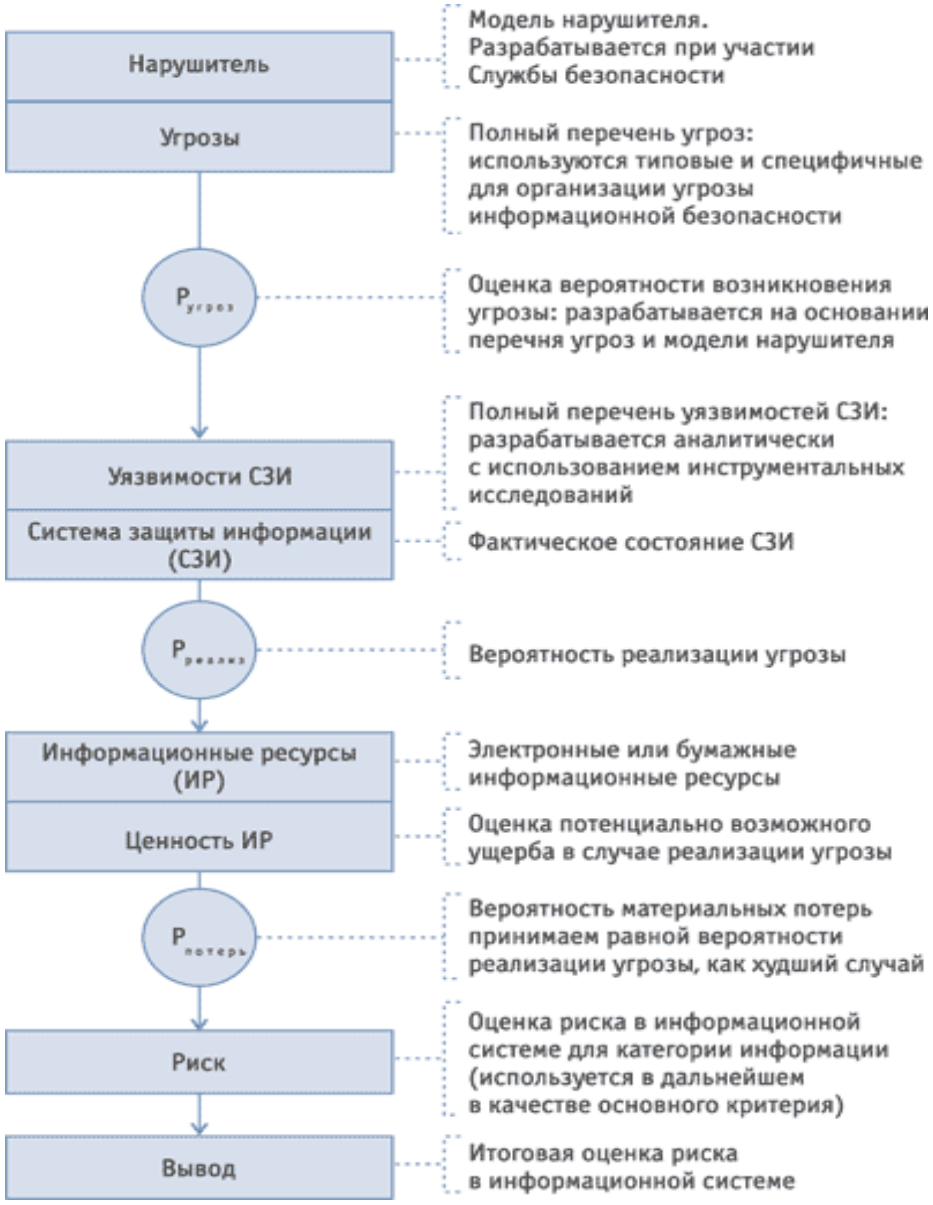
МОДЕЛЬ ПОСТРОЕНИЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С УЧЕТОМ МЕНЕДЖМЕНТА КАЧЕСТВА



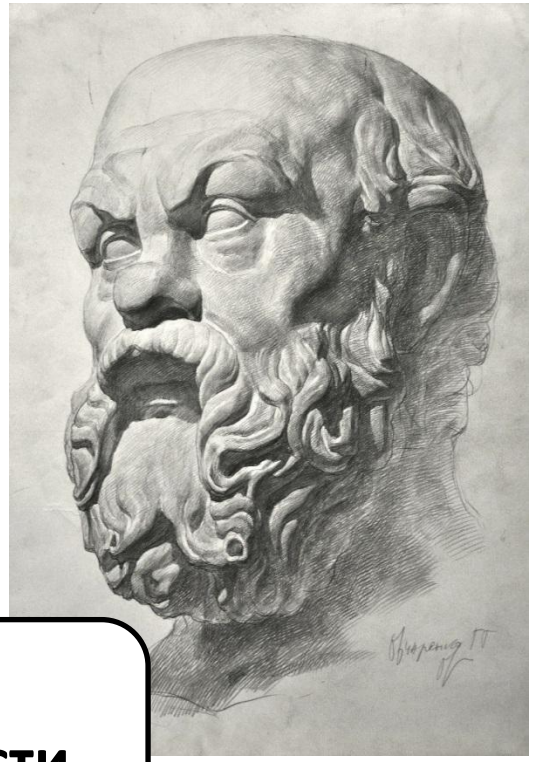
ОСНОВНЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



ВОЗМОЖНЫЙ АЛГОРИТМ ОЦЕНИВАНИЯ ИНФОРМАЦИОННЫХ РИСКОВ



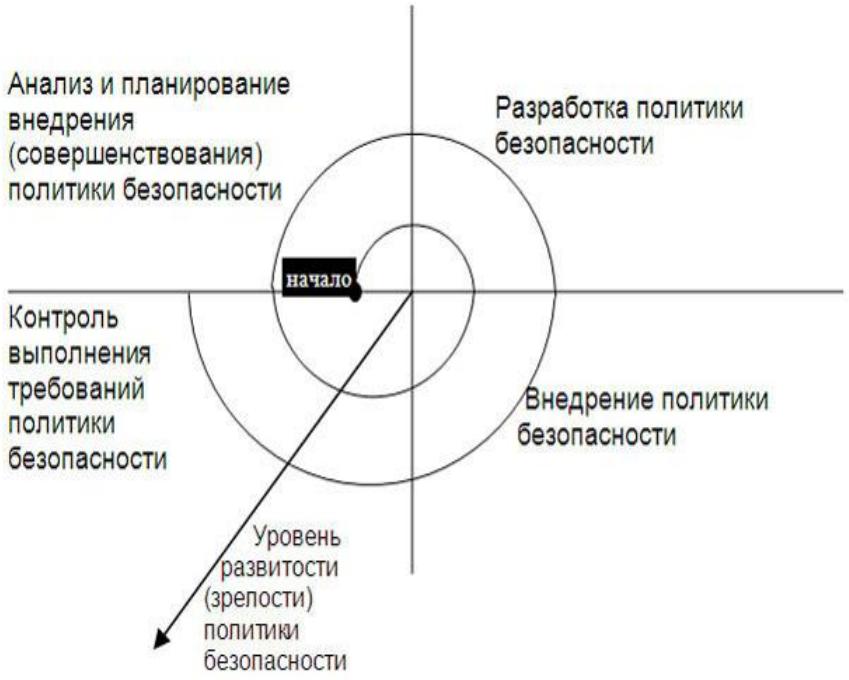
Политики информационной безопасности



Сократ, мудрец

ФОРМИРОВАНИЕ ПОЛИТИКИ БЕЗОПАСНОСТИ

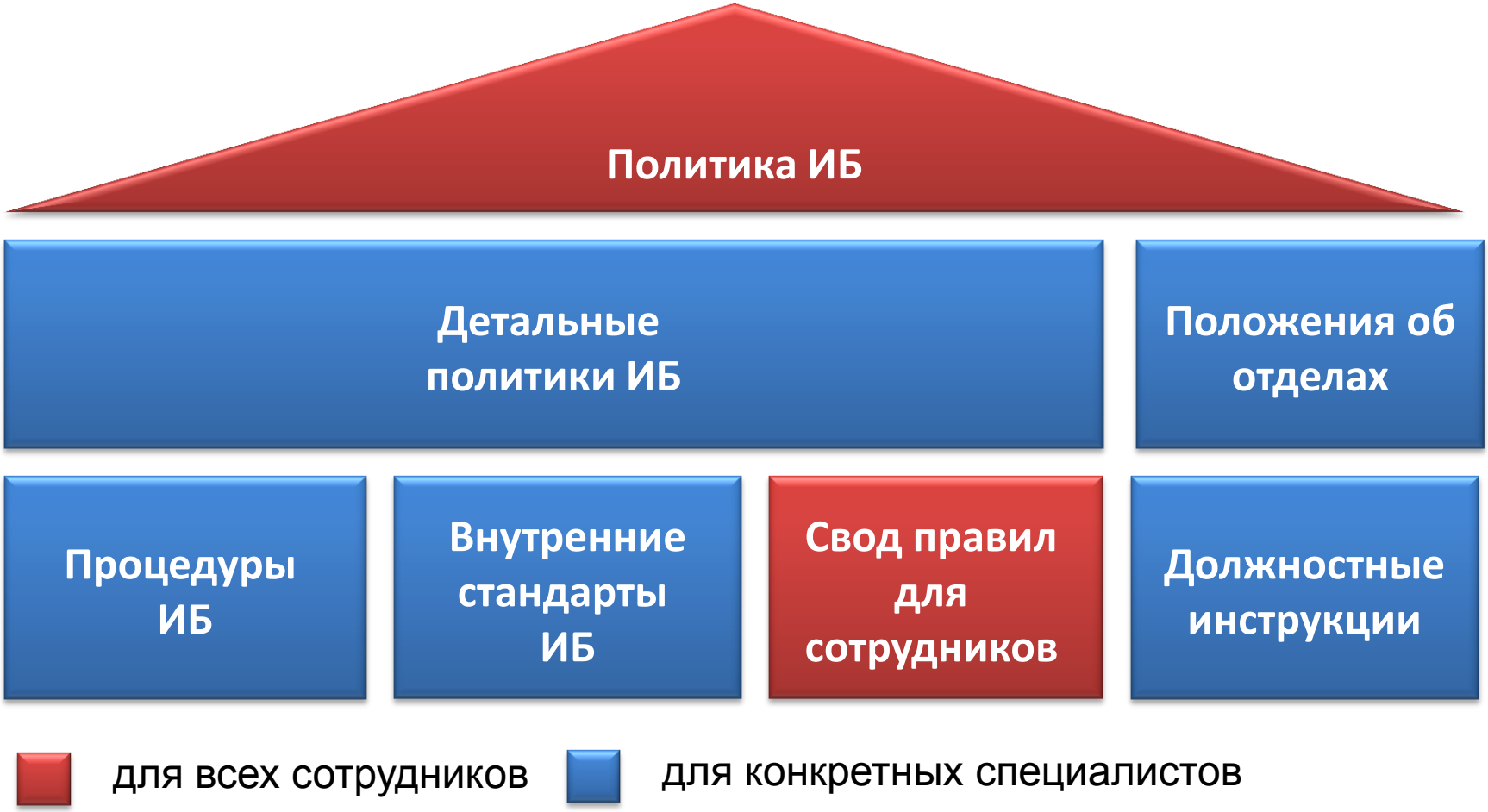
Политика информационной безопасности представляет собой комплекс документов, отражающих все основные требования к обеспечению защиты информации и направления работы предприятия в этой сфере.



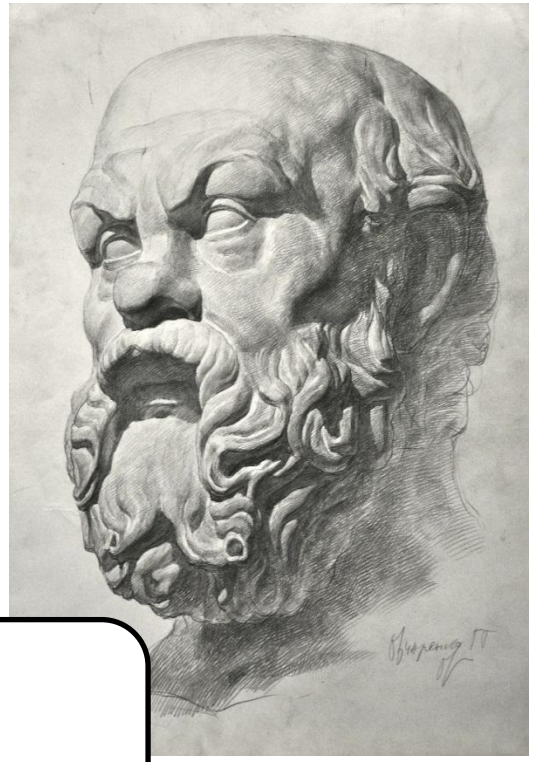
ОБЩИЙ ЖИЗНЕННЫЙ ЦИКЛ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- **Проведение предварительного исследования состояния информационной безопасности.**
- **Собственно разработку политики безопасности.**
- **Внедрение разработанных политик безопасности.**
- **Анализ соблюдения требований внедренной политики безопасности и формулирование требований по ее дальнейшему совершенствованию (возврат к первому этапу, на новый цикл совершенствования).**

СТРУКТУРА ПОЛИТИКИ ИНФОРАЦИОННОЙ БЕЗОПАСНОСТИ



Модели безопасности



Сократ, мудрец

МОДЕЛЬ БЕЗОПАСНОСТИ

МОДЕЛЬ БЕЗОПАСНОСТИ - **формальное (*математическое*, *алгоритмическое*, *схемотехническое* и т.п.) выражение политики безопасности**

МОДЕЛЬ БЕЗОПАСНОСТИ СЛУЖИТ ДЛЯ:

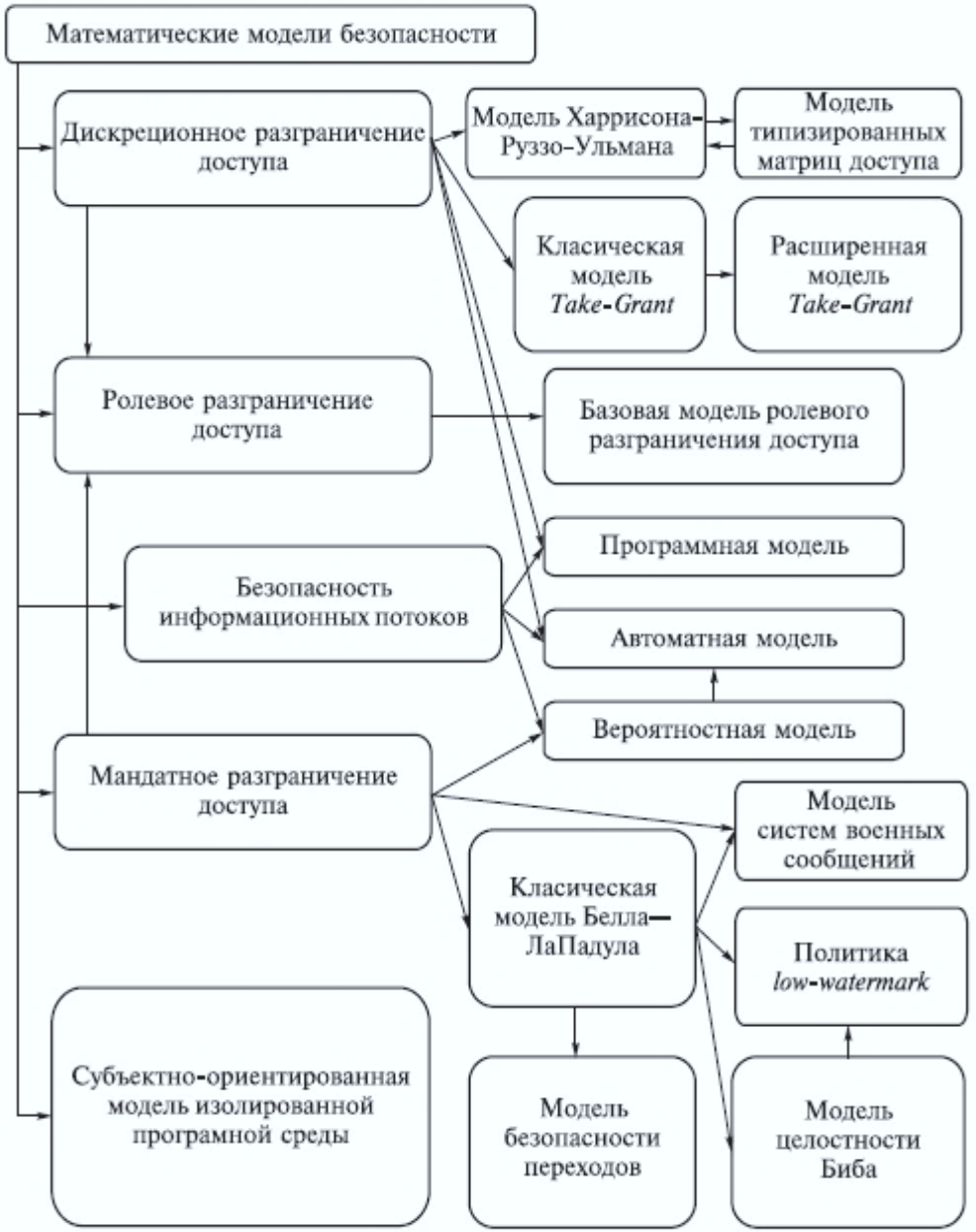
- **выбора и обоснования базовых принципов архитектуры, определяющих механизмы реализации средств защиты информации**
- **подтверждения свойств (защищенности) разрабатываемой системы путем формального доказательства соблюдения политики (требований, условий, критериев) безопасности**
- **оставления формальной спецификации политики безопасности разрабатываемой системы**

МОДЕЛИ ОРГАНИЗАЦИИ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ

ОСНОВНЫЕ ТРЕБОВАНИЯ К МОДЕЛЯМ ОБЕСПЕЧЕНИЯ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ

CIA (Confidentiality, Integrity, and Availability — конфиденциальность, целостность и доступность).
Эти три группы принципов являются общепризнанными при оценке рисков, связанных с важной информацией, и при утверждении политики безопасности.

Конфиденциальность — Важная информация должна быть доступна только ограниченному кругу лиц.
Целостность — Изменения информации, приводящие к её потере или искажению, должны быть запрещены.
Доступность — Информация должна быть доступна авторизованным пользователем, когда она им необходима.



МОДЕЛЬ ИЗБИРАТЕЛЬНОГО (ДИСКРЕЦИОННОГО) ДОСТУПА

- **права доступа предоставляются (*«прописываются» в специальных информационных объектах-стуктурах*), отдельно каждому пользователю к тем объектам, которые ему необходимы для работы в КС;**

- **при запросе субъекта на доступ к объекту диспетчер, обращаясь к ассоциированным с ним информационным объектам, в которых «прописана» политика разграничения доступа, определяет «легальность» запрашиваемого доступа и разрешает/отвергает доступ.**

ДОСТОИНСТВА ДИСКРЕЦИОННЫХ МОДЕЛЕЙ:

- ***Хорошая детализация защиты* (*позволяют управлять доступом с точностью до отдельной операции над отдельным объектом*)**
- ***Простота реализации***

НЕДОСТАТКИ ДИСКРЕЦИОННЫХ МОДЕЛЕЙ:

- ***Слабые защитные характеристики из-за невозможности для реальных систем выполнять все ограничения безопасности***
- ***Проблема "троянских коней"***
- ***Сложности в управлении доступом из-за большого количества назначений прав доступа***

МОДЕЛИ ПОЛНОМОЧНОГО (МАНДАТНОГО) ДОСТУПА

Основаны:

✓ на *субъектно-объектной* модели КС

✓ на *правилах организации секретного делопроизводства*, принятых в государственных учреждениях многих стран.

Информация (точнее документы, ее содержащие) категорируется специальными метками конфиденциальности – т.н. ***грифы секретности*** документов

Сотрудники по уровню благонадежности (доверия к ним) получают т.н. ***допуски*** определенной ***степени***

Сотрудники с допуском определенной степени приобретают ***полномочия*** работы с документами определенного грифа секретности

Главная задача: не допустить утечки информации из документов с высоким грифом секретности к сотрудникам с низким уровнем допуска

Достоинства моделей мандатного доступа

- *ясность и простота реализации*
- *отсутствие проблемы "Троянских коней" (контролируется направленность потоков, а не взаимоотношения конкретного субъекта с конкретным объектом, поэтому недекларированный поток троянской программы «сверху-вниз» будет считаться опасным и отвергнут МБО)*
- *каналы утечки не заложены в саму модель, а могут возникнуть только в практической реализации*

Недостатки моделей мандатного доступа

- *возможность скрытых каналов утечки - механизм, посредством которого субъект с высоким уровнем безопасности может предоставить определенные аспекты конфиденциальной информации субъекту, уровень безопасности которого ниже уровня безопасности конфиденциальной информации*
- *проблема удаленного доступа. В распределенных системах осуществление доступа всегда сопровождается потоком информации в прямом и обратном направлении, что в результате может приводить к нарушениям привил NRU и NWD*
- *проблема избыточности прав доступа. Без учета матрицы доступа (т.е. без использования дискреционного доступа) мандатный принцип доступа организует доступ более жестко, но и более грубо, без учета потребностей конкретных пользователей-субъектов*

МОДЕЛЬ РОЛЕВОГО (ТИПИЗОВАННОГО) ДОСТУПА

Множество потоков информации, характеризующих легальный доступ, задается через введение в системе дополнительных абстрактных сущностей – ролей, с которыми ассоциируются конкретные пользователи, и наделение ролевых субъектов доступа на основе дискреционного или мандатного принципа правами доступа к объектам системы.

Основная идея: политика и система защиты должны учитывать ***организационно-технологическое взаимодействие пользователей.*** *(Впервые была применена в продуктах управления доступом корпорации IBM в 70-80.гг.)*

Вместо субъекта

- ***пользователь*** (конкретная активная сущность)
- ***роль*** (абстрактная активная сущность)

Неформально ***Роль***: типовая работа в КС (ИС) определенной группы пользователей
Аналог: нормативное положение, функциональные обязанности и права сотрудников по определенной должности, *например могут быть роли* - кассира, бухгалтера, делопроизводителя, менеджера и т.п.

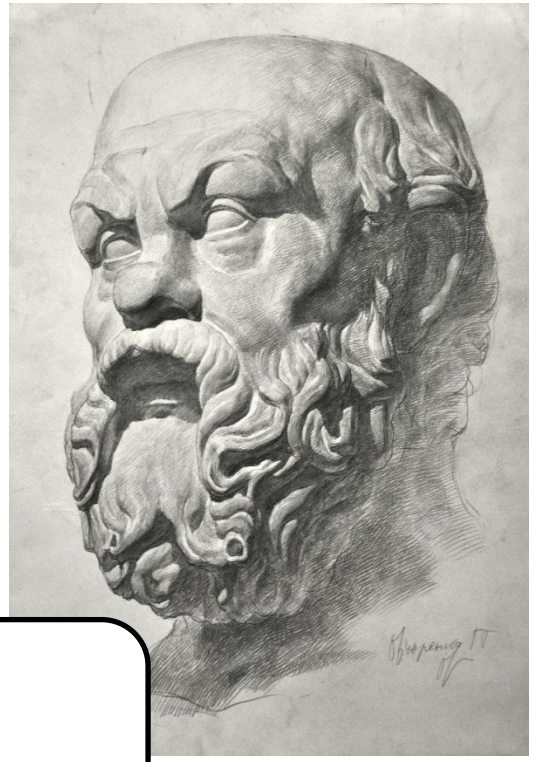
Наиболее распространены модели с иерархической системой ролей:

- чем выше роль по иерархии, тем больше полномочий
- если пользователю присвоена какая-то роль, то ему автоматически присваиваются все роли ниже по иерархии

MMS (military message system)-модель
Основная схема функционирования системы - пользователи после ***идентификации*** запрашивают у системы операции над сущностями от своего ***ID*** или от имени ***Роли***, с которой в данный момент ***авторизован.***

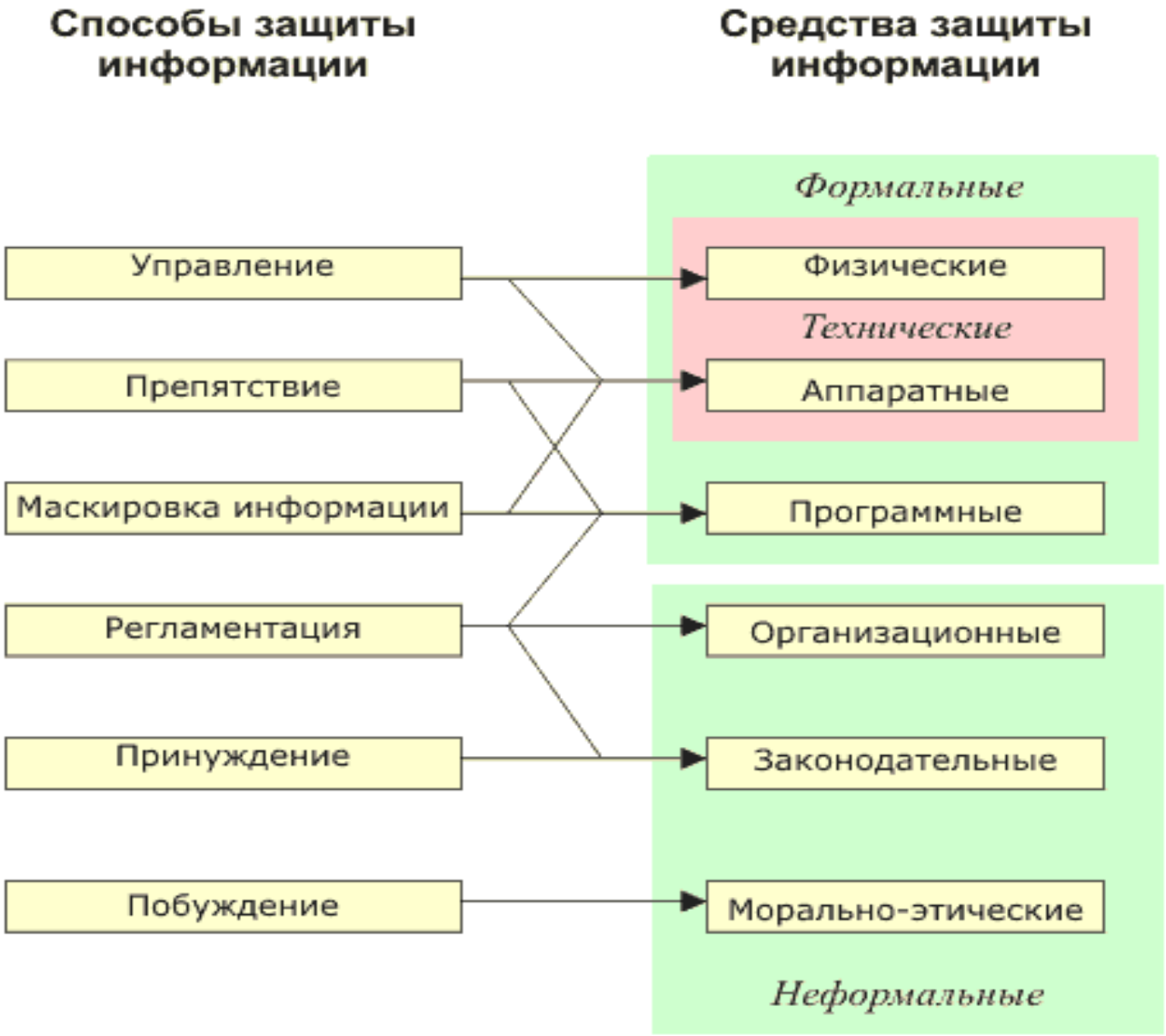
Модель Лендвера-Маклина (MMS) сочетает принципы: ***ролевой, дискреционной и мандатной моделей*** и оказывает сильное влияние на модели и технологии современных защищенных КС.

Выбор средств защиты системы информационной безопасности



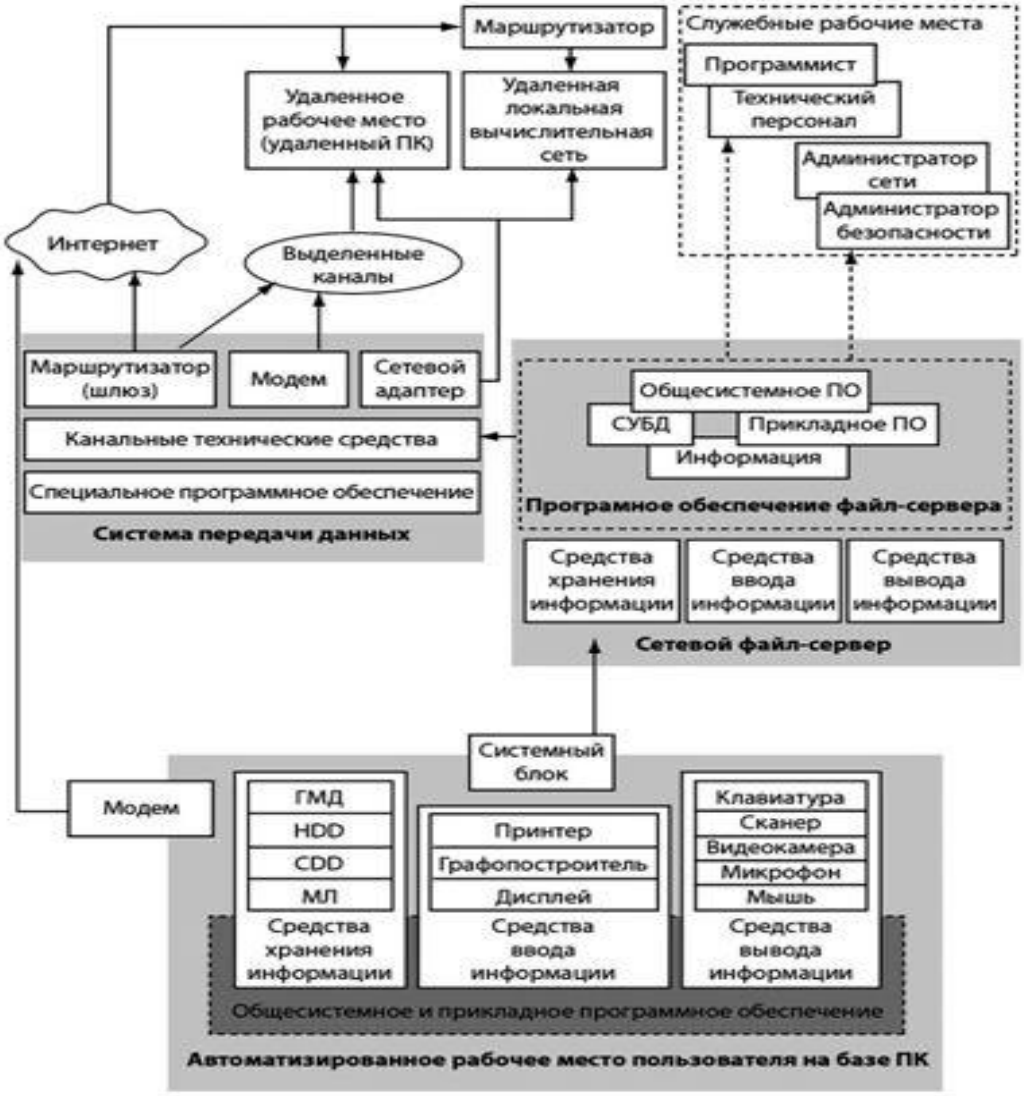
Сократ, мудрец

СПОСОБЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ



СОСТАВЛЯЮЩИЕ ИНФРАСТРУКТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

СХЕМА КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ, ВКЛЮЧАЮЩЕЙ ЛОКАЛЬНЫЕ СЕТИ И ВЫХОД В INTERNET



ТЕХНОЛОГИЧЕСКАЯ МОДЕЛЬ ПОДСИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ЗАЩИТА ПЕРВОГО УРОВНЯ ПОДСИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1-Й УРОВЕНЬ КИС :

- серверы,
- рабочие станции,
- персональные компьютеры различного назначения,
- коммуникационные устройства,
- программное обеспечение, реализующее работу устройств 1-го уровня.

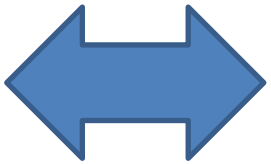
ЗАЩИТНЫЕ СРЕДСТВА

- защитные средства операционных систем,
- антивирусные пакеты,
- средства и устройства аутентификации пользователя,
- средства криптографической защиты паролей и данных прикладного уровня.

ЗАЩИТА ВТОРОГО УРОВНЯ ПОДСИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2-Й УРОВЕНЬ КИС :

локальные сети из рабочих станций, серверов и персональных компьютеров, которые организуют внутреннее Intranet-пространство предприятия и могут быть иметь выходы во внешнее Internet-пространство. — уровня защиты локальных сетей, который обычно включает:



СРЕДСТВА ИНФОРМАЦИОННОЙ ЗАЩИТЫ (СЗИ) ВТОРОГО УРОВНЯ

- **средства безопасности сетевых ОС;**
- **средства аутентификации пользователей (User Authentication Facilities — UAF);**
- **средства физического и программного разграничения доступа к распределенным и разделяемым информационным ресурсам;**
- **средства защиты домена локальной сети (Local Area Network Domain — LAND);**
- **средства промежуточного доступа (Proxy Server) и межсетевые экраны (Firewall);**
- **средства организации виртуальных локальных подсетей (Virtual Local Area Network — VLAN);**
- **средства обнаружения атаки и уязвимостей в системе защиты локальных сетей.**

ЗАЩИТА ТРЕТЬЕГО УРОВНЯ ПОДСИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3-Й УРОВЕНЬ КИС :

объединение нескольких локальных сетей географически распределенного предприятия в общую корпоративную Intranet-сеть через открытую сеть на базе современных технологий поддержки и сопровождения таких сетей (Quality of Service — QoS) с использованием открытой среды Internet в качестве коммутационной среды

СРЕДСТВА ЗАЩИТЫ ТРЕТЬЕГО УРОВНЯ

технологии защищенных виртуальных сетей (Virtual Private Networks — VPN).

VPN-технологии часто интегрируются со средствами первого и второго уровней. Защищенный VPN-канал может реализовываться не только до маршрутизаторов доступа и пограничных Fairwall'лов, но и до серверов и рабочих станций локальной сети.

ЗАЩИТА ЧЕТВЕРТОГО УРОВНЯ ПОДСИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4-Й УРОВЕНЬ КИС :

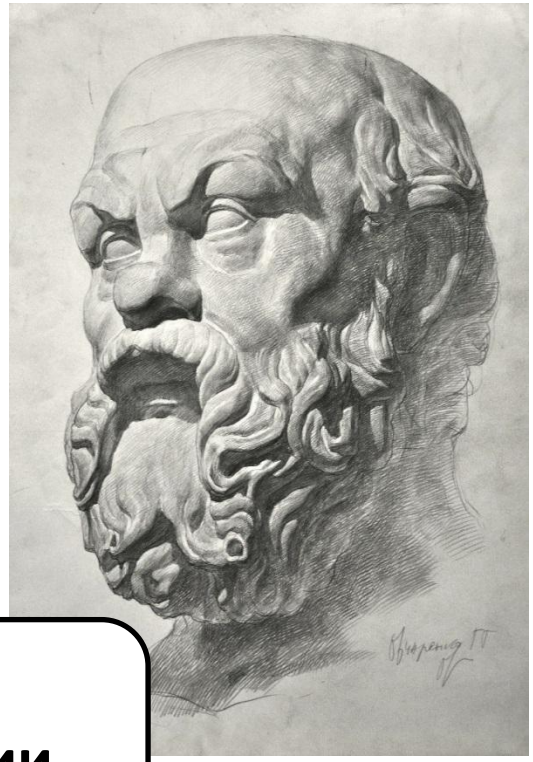
организация защищенного межкорпоративного обмена в среде электронного бизнеса (eBusiness)

СРЕДСТВА ЗАЩИТЫ ЧЕТВЕРТОГО УРОВНЯ

методы и технологии управления публичными ключами и сертификатами криптографической защиты (Public Key Infrastructure — PKI).

Базой для реализации средств защиты будут электронная цифровая подпись (Electronic Digital Signature — EDS) и VPN-технологии

Криптографическая защита информации



Сократ, мудрец

ТЕХНОЛОГИИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Криптография - это совокупность технических, математических, алгоритмических и программных методов преобразования данных (шифрование данных), которая делает их бесполезными для любого пользователя, у которого нет ключа для расшифровки.

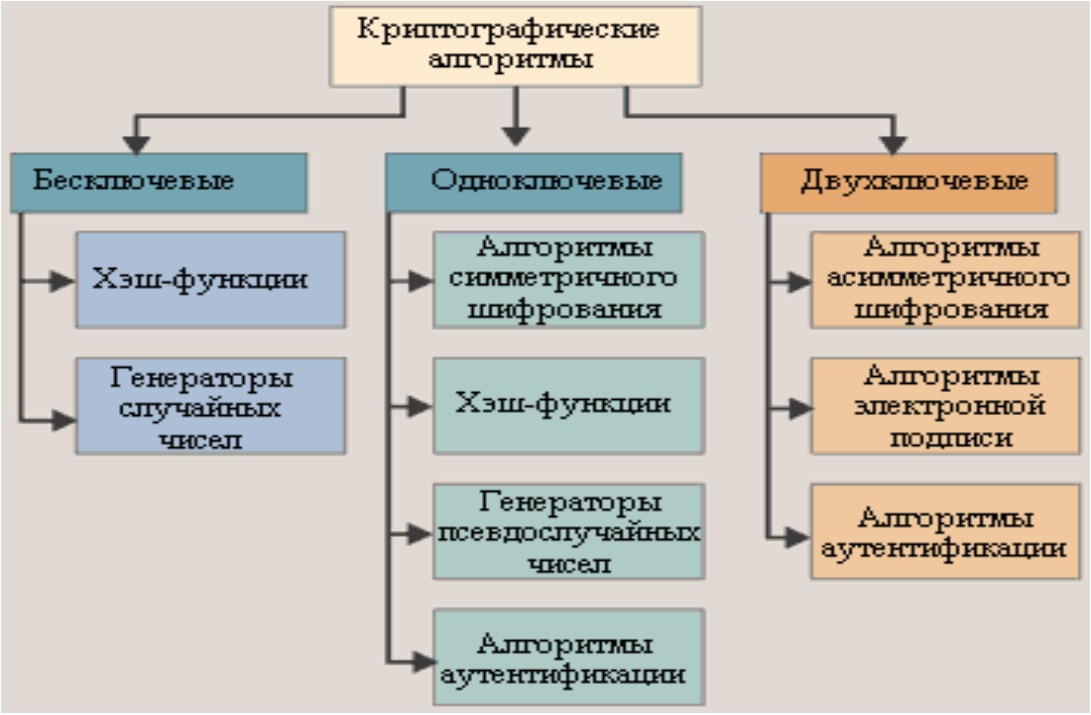
Криптографические преобразования обеспечивают решение следующих базовых задач защиты:

- **конфиденциальности (невозможности прочитать данные и извлечь полезную информацию)**
- **целостности (невозможность модифицировать данные для изменения смысла или внесения ложной информации).**

КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ

ТЕХНОЛОГИИ КРИПТОГРАФИИ ПОЗВОЛЯЮТ РЕАЛИЗОВАТЬ СЛЕДУЮЩИЕ ПРОЦЕССЫ ИНФОРМАЦИОННОЙ ЗАЩИТЫ:

- **идентификация (отождествление) объекта или субъекта сети или информационной системы;**
- **аутентификация (проверка подлинности) объекта или субъекта сети;**
- **контроль/разграничение доступа к ресурсам локальной сети или внесетевым сервисам;**
- **обеспечение и контроль целостности данных.**



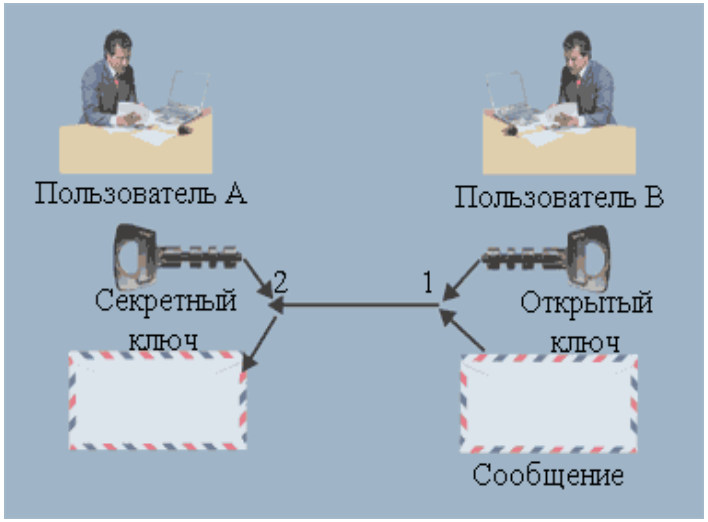
СИММЕТРИЧНОЕ И АССИМЕТРИЧНОЕ ШИФРОВАНИЕ

СИММЕТРИЧНОЕ ШИФРОВАНИЕ

отправитель и получатель владеют одним и тем же ключом (секретным), с помощью которого они могут зашифровывать и расшифровывать данные.

Недостатки:

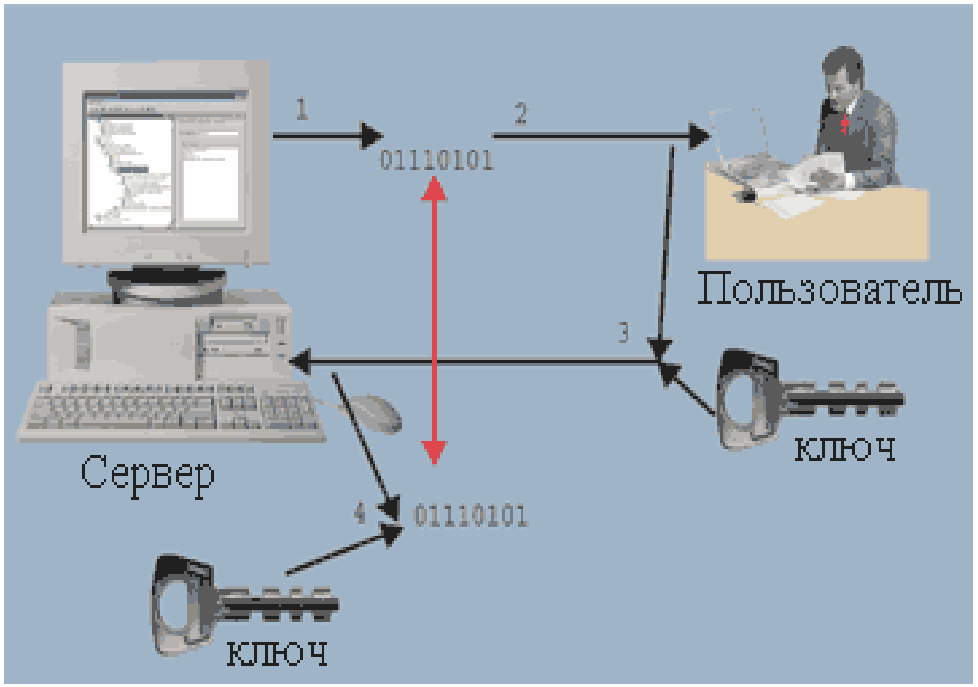
- **очень сложно найти безопасный механизм, при помощи которого отправитель и получатель смогут тайно от других выбрать ключ. Возникает проблема безопасного распространения секретных ключей;**
- **для каждого адресата необходимо хранить отдельный секретный ключ;**
- **в схеме симметричного шифрования невозможно гарантировать личность отправителя, поскольку два пользователя владеют одним ключом.**



АСИММЕТРИЧНОЕ ШИФРОВАНИЕ

1. **Пользователь В зашифровывает сообщение на открытом ключе пользователя А (который когда-либо передал его пользователю В).**
2. **Пользователь А расшифровывает сообщение своим секретным ключом.**

ПРИМЕР АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ СЕРВЕРОМ



Сервер проверяет «истинность» удаленного пользователя:

1. **Сервер генерирует случайное число.**
2. **Отправляет его пользователю.**
3. **Пользователь зашифровывает полученное число секретным ключом и отправляет результат серверу.**
4. **Сервер расшифровывает полученные данные таким же секретным ключом.**
5. **Сравнивает с исходным числом.**

Равенство чисел означает, что пользователь обладает требуемым секретным ключом, т.е. ему удалось доказать свою легитимность.

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ

Электронная цифровая подпись (ЭЦП) — реквизит электронного документа, позволяющий установить отсутствие искажения информации в документе и проверить принадлежность подписи конкретному лицу

Простая ЭЦП *

Подтверждает, что электронное сообщение отправлено конкретным лицом. Предназначена для подписания электронных сообщений, направляемых в государственный орган, орган местного самоуправления или должностному лицу

Иванов

Усиленная ЭЦП *

Позволяет не только идентифицировать отправителя, но и подтвердить, что с момента подписания документ не менялся. Применяется во всех видах отношений, если иное не установлено нормативным правовым актом или соглашением участников отношений

** Сообщение с простой или усиленной ЭЦП может быть приравнено к бумажному документу, подписанному собственноручно (по предварительной договоренности сторон), а также в специально предусмотренных законом случаях*

Иванов

Квалифицированная ЭЦП **

Предназначена для взаимодействия госорганов с использованием государственных информационных систем

*** Дополнительно подтверждается сертификатом от аккредитованного удостоверяющего центра, а сообщение во всех случаях приравнивается к бумажному документу с собственноручной подписью*

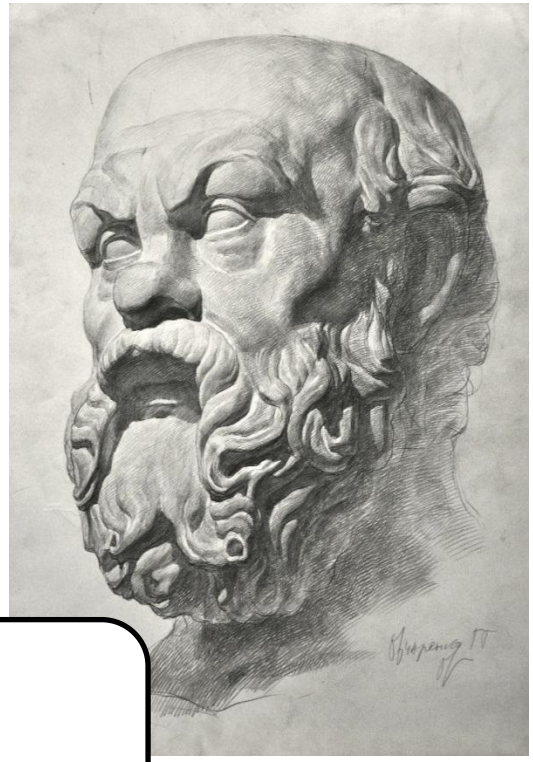
Иванов

Кто может получить ЭЦП?

- Юридические лица
- Индивидуальные предприниматели
- Физические лица

Как получить ЭЦП?

ЭЦП выдается центром сертификации (удостоверяющим центром)



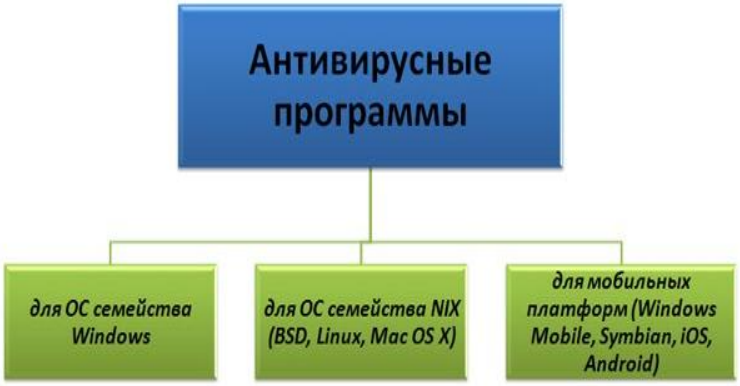
Сократ, мудрец

Антивирусные программы

АНТИВИРУСНЫЕ ПРОГРАММЫ

Классификация по используемым технологиям защиты

АНТИВИРУСНЫЕ ПРОГРАММЫ



Классификация по целевым платформам

Классификация по функционалу

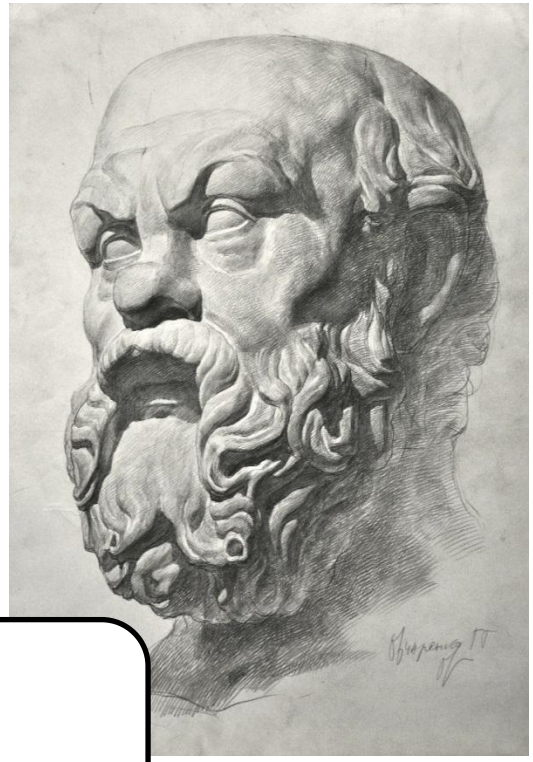
ПРИМЕРЫ АВП

Scan McAfee Associates и Aidstest позволяют обнаруживать около 1000, но всего их более пяти тысяч!

Norton AntiVirus или AVSP (программы-детекторы) могут настраивать на новые типы вирусов, им необходимо лишь указать комбинации байтов, присущие этим вирусам. Тем не менее, невозможно разработать такую программу, которая могла бы обнаруживать любой заранее неизвестный вирус.

Антивирус Касперского (AVP) использует все современные типы антивирусной защиты: антивирусные сканнеры, мониторы, поведенческие блокираторы и ревизоры изменений. Различные версии продукта поддерживают все популярные операционные системы, почтовые шлюзы, межсетевые экраны (firewalls), web-серверы.
Система позволяет контролировать все возможные пути проникновения вирусов на компьютер пользователя, включая Интернет, электронную почту и мобильные носители круга задач обеспечения безопасности, и обладает рядом специфических свойств. Концепция AVP позволяет легко и регулярно обновлять антивирусные программы, путем замены антивирусных баз – набора файлов с расширением AVC, которые на сегодняшний день позволяют обнаруживать и удалять более 50000 вирусов.

Средства защиты АСУ ТП

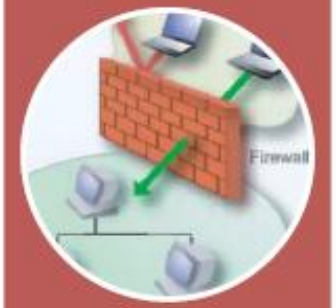


Сократ, мудрец

ВЫБОР СРЕДСТВ ЗАЩИТЫ ДЛЯ АСУ ТП

Физической безопасности

ограничение физического доступа к панелям управления, диспетчерским и другим помещениям, устройствам, кабелям



Сетевой безопасности сетевая инфраструктура

межсетевые экраны со встроенными сенсорами систем предотвращения вторжения и средства защиты, интегрированные в сетевое оборудование (коммутаторы и маршрутизаторы)

Безопасности рабочих станций и серверов

управление обновлениями ПО, применение антивирусного ПО, удаление неиспользуемых приложений, протоколов и сервисов

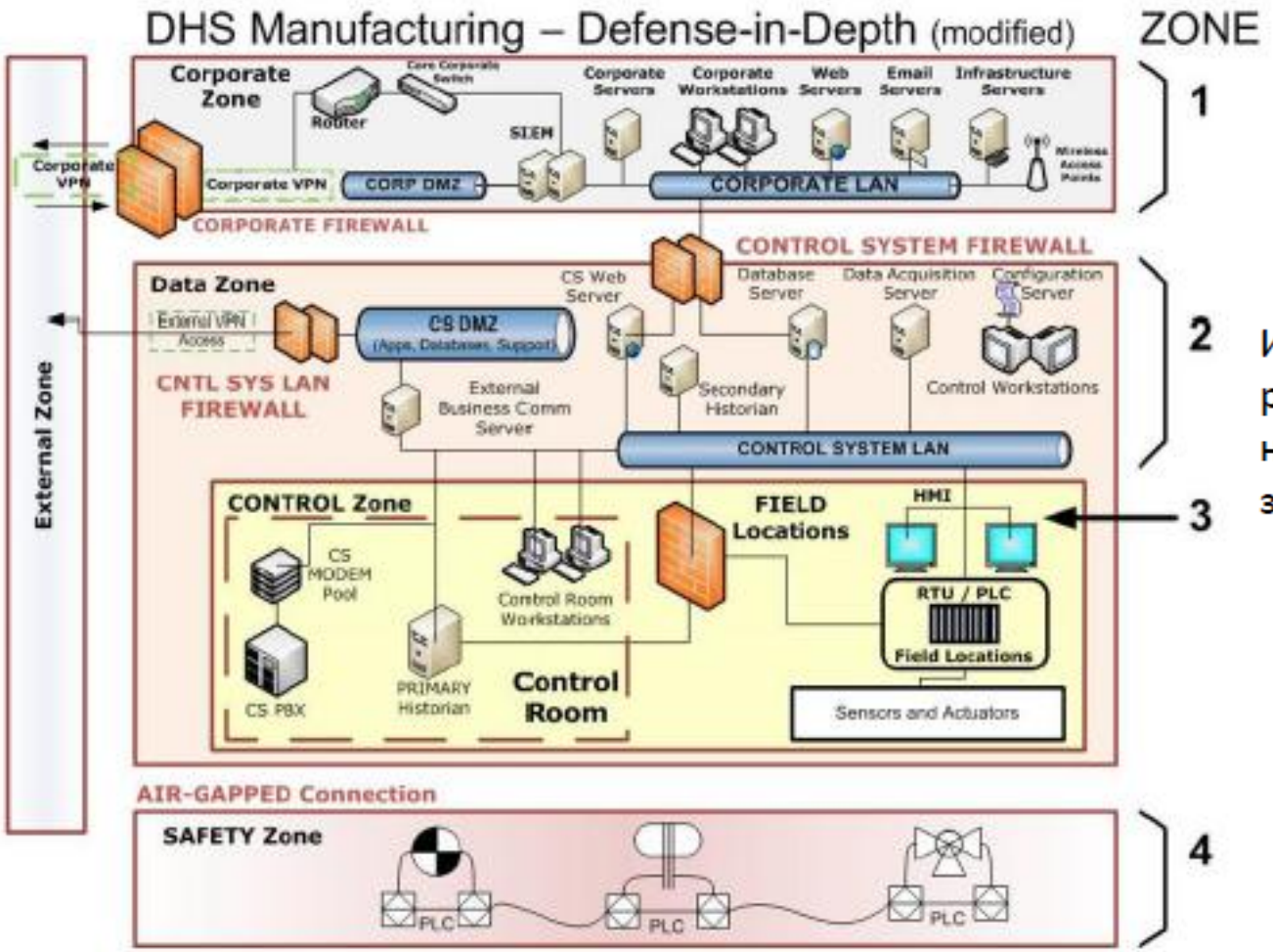
Безопасности приложений

аутентификация, авторизация и аудит при доступе к приложениям

Безопасности устройств

контроль над изменениями и ограничение доступа).

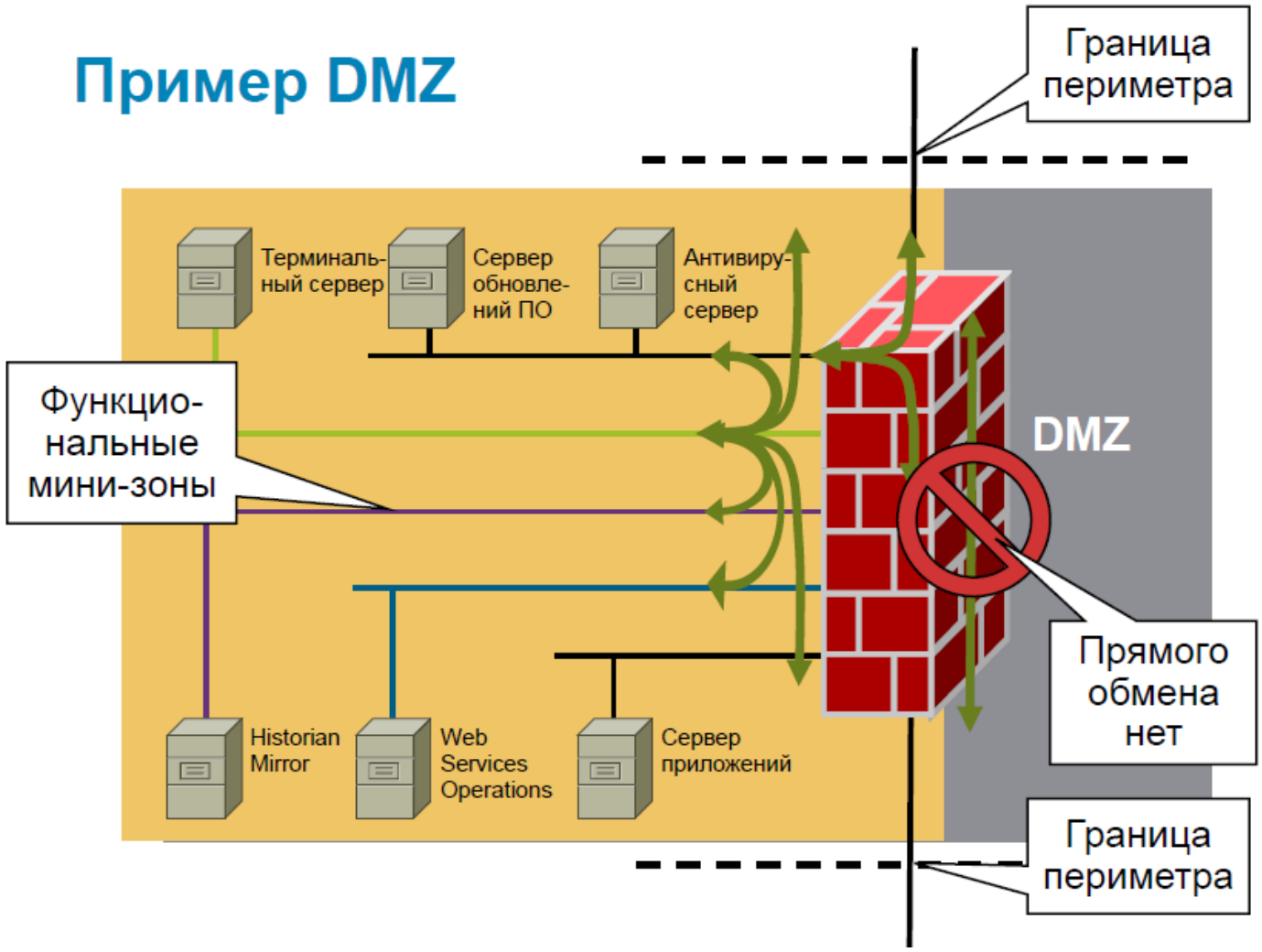
ЭШЕЛОНИРОВАННЫЙ ПОДХОД



Инфраструктура разбивается на изолированные зоны безопасности

Источник: рекомендации от американской транспортной ассоциации APTA

СОЗДАНИЕ ДЕМИЛИТАРИЗОВАННЫХ ЗОН



КЛЮЧЕВЫЕ МЕХАНИЗМЫ КИБЕРБЕЗОПАСНОСТИ АСУ ТП

1. Доверенная операционная среда

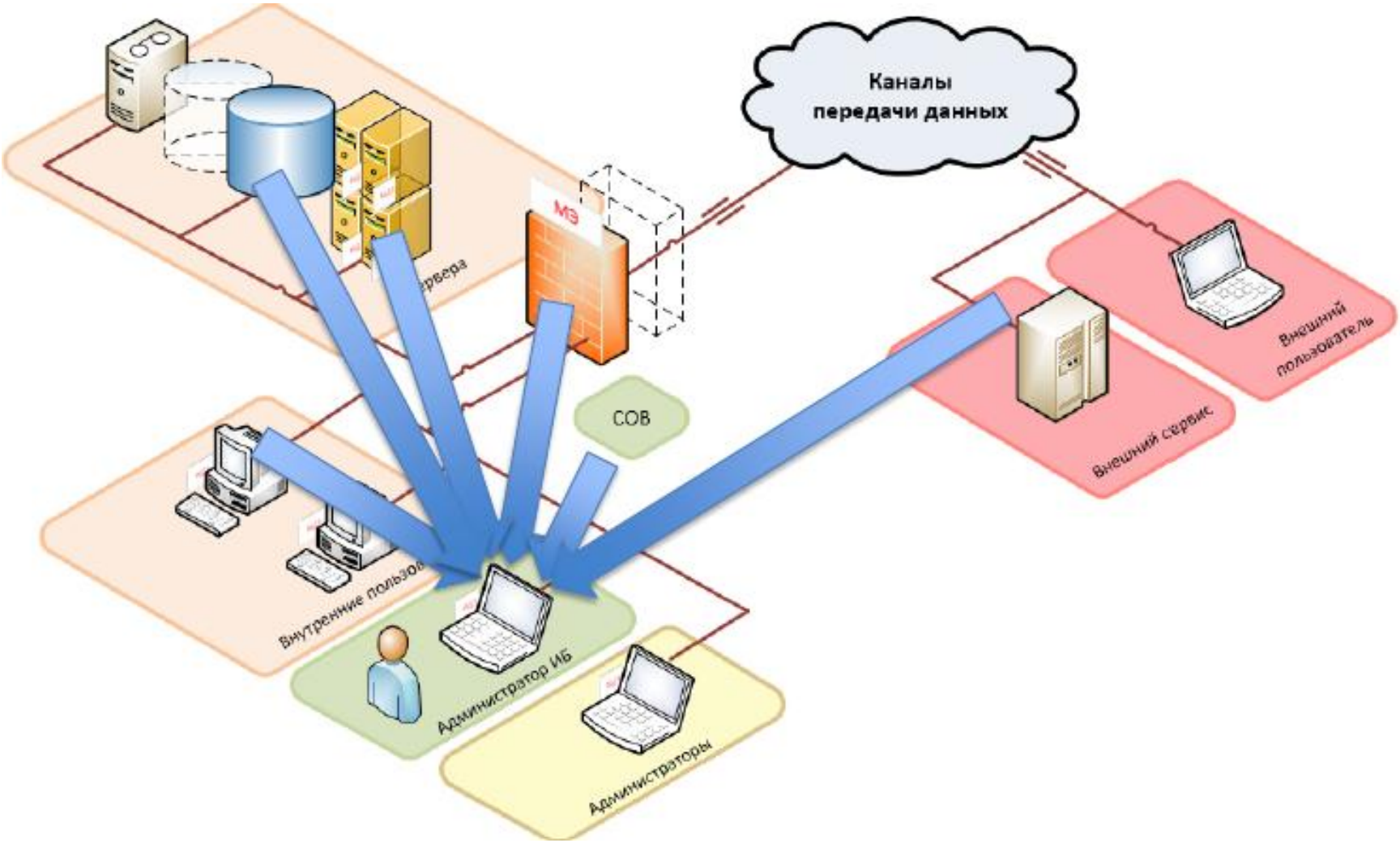
2. Эффективное межсетевое экранирование

3. Эффективный мониторинг событий ИБ и управление инцидентами

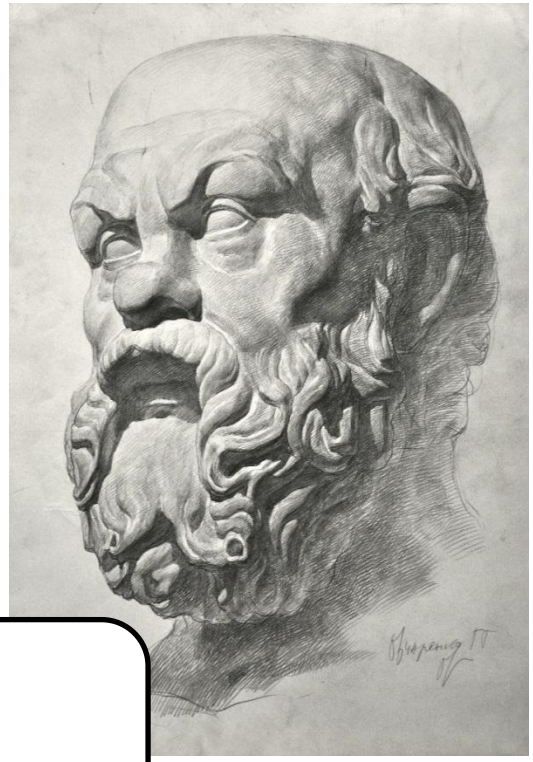
4. Эффективный контроль защищенности

5. Доверенное (безопасное) программное обеспечение

ОСУЩЕСТВЛЕНИЕ МОНИТОРИНГА ВСЕЙ ИНФРАСТРУКТУРЫ



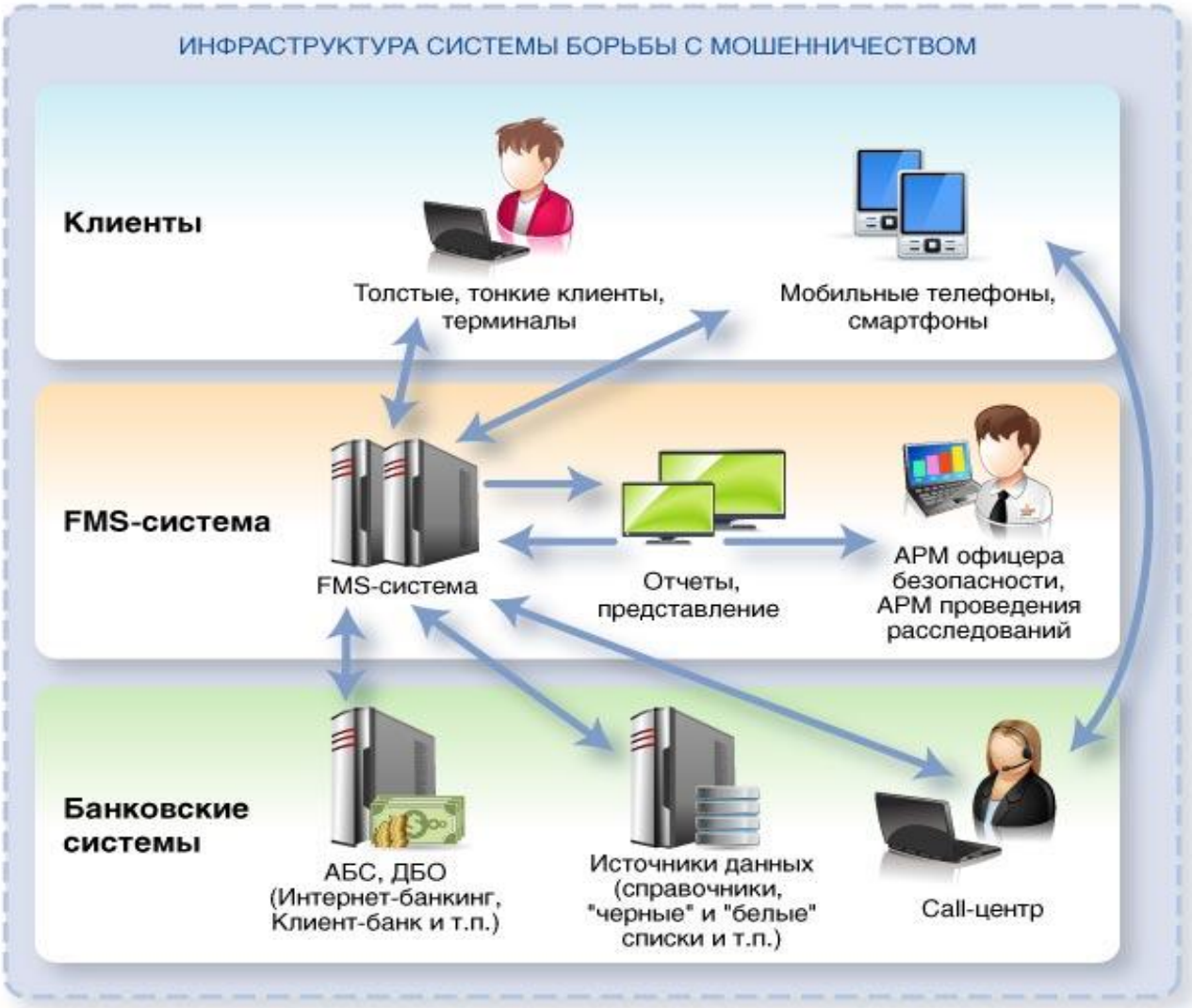
Защита электронных финансов



Сократ, мудрец

ЗАЩИТА ЭЛЕКТРОННЫХ ФИНАНСОВ

БОРЬБА С МОШЕННИЧЕСТВОМ В БАНКОВСКИХ СИСТЕМАХ



ПЕРСПЕКТИВЫ В ЗАЩИТЕ ОН-ЛАЙН ПЛАТЕЖЕЙ

Без установки дополнительного программного обеспечения на устройства клиентов, в режиме реального времени Bot-Trek SB выявляет подготовку и хищение денежных средств с использованием:

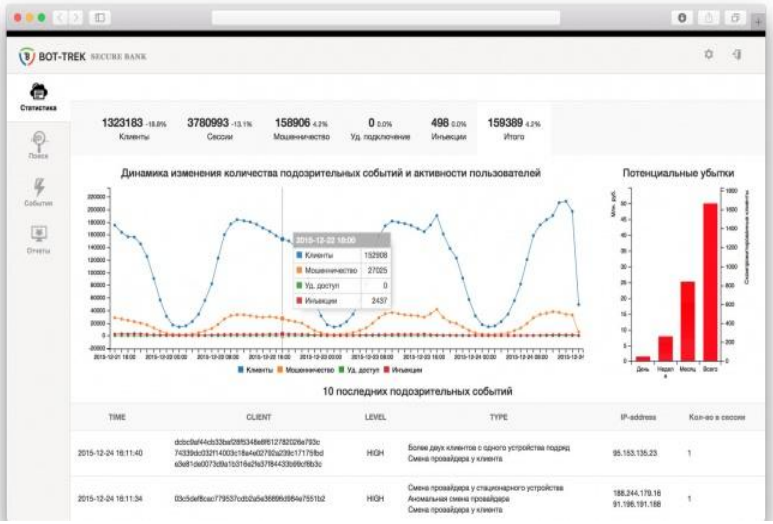
- **внедрения зловредных инъекций на страницы интернет-банкинга для получения аутентификационных и дополнительных данных для проведения платежа**
- **фишинговых атак и приемов социальной инженерии**
- **несанкционированных удаленных подключений к устройству клиента и проведения транзакции от его имени**
- **вредоносного кода для автоматического создания платежа или подмены реквизитов получателя на устройстве клиента**
- **модернизации вредоносного кода и проникновения через уязвимости «нулевого» дня.**

Решения Group-IB

Преимущества Bot-Trek Secure Bank

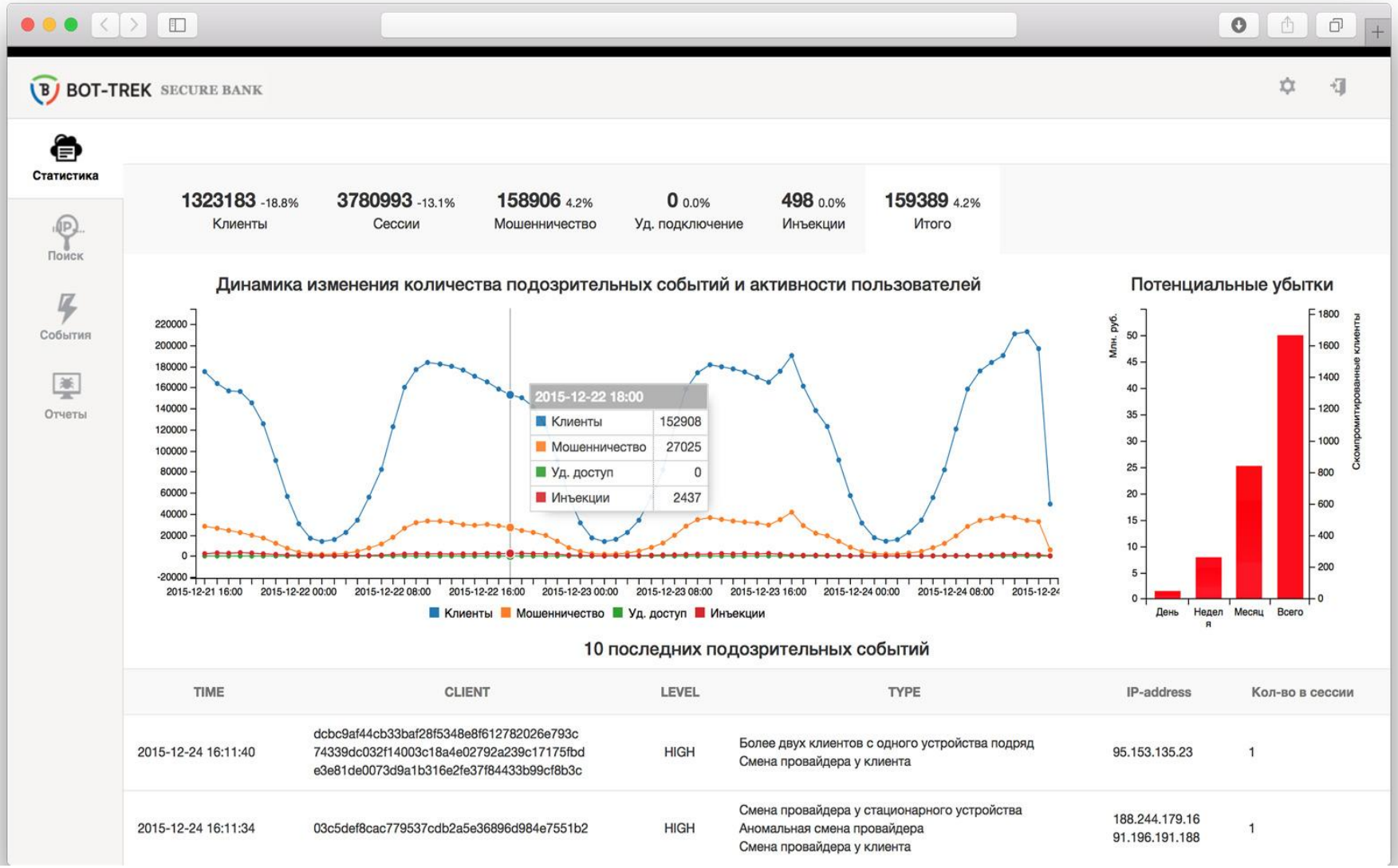
	Антифрод-системы	Антивирусы	Спец. агентские решения	SMS OTP	Token	Bot-Trek SB
Внедрение в ДБО			✓	✓	✓	✓
Удаленное подключение	Существенный процент ложных срабатываний	Опосредованно защищает — млн. компьютеров заражены, несмотря на антивирус	✓	✓	✗	✓
Фишинг/форминг			✓	✗	✓	✓
«Автозаливы»			✓	✗	✗	✓
Дополнительные проблемы	Издержки на звонки клиентам	Банк не знает, стоит ли у клиента антивирус, который выявляет вирус, а не мошенническую активность	1% роста установивших клиентов в год	Лавинообразный рост инфицированных мобильных устройств	Крайне низкое распространение для клиентов — физических лиц	✓

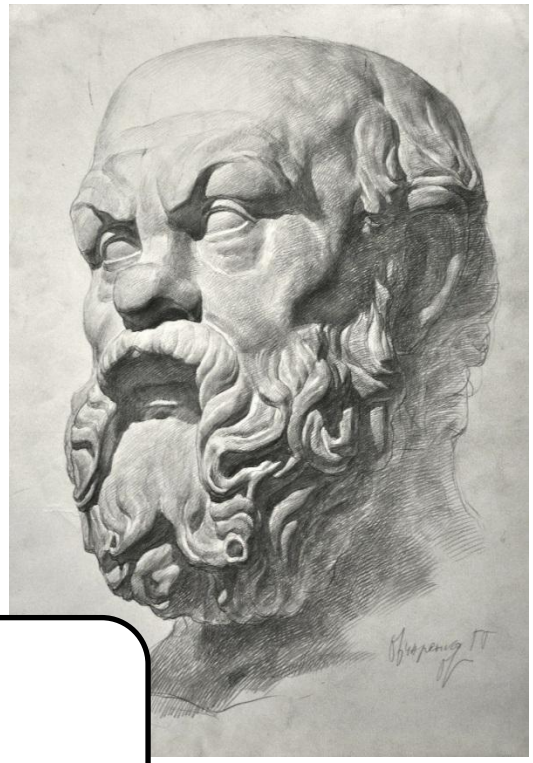
Bot-Trek Secure Bank дополняет существующие решения



ОКНО СИСТЕМЫ BOT-TREK

Решения Group-IB





Сократ, мудрец

Библиография

Основная литература

1. Шульц В.Л., Рудченко А.Д., Юрченко А.В. Безопасность предпринимательской деятельности. М.: Издательство «Юрайт», 2016;
2. Шульц В.Л., Рудченко А.Д., Юрченко А.В. Пособие для обучения на майноре. (на начальном этапе)

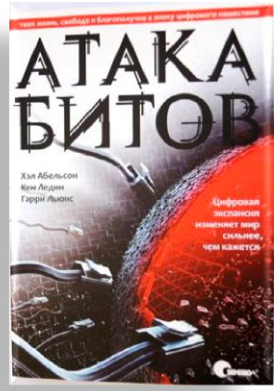
Дополнительная литература

3. Литература для продвинутых слушателей (см. следующий слайд)

Нормативные акты

4. ISO/IEC 15408 «Общие критерии безопасности информационных технологий»

5. ISO 17799 «Информационные технологии — Технологии безопасности — Практические правила менеджмента информационной безопасности»


АТАКА БИТОВ
Хэл Абельсон
Кен Леди
Гарри Льюис
Цифровая экспансия изменит мир сильнее, чем кажется


Национальная платежная система
Бизнес-энциклопедия


Безопасность карточного бизнеса
Бизнес-энциклопедия
МФПА
CompuTel
Золотая Корона


Обеспечение информационной безопасности бизнеса
под редакцией А.П. Курило
IBM
CompuTel


Д.А. Мельников
ОРГАНИЗАЦИЯ И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО - ТЕХНОЛОГИЧЕСКИХ СЕТЕЙ И СИСТЕМ
IDO PRESS


ВИКИ ЛИКС
КОМПРОМАТ НА РОССИЮ


Е. П. Ищенко
ВИРТУАЛЬНЫЙ КРИМИНАЛ


Юрий Жуков
ОСНОВЫ ВЕБ-ХАКИНГА
НАПАДЕНИЕ И ЗАЩИТА
DVD
ПИТЕР


ВОПРОСЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ
А. П. Курило
Н. Г. Милославская
М. Ю. Сенаторов
А. И. Толстой
ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ


ВОПРОСЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ
Н. Г. Милославская
М. Ю. Сенаторов
А. И. Толстой
УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ


Крис Просис
Кевин Мандиа
Расследование компьютерных преступлений


СЕРИЯ «ВЫСШАЯ ШКОЛА»
А.Ю. Щербаков
СОВРЕМЕННАЯ КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ
Теоретические основы
Практические аспекты
Учебное пособие


В.А.Сердюк
ОРГАНИЗАЦИЯ И ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ
ОБНАРУЖЕНИЕ И ПРЕДОТВРАЩЕНИЕ ИНФОРМАЦИОННЫХ АТАК В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРЕДПРИЯТИЙ


Основы современной криптографии и стеганографии


Дж. Макнамара
СЕКРЕТЫ КОМПЬЮТЕРНОГО ШПИОНАЖА
ТАКТИКА И КОНТРМЕРЫ