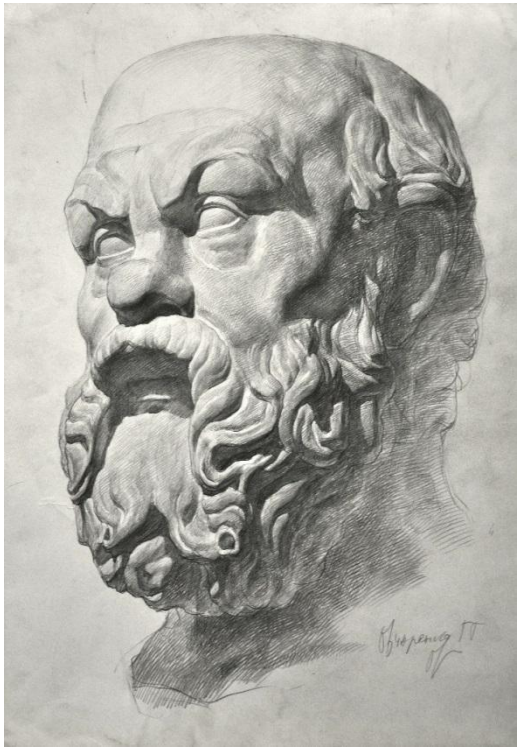
Комплексное противодействие атакам на информационные и материальные ресурсы бизнеса

Тема № 8

# Защита информации в сети Интернет. Расследование киберинцидентов

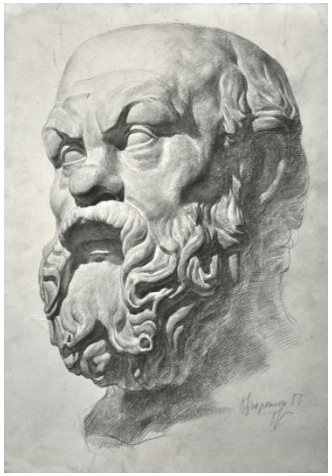
Лекция, 2 часа



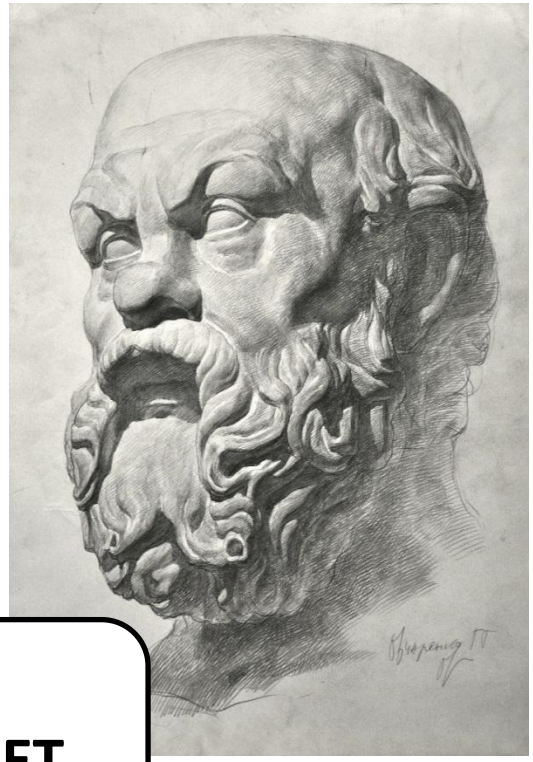
Сократ, мудрец

Информационная безопасность

## Оглавление

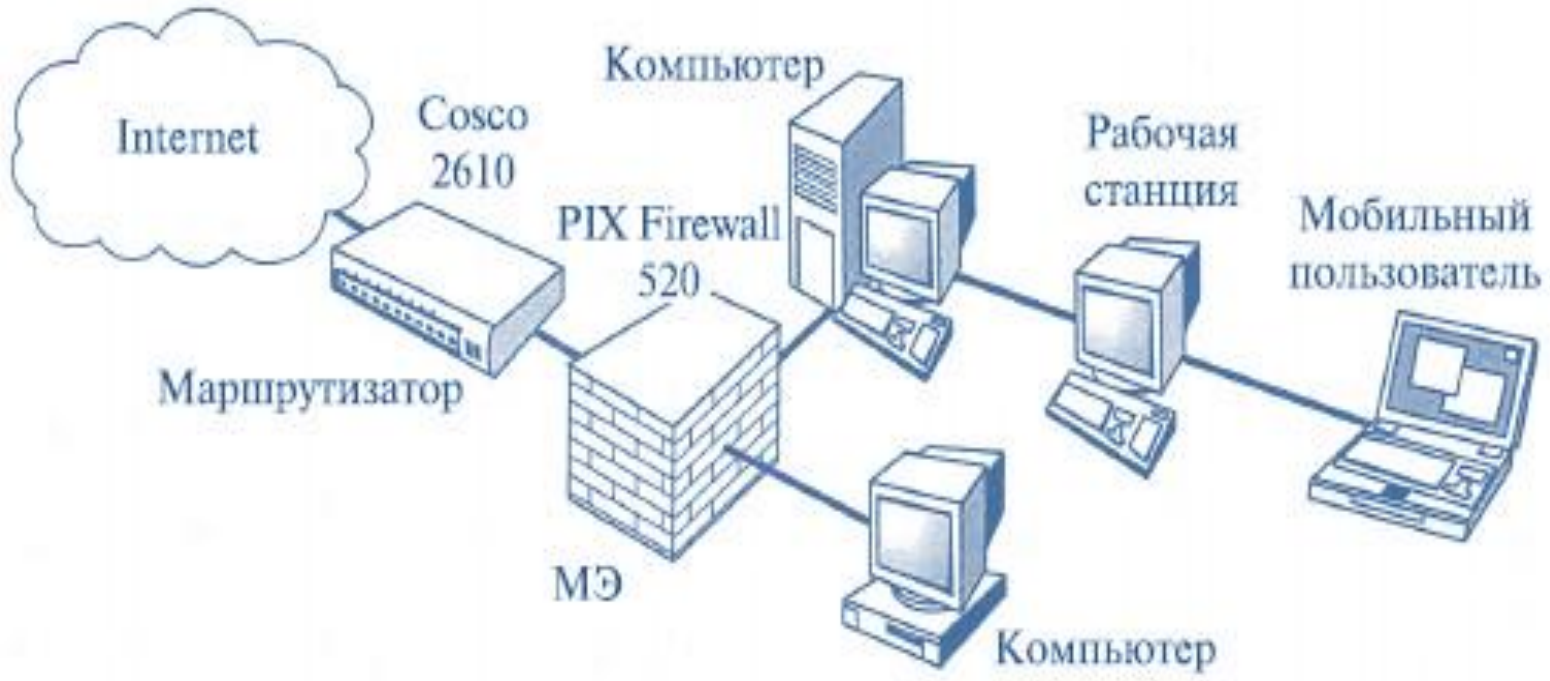


# ЗАЩИТА ИНФОРМАЦИИ В СЕТИ ИНТЕРНЕТ



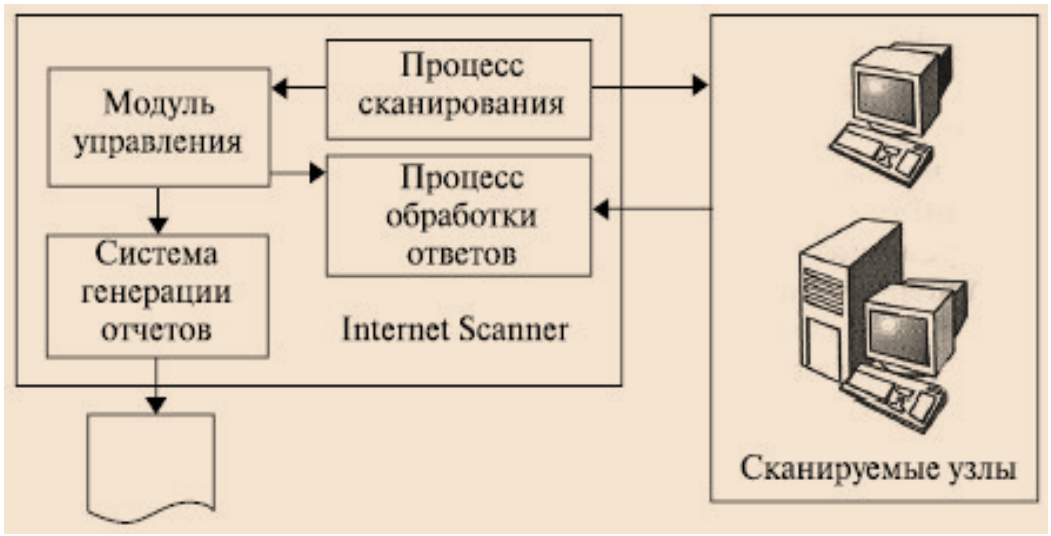
Сократ, мудрец

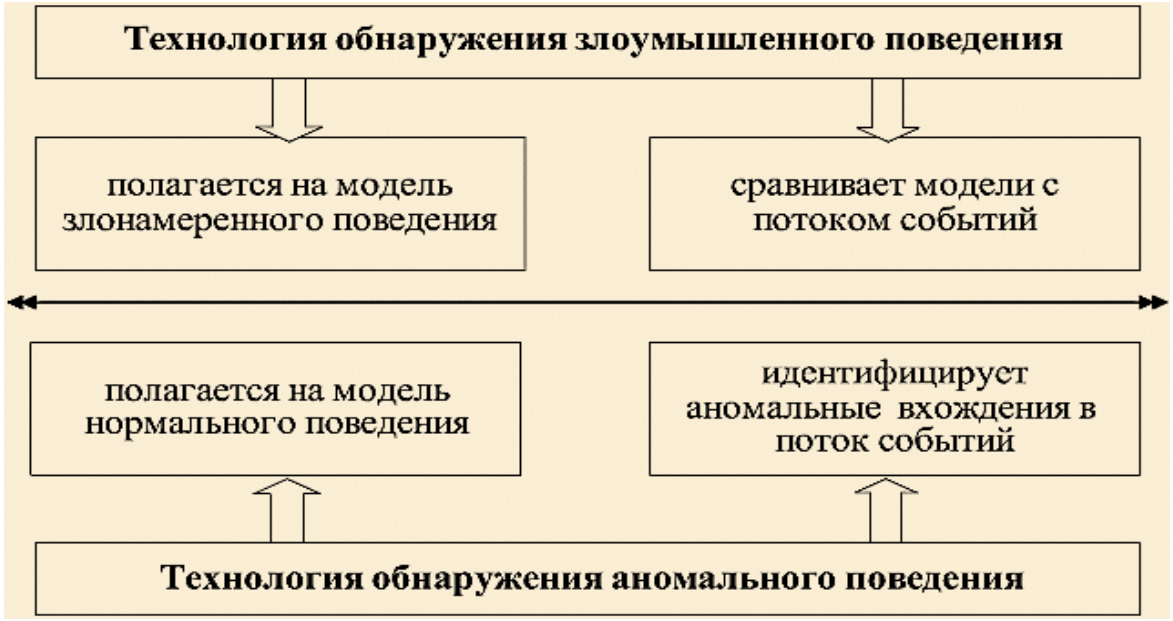
# СИСТЕМЫ РАЗГРАНИЧЕНИЯ ДОСТУПА И МЕЖСЕТЕВЫЕ ЭКРАНЫ



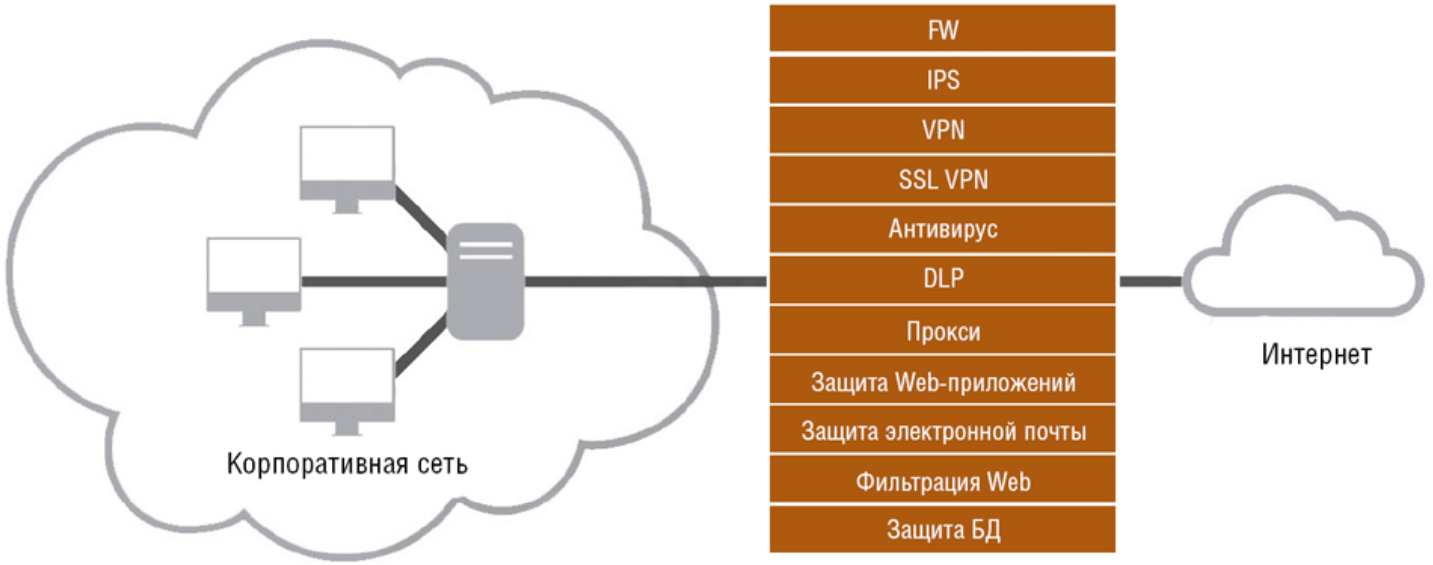

**Использование комплекса "маршрутизатор-файерволл" в системах защиты информации при подключении к Internet**

# СИСТЕМЫ ОБНАРУЖЕНИЯ АТАК



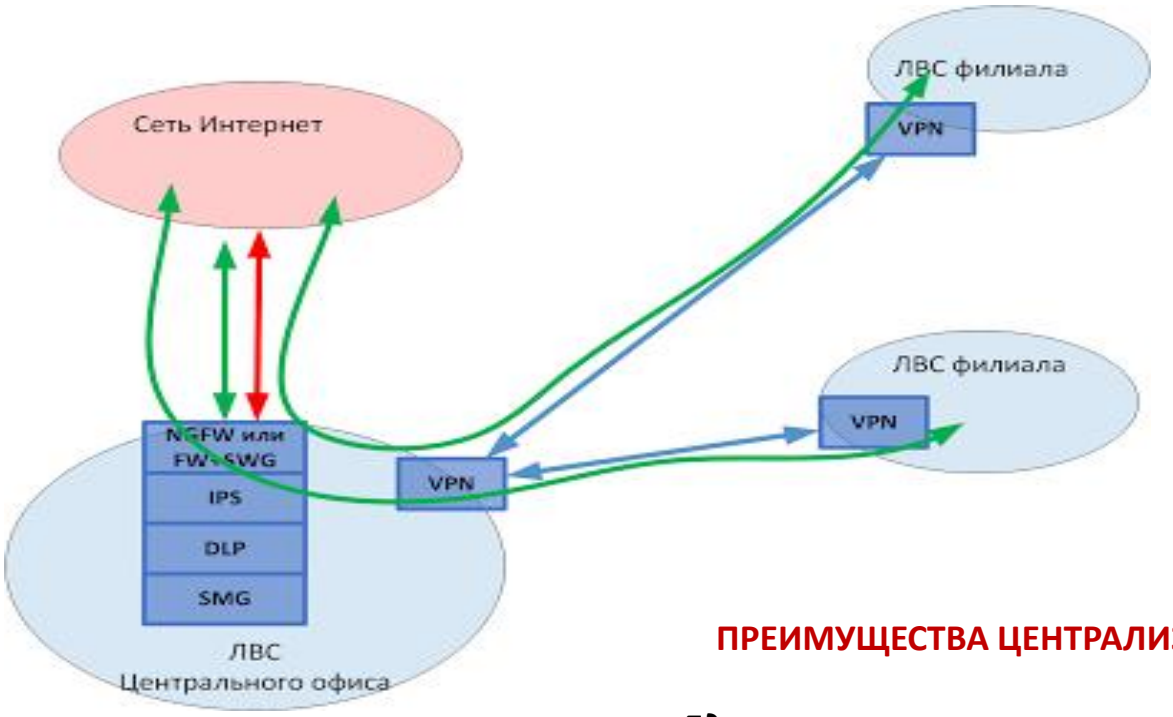



# ЭВОЛЮЦИЯ СИСТЕМ СЕТЕВОЙ БЕЗОПАСНОСТИ




**Многофункциональные шлюзы безопасности (UTM) объединяют наиболее востребованные функции: межсетевое экранирование, предотвращение вторжений, криптографическую защиту каналов связи, защищенный удаленный доступ (VPN), антивирусную защиту сетевого трафика, защиту электронной почты, DLP, фильтрацию Web, мониторинг и оптимизацию трафика.**

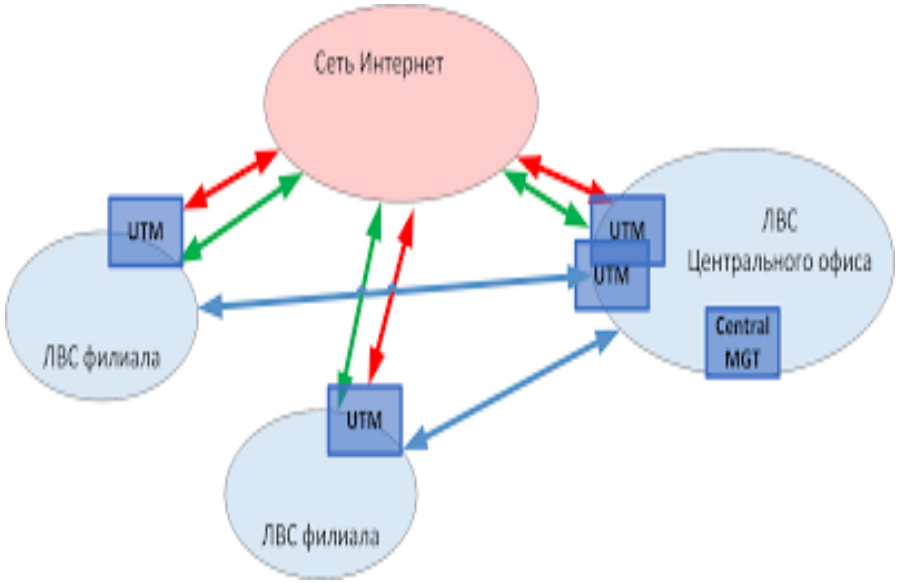
# ОРГАНИЗАЦИЯ ЗАЩИТЫИНФОРМАЦИИ ПРИ ЦЕНТРАЛИЗОВАННОМ ДОСТУПЕ




**ПРЕИМУЩЕСТВА ЦЕНТРАЛИЗОВАННОГО ВАРИАНТА :**

- ***Единая точка контроля взаимодействия со внешними сетями, а значит более надежный и простой контроль***
- ***Меньшие затраты на управление (в данном случае 1 шлюз DLP, а не 50 шлюзов DLP)***
- ***Меньшие затраты на мониторинг и анализ инцидентов (в данном случае события поступают от 3-5 источников, а не от 50)***

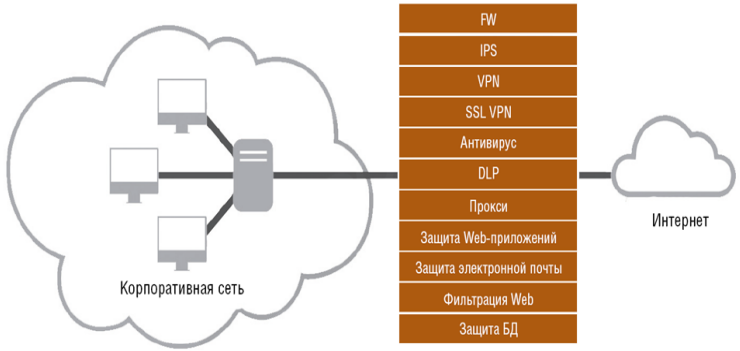
# ОРГАНИЗАЦИЯ ЗАЩИТЫИНФОРМАЦИИ ПРИ ДЕЦЕНТРАЛИЗОВАННОМ ДОСТУПЕ



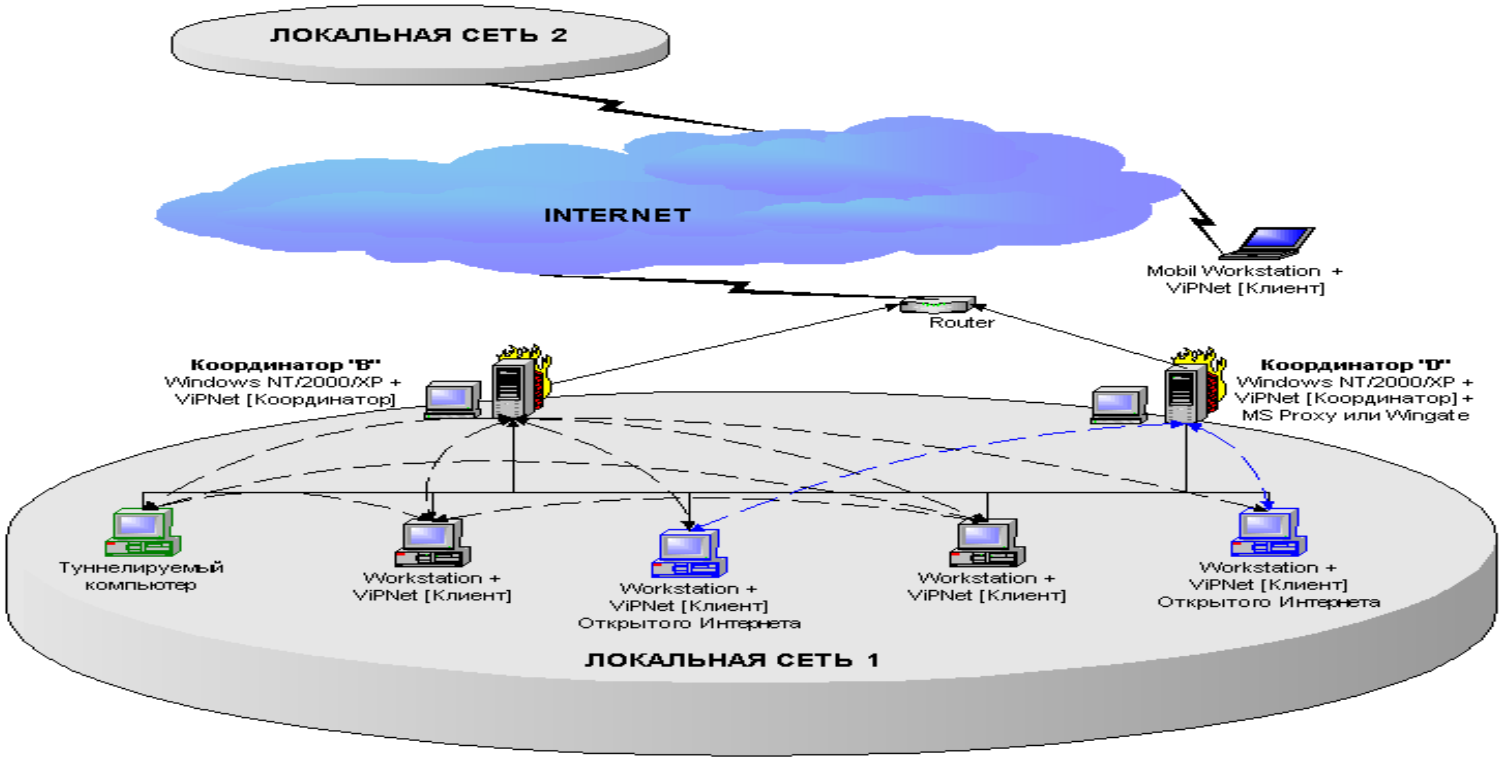

**ПРЕИМУЩЕСТВА ДЕЦЕНТРАЛИЗОВАННОГО ВАРИАНТА :**

- ***Независимость от доступности одного-двух офисов.***
- ***Экономия трафика (так как в случае централизованного доступа, трафик из удаленных офисов оплачивается дважды – в центральном офисе для этого должны быть предусмотрены каналы более высокой пропускной способности).***
- ***Большие возможности для делегирования обязанностей по управлению в удаленные офисы.***

***Для работы функций UTM на небольшом устройстве в удаленном офисе они упрощаются*** *(уменьшается количество сигнатур, поддерживаемых протоколов)* ***либо настраиваются так, чтобы были задействованы только выборочно несколько функций.*** *При этом должна обеспечиваться возможность корректно настроить устройства чтобы в наиболее опасных направлениях была более глубока защита.*

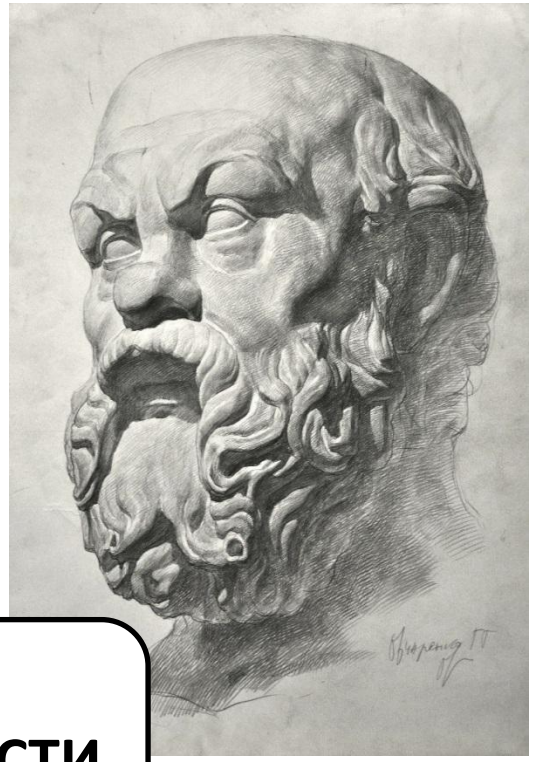


# ПРИМЕНЕНИЕ СИСТЕМ ШИФРОВАНИЯ - ТЕХНОЛОГИЯ "ОТКРЫТЫЙ ИНТЕРНЕТ"




*Путем установки на выходе из локальной сети специального ViPNet[координатора] (Координатор "D") внутри распределенной сети может быть организован* ***виртуальный контур частично или полностью изолированный от остальной сети, компьютеры которого могут получать доступ к открытым ресурсам Интернет.*** *Весь потенциально опасный открытый трафик из Интернет зашифровывается на Координаторе "D" и может быть расшифрован только на компьютерах локальной сети, включенных в этот виртуальный контур. Любые стратегии атак извне не могут нанести вреда остальным ресурсам локальной сети. ПО . ViPNet[клиент] при работе станции в Интернет полностью блокирует любой иной трафик данной станции в локальной сети.*

# АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



Сократ, мудрец

# ЧТО ЭТО ТАКОЕ?

**Аудит информационной безопасности** — системный процесс получения объективных качественных и количественных оценок текущего состояния информационной безопасности предприятия в соответствии с определенными критериями и показателями безопасности

# БЫЛО БЫ ЗДОРОВО, ЕСЛИ БЫ У ВАС БЫЛО…

Независимая оценка текущего состояния ИБ

Анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов ИС

Постоянная идентификация и ликвидация уязвимостей

Технико-экономическое обоснование механизмов ИБ

Обеспечение требованиям внутренних, отраслевых регламентов и действующего законодательства РФ

Управляемая минимизация ущерба от инцидентов безопасности

# ПОДХОДЫ К ПРОВЕДЕНИЮ АУДИТА ИБ


Использование стандартов ИБ

Использование методологии анализа рисков

Комбинирование анализа рисков и стандартов для определения критериев проведения аудита ИБ

Комбинирование активного и экспертного аудитов ИБ

# ОБЛАСТИ ПРОВЕДЕНИЯ ЭКСПЕРТНОГО АУДИТА

# ОБЛАСТИ ПРОВЕДЕНИЯ АКТИВНОГО АУДИТА

# ЭТАПЫ ПРОВЕДЕНИЯ АУДИТА ИБ

Подготовка к проведению аудита ИБ

Анализ внутренних документов

Проведение аудита ИБ на месте

Подготовка, утверждение отчета по аудиту ИБ
включающего рекомендации и технико-экономическое обоснование

Завершение аудита ИБ

# ПРИМЕНЯЕМЫЕ СТАНДАРТЫ И МЕТОДОЛОГИИ ПРИ ПРОВЕДЕНИИ АУДИТА ИБ

1. ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.»
2. **ГОСТ Р ИСО/МЭК 27001** «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.»
3. ГОСТ Р ИСО/МЭК 27005 «Информационные технологии. Методы обеспечения безопасности. Управление рисками информационной безопасности.»
4. ГОСТ Р ИСО/МЭК 27006 «Информационные технологии. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью»
5. ГОСТ Р ИСО/МЭК 13335 «Информационная технология. Методы и средства обеспечения безопасности»
6. ГОСТ Р ИСО/МЭК 15026 «Информационная технология. Уровни целостности систем и программных средств»
7. ГОСТ Р ИСО/МЭК ТО 18044 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности»
8. ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий»
9. ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования»

# ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ

## Внутренний тест на проникновение

Сбор информации о доступных ресурсах сети (сетевых сервисах, операционных системах и приложениях) и определение мест возможного хранения/обработки критичных данных

Попытки получения учетных записей и паролей пользователей и администраторов информационных систем путём перехвата сетевого трафика

Поиск уязвимостей ресурсов, способных привести к возможности осуществления несанкционированных воздействий на них

Разработка векторов атак и методов получения несанкционированного доступа к критичным данным

Попытки получения несанкционированного доступа к серверам, базам данных, компьютерам пользователей с использованием уязвимостей программного обеспечения, сетевого оборудования, некорректных настроек

# ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ

## Внешний тест на проникновение

Сбор общедоступной информации о Заказчике с помощью поисковых систем, через регистрационные базы данных (регистраторы имен и адресов, DNS, Whois и т.п.) и других публичных источников информации

Сбор информации о доступных из сетей общего доступа ресурсах (сетевых сервисах, операционных системах и приложениях)

Определение мест возможного хранения/обработки критичных данных, доступных извне

Сбор публично доступной информации о сотрудниках Заказчика (корпоративные электронные адреса, посещение веб-сайтов, Интернет форумов, социальные сети, личная информации о человеке)

Поиск уязвимостей в веб-приложениях Заказчика, эксплуатация которых может привести к неавторизированному доступу к критичным данным

Выявление уязвимостей ресурсов внешнего сетевого периметра, эксплуатация которых может привести к компрометации ресурса и/или использована для получения неавторизованного доступа к критичным данным

Разработка векторов и методов проникновения

# РЕЗУЛЬТАТЫ ПРОВЕДЕНИЯ АУДИТА ИБ

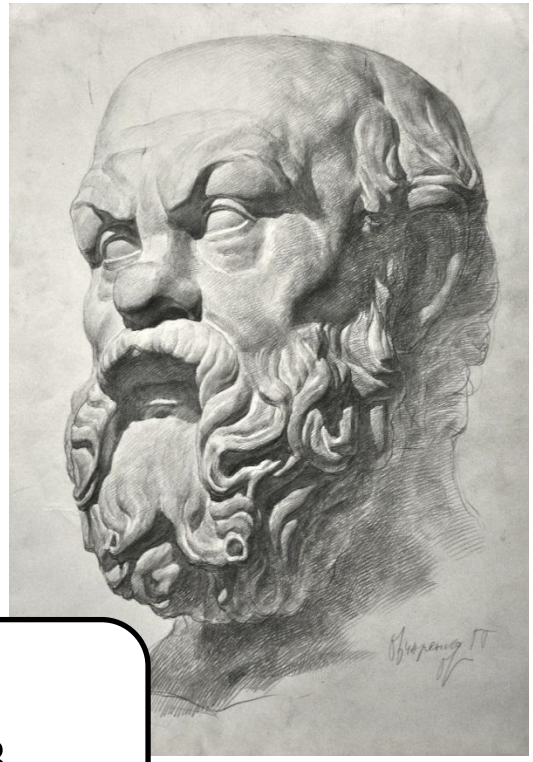
Лучшее понимание руководством и сотрудниками целей, задач, проблем организации в области ИБ

Осознание ценности информационных ресурсов

Надлежащее документирование процедур и моделей ИС с позиции ИБ

Принятие ответственности за остаточные риски

# РАССЛЕДОВАНИЕ КИБЕРИНЦИДЕНТОВ



Сократ, мудрец

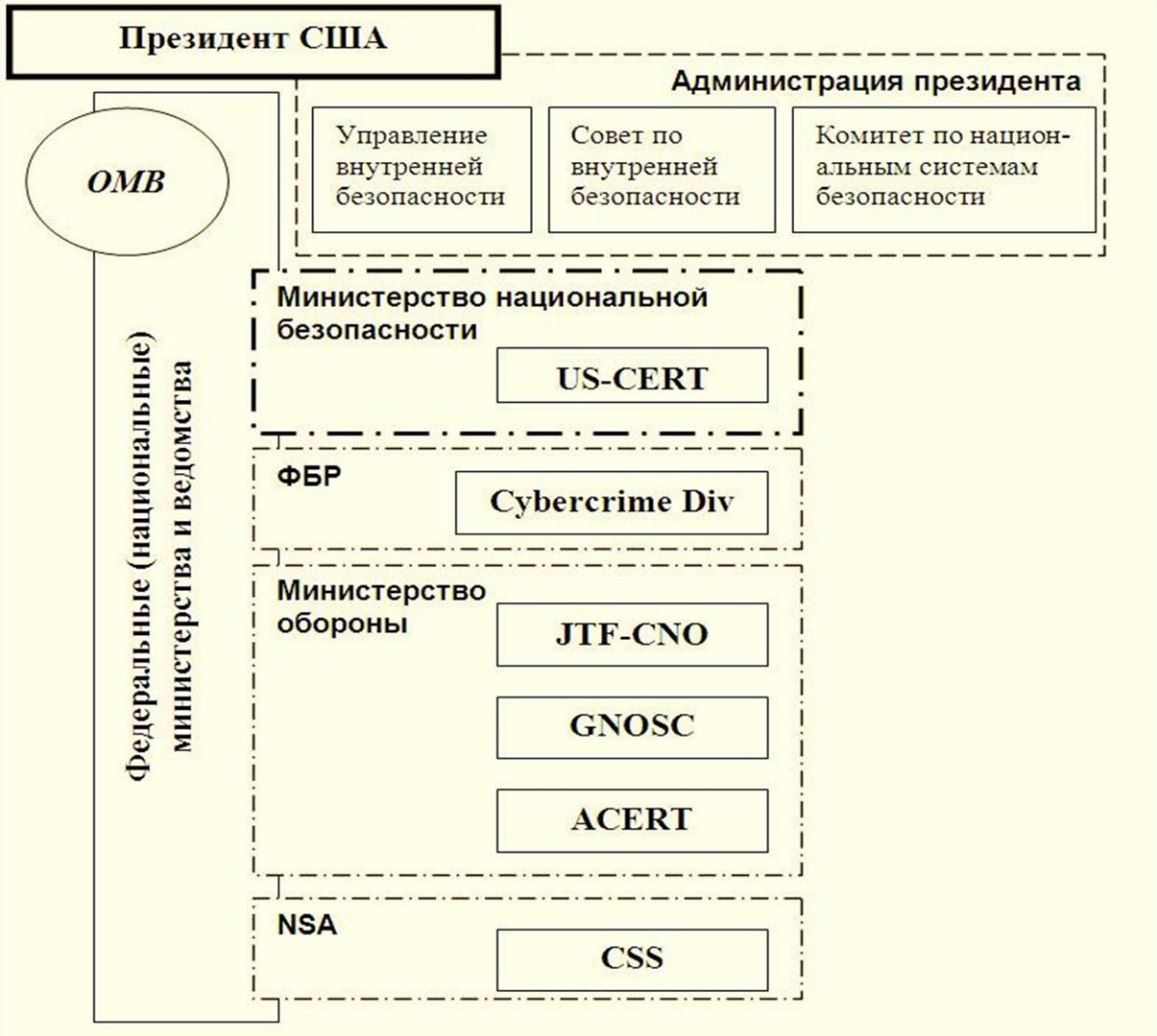
# ОСНОВНЫЕ ПОНЯТИЯ

**ИНЦИДЕНТ (ИЛИ ИНЦИДЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ)** — системное событие, в рамках которого произошло нарушение политики безопасности (в соответствии с определением из документа RFC 2828).

**РЕАГИРОВАНИЕ НА ИНЦИДЕНТ** — совокупность действий, направленных на выявление компьютерной информации, имеющей отношение к инциденту, и сохранение ее целостности и юридической значимости, а также на сбор иных сведений, имеющих отношение к инциденту.

**РАССЛЕДОВАНИЕ ИНЦИДЕНТА** — исследование компьютерной информации и иных сведений с целью установления обстоятельств инцидента (характера, временной шкалы и других фактов) и выявления причастных лиц.

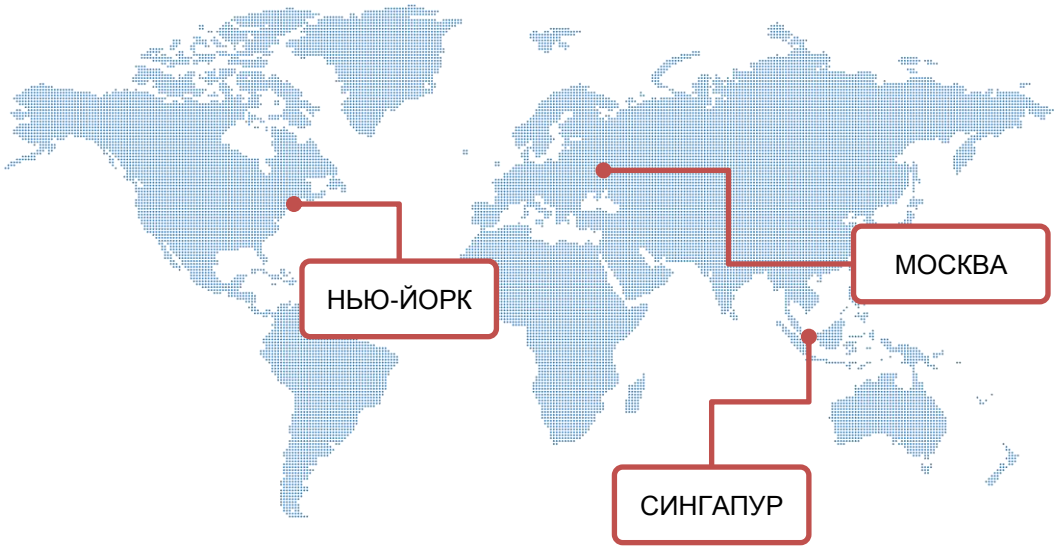
# СИСТЕМА РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИБ В США




**Структура органов государственной власти, обеспечивающих информационную безопасность в США**

# СИСТЕМА РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИБ В РОССИИ

**CERT-GIB**
**центр реагирования на инциденты информационной безопасности**




1

→ **Первый 24/7 CERT в Восточной Европе**

CERT-GIB первый в Восточной Европе круглосуточный центр реагирования на инциденты информационной безопасности

2

→ **Трансконтинентальная поддержка**

Группы мониторинга и реагирования присутствуют в разных частях земного шара: **Северная Америка → Европа → Азия**

3

→ **Противодействие следующим типам угроз:**

Фишинг, спам, DDoS-атаки, вредоносное ПО, бот-сети

4

→ **.RU, .РФ, .SU: компетентная организация по противодействию киберугрозам**

Обладает статусом экспертной организации Координационного центра национального домена сети Интернет в Рунете

# CERT-GIB МЕТОДОЛОГИЯ РАБОТЫ

1

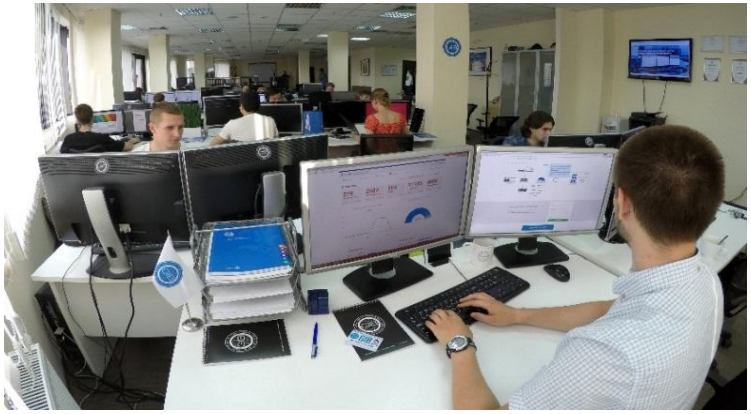
## →Активный мониторинг

- Мониторинг инцидентов информационной безопасности: фишинг, спам-сообщения, вредоносное ПО и т. д.
- Прием заявок с помощью формы на сайте, e-mail, «горячей линии»
- Мониторинг профессиональных сообществ

2

## →Сбор информации об инциденте

- Определение источника угрозы
- Анализ угрозы
- Установление лиц, причастных к угрозе
- Проведение криминалистической экспертизы




3

## →Классификация инцидента

- Фишинг
- Вредоносное ПО
- Распространение конфиденциальной информации
- DoS/DDoS-атака
- Спам
- Иные угрозы

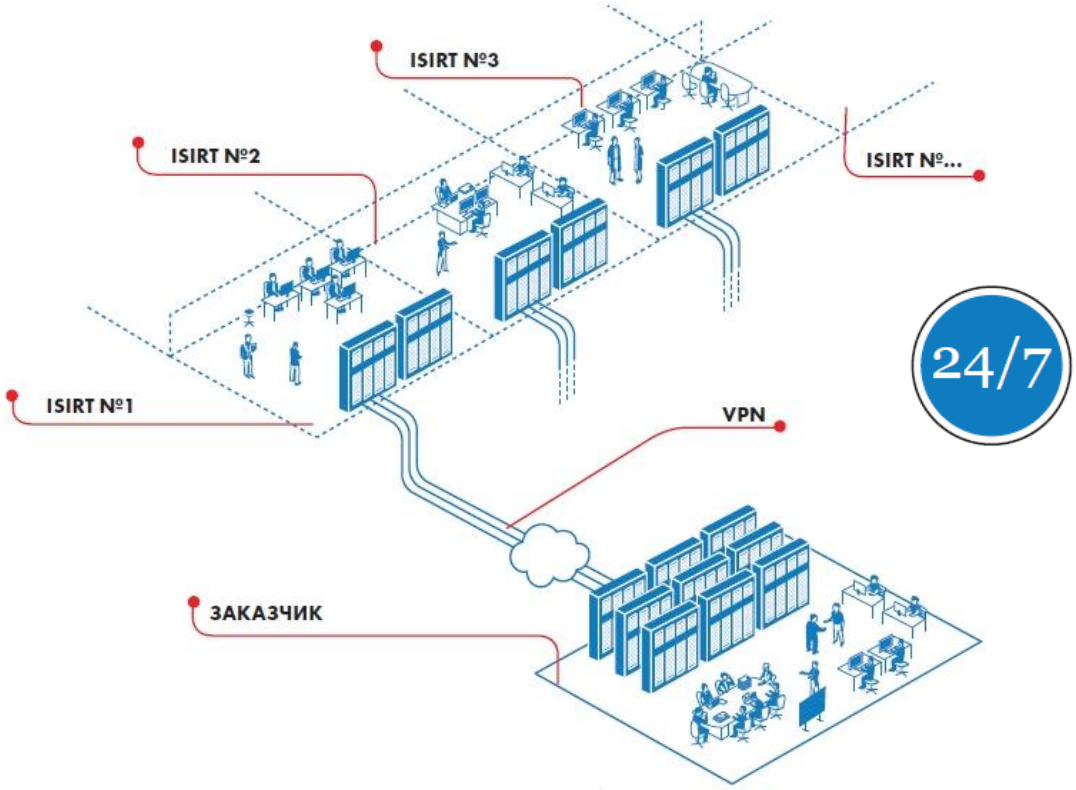
4

## →Нейтрализация инцидента

- Устранение причин возникновения инцидента
- Привлечение зарубежных CERT/CSIRT к сотрудничеству (при необходимости)
- Предоставление отчета обратившейся стороне
- Передача материалов в правоохранительные органы (при необходимости)

# СТРУКТУРА CERT-GIB

Команды Group-IB по мониторингу и реагированию на инциденты информационной безопасности




1

→ **Мониторинг** событий информационной безопасности

2

→ **Немедленное реагирование** на инциденты информационной безопасности

3

→ **Сбор, исследование и обработка** цифровых доказательств и журналов событий

4

→ **Проведение** внешних и внутренних расследований

5

→ **Юридическое сопровождение** всего комплекса мероприятий и их результатов

# ПРИЗНАКИ ИНЦИДЕНТА В СИСТЕМЕ ДБО

- **Обнаружение платежных поручений, которые не передавались уполномоченными работниками организации.**

- **Сообщение из банка, содержащее требование подтвердить исполнение платежных поручений, которые не передавались уполномоченными работниками организации.**

- **Уменьшение или отсутствие денежных средств на счете при условии, что передача денежных средств не проводилась.**

- **Невозможность входа в систему ДБО из-за ошибок, достоверно не связанных с техническими проблемами на стороне банка (ошибки аутентификации, возникающие при корректном вводе логина и пароля, недоступность серверов системы ДБО и т. п.).**

- **Невозможность загрузки операционной системы ЭВМ, на которой работали с системой ДБО.**

# ТЕХНИЧЕСКИЕ МЕРОПРИЯТИЯ

1. **Выявление всех ЭВМ организации, на которых работали с системой ДБО. Составление их списка (в том числе ЭВМ, которые на момент инцидента были выключены).**
2. **Немедленное выключение работающих ЭВМ из указанного списка методом прерывания электропитания (отключение шнура от блока питания компьютера, снятие аккумуляторной батареи) либо иным методом, обеспечивающим выключение без применения программных средств.**
3. **Извлечение энергонезависимых носителей информации (НЖМД, флеш-накопители) из ЭВМ, на которых работали с системой ДБО.**
4. **Упаковка и опечатывание извлеченных носителей информации**
5. **Упаковка и опечатывание носителей ключевой информации (флеш-накопителей, аппаратных ключей), используемых для подписи платежных поручений.**
6. **Включение ЭВМ, на которых работали с системой ДБО, без подключения загрузочных носителей информации с целью определения (с помощью интерфейса базовой системы ввода и вывода) и документирования отклонения системных часов компьютера от текущего времени (необязательный шаг).**
7. **Копирование журналов систем контроля доступа в помещения организации, копирование видеопотока систем видеонаблюдения в офисе или офисном центре за максимально возможный промежуток времени. Запись соответствующих журналов и видеопотоков на компакт-диски, их упаковка и опечатывание.**
8. **Составление соответствующего акта, в котором отражаются характеристики упакованных и опечатанных носителей и иная значимая информация (пример акта приведен в приложениях).**
9. **Передача упакованных и опечатанных носителей информации на хранение в специальном помещении или сейфе.**

# ОРГАНИЗАЦИОННЫЕ МЕРОПРИЯТИЯ

1. **Немедленно сообщить по телефону в подразделение информационной безопасности банка о факте несанкционированной передачи платежных поручений с указанием их реквизитов: номеров, сумм, получателей, назначений платежей. Потребовать отмены указанных платежных поручений и аннулирования действующего сертификата ключа электронной подписи организации.**

2. **Оформить докладную записку руководителю организации о факте инцидента с указанием реквизитов переданных платежных поручений (пример докладной записки приведен в приложениях).**

3. **Подготовить документы для правоохранительных органов и работников банка (описание инцидента в письменной форме, договор на предоставление услуги ДБО, договор на предоставление услуги доступа в сеть Интернет, копии несанкционированных платежных поручений, заявление о преступлении). Заявление о преступлении оформляется с учетом требований статьи 141 Уголовно-процессуального кодекса РФ и передается в орган МВД России для регистрации1 и последующей проверки**

***Если заявление о преступлении передается при личном обращении заявителя, то ему выдается талон-уведомление (пункт 68 приложения к приказу МВД России от 01.03.2012 №140).***

# ОШИБКИ ПРИ РЕАГИРОВАНИИ НА ИНЦИДЕНТ В СИСТЕМЕ ДБО

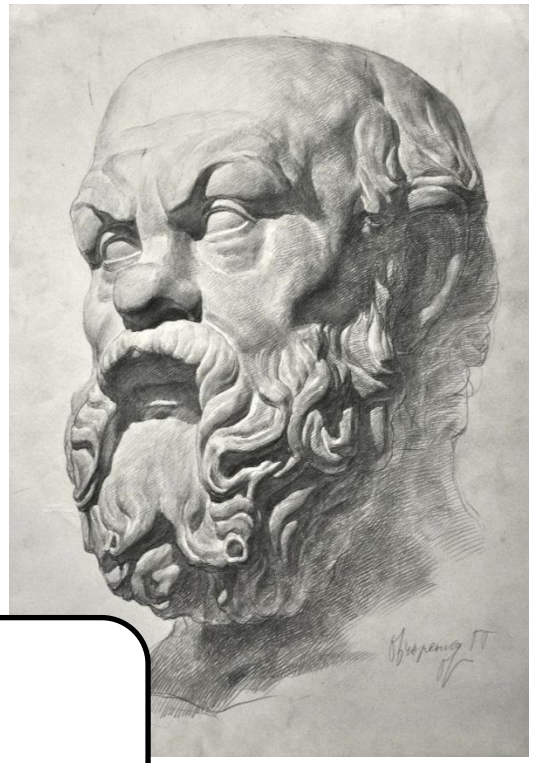
- **Антивирусная проверка файловых систем носителей информации ЭВМ, на которых работали в системе ДБО, после обнаружения инцидента (приводит к изменению временных меток файлов вредоносных программ, перемещению или удалению файлов вредоносных программ).**

- **Переустановка операционных систем ЭВМ, на которых работали в системе ДБО, после обнаружения признаков инцидента (приводит к удалению файлов вредоносных программ, следов их работы и усложняет расследование инцидента за счет необходимости восстановления данных).**

- **Продолжение работы пользователей с ЭВМ, имеющими отношение к инциденту, после обнаружения инцидента; необоснованный перенос выключения ЭВМ на более поздний срок (дает возможность злоумышленнику удалить следы собственной активности).**

- **Несвоевременное информирование подразделения информационной безопасности банка о факте несанкционированной передачи платежных поручений (приводит к исполнению платежных поручений, переданных злоумышленником, а также к возможности передачи новых платежных поручений с помощью скопированных злоумышленником ключей электронной подписи).**

- **Необоснованное отклонение от рекомендуемой последовательности действий, медленное реагирование на инцидент (приводит к снижению юридической значимости собираемых материалов, перезаписи криминалистически значимых данных).**



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)

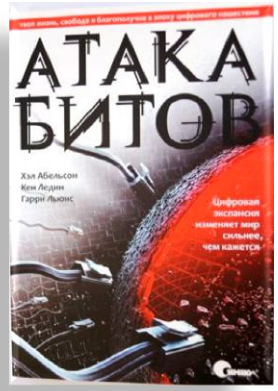
**Дополнительная литература**

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