Национальный исследовательский университет
«Высшая школа экономики»

Институт проблем безопасности

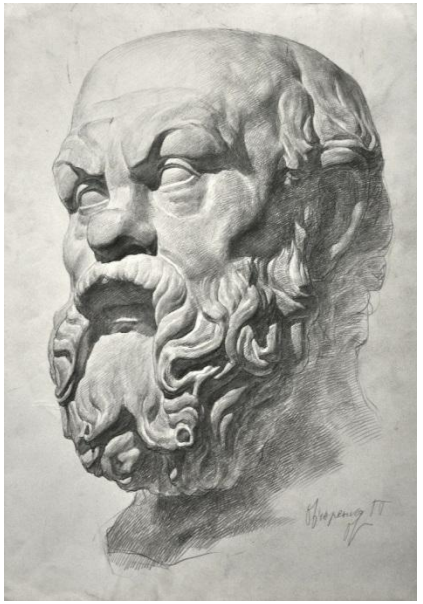
2015/2016-2016/2017 гг.

**760 часов**

**майнор**

# Безопасность предпринимательской деятельности

**Безопасность предпринимательской деятельности**

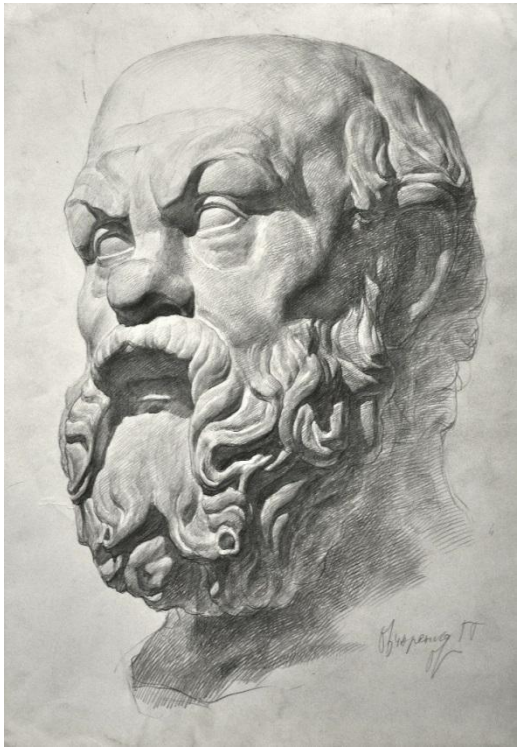


1-й и 2-й модули 2016/2017 учебного года:
сентябрь, октябрь, ноябрь, декабрь
190 академических часов

**Дисциплина № 3**

# Комплексное противодействие атакам на информационные и материальные ресурсы бизнеса

Комплексное противодействие атакам на информационные и материальные ресурсы бизнеса



Сократ, мудрец

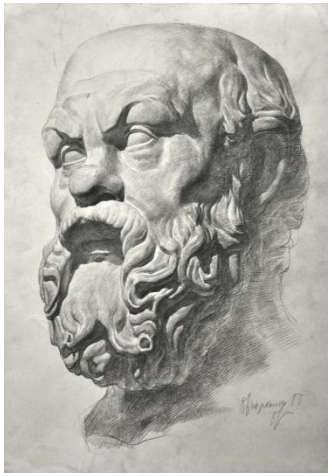
Тема № 5

# Типовые угрозы кибернетической безопасности предприятия

Лекция, 2 часа

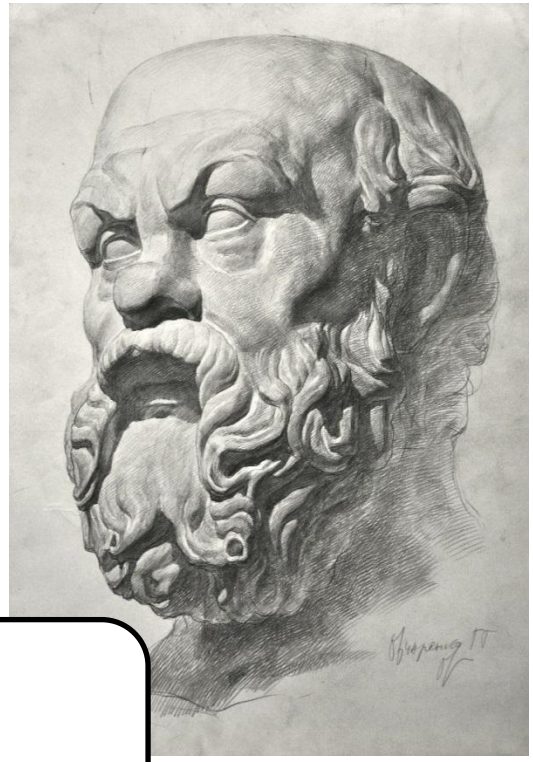
Информационная безопасность

## Оглавление




1. Что такое кибернетические угрозы
2. Основные виды кибератак
3. Причины изменения ландшафта киберугроз
4. Кибератаки на объекты критически важной инфраструктуры
5. Библиография

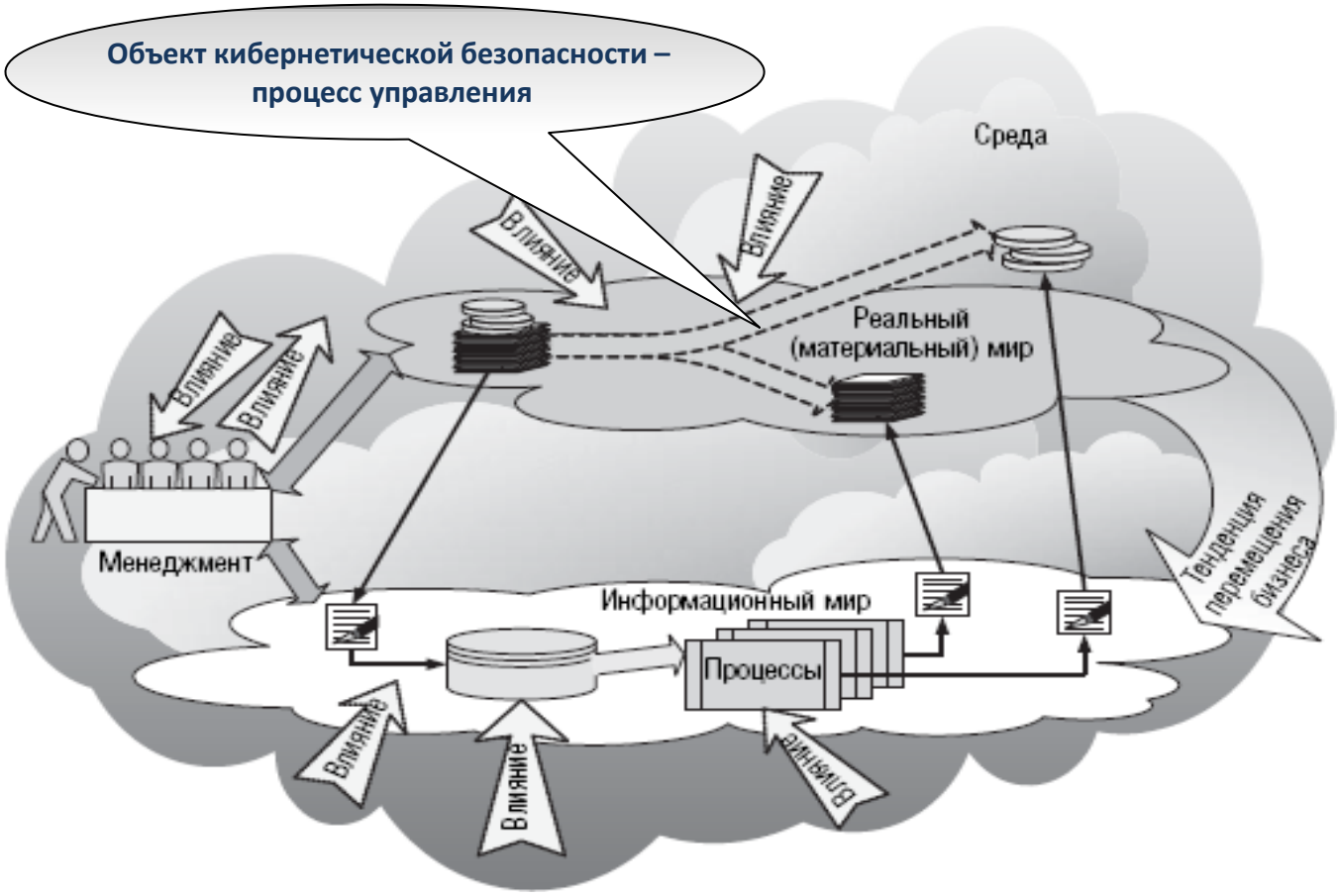
# Мировые информационные ресурсы



Сократ, мудрец

# КИБЕРНЕТИЧЕСКИЕ УГРОЗЫ

***явления, деяния, условия, факторы, представляющие опасность для информации управления, инфраструктуры управления, субъектов управления и порядка управления.***




**Деформация бизнеса через инциденты в информационной сфере**

# ПОНЯТИЕ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ

# ЧТО ТАКОЕ КИБЕРНЕТИЧЕСКИЕ УГРОЗЫ?

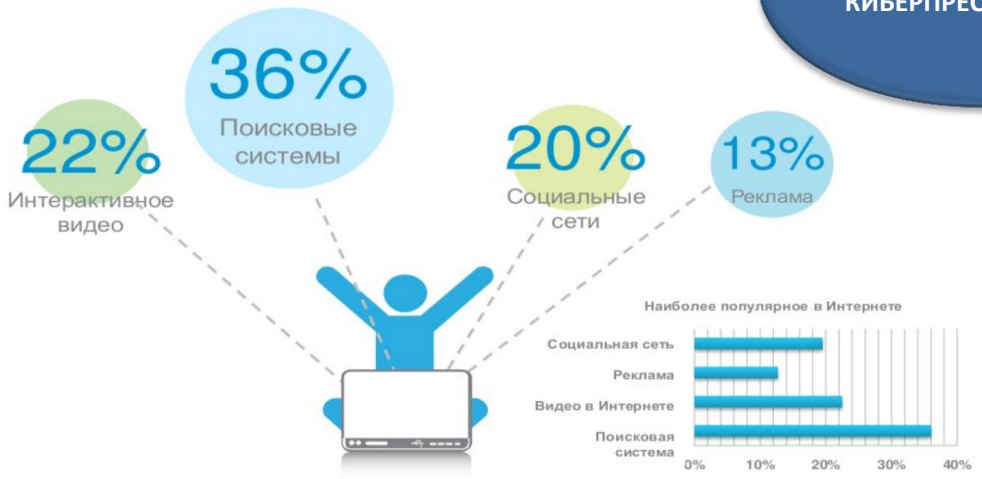
**ОБЪЕКТ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ – ПРОЦЕСС УПРАВЛЕНИЯ**

***Кибернетические угрозы*** **– явления, деяния, условия, факторы, представляющие опасность для информации управления, инфраструктуры управления, субъектов управления и порядка управления.**

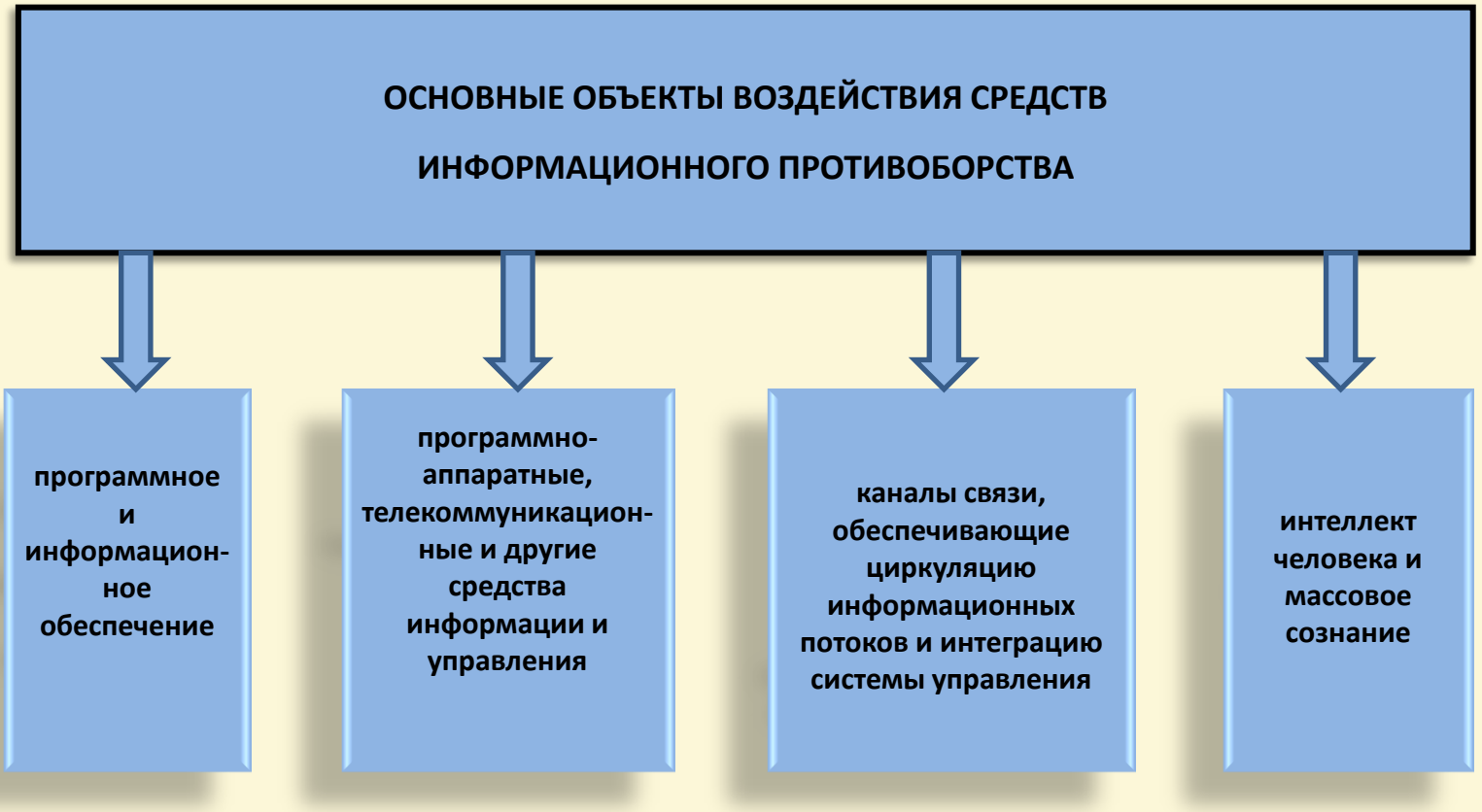
***Опасность*** **заключается в возможности нарушения свойств одного, либо нескольких указанных элементов, что может привести к нарушению управления.**

# АКТУАЛЬНЫЕ ТИПЫ КИБЕРУГРОЗ


*По материалам А. Лукацкого*




# ОСНОВНЫЕ ОБЪЕКТЫ КИБЕРУГРОЗ



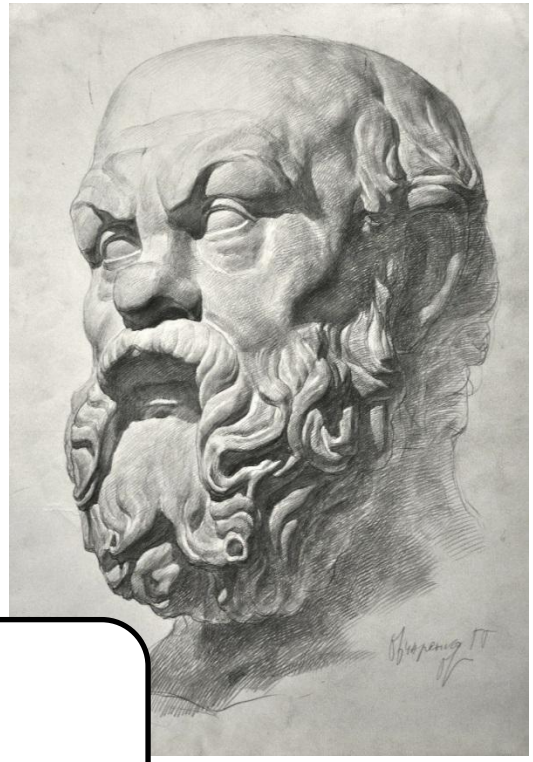
# ПОЧЕМУ ЭТО ТАК ВСЕ ВОЛНУЕТ?

- ✓ **отсутствие международно-правовой основы запрещающей применение информационного оружия и проведение информационных операций;**
- ✓ **несовершенство нормативной правовой основы устанавливающей ответственность за совершение преступлений в сфере информационных технологий;**
- ✓ **разработка отдельными государствами доктрин и стратегий наступательных и подрывных действий в информационном пространстве;**
- ✓ **интенсивное развитие военных информационных технологий, в том числе средств поражения систем управления гражданского и военного назначения;**
- ✓ **нивелирование роли международных организаций и их органов, в области обеспечения международной информационной безопасности;**

# ПОЧЕМУ ЭТО ТАК ВСЕ ВОЛНУЕТ?

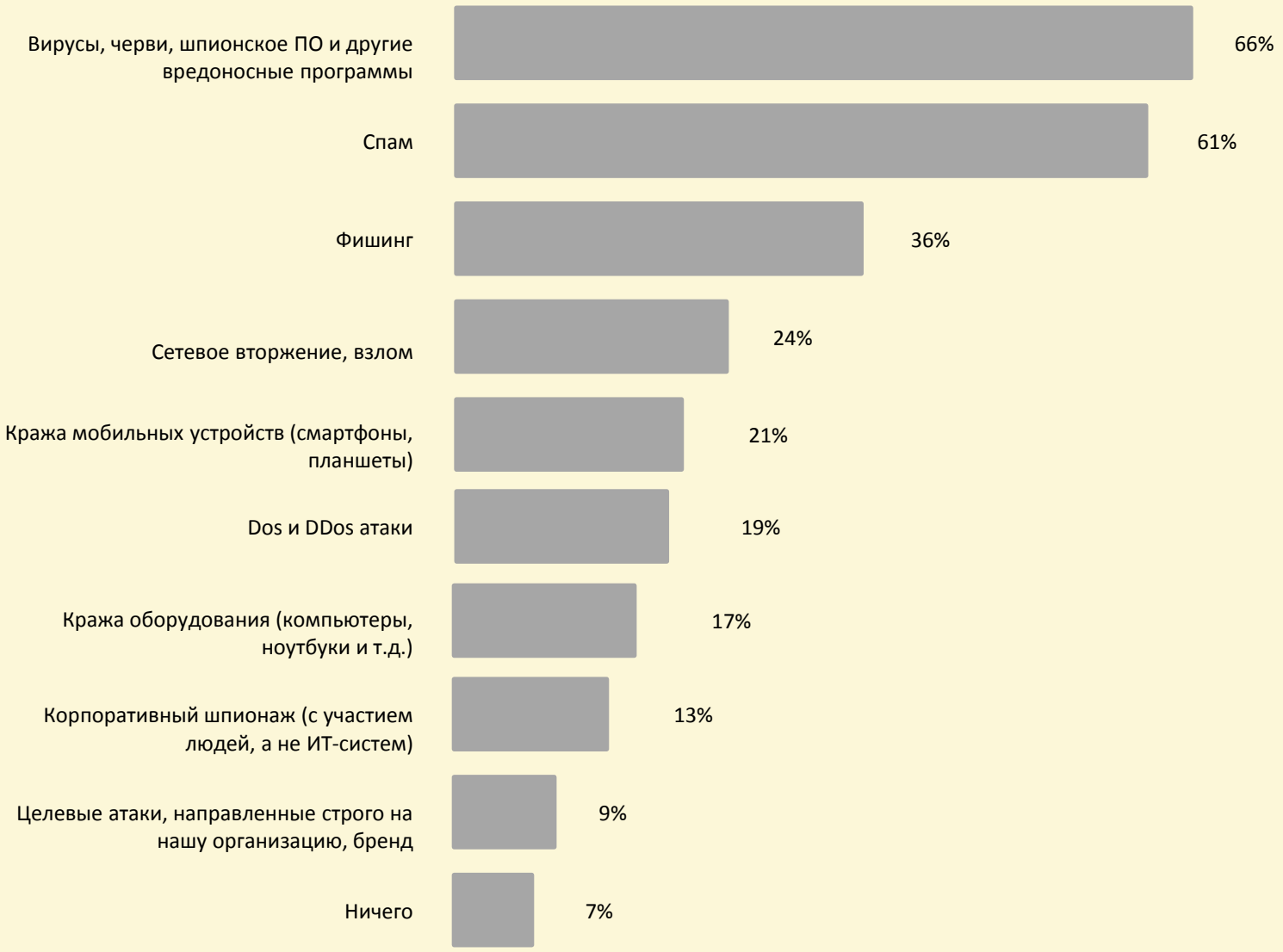
- ✓ **создание и применение специальных сил и средств негативного воздействия на информационную инфраструктуру;**
- ✓ **существование специальных образцов вредоносного программного обеспечения поражающего автоматизированные системы управления промышленных и других объектов критически важной инфраструктуры;**
- ✓ **появление форм гражданского неповиновения связанных с посягательствами на информационную инфраструктуру в знак протеста против политики государства и деятельности органов власти;**
- ✓ **проникновение информационных технологий во все сферы государственной и общественной жизни, построение на их основе систем государственного и военного управления;**
- ✓ **развитие государственных проектов и программ в сфере информатизации (электронный документооборот, межведомственное электронное взаимодействие, универсальные электронные карты, предоставление государственных услуг в электронной форме) направленных на формирование информационного общества**

# Основные виды кибератак



Сократ, мудрец

# ОСНОВНЫЕ ВИДЫ КИБЕРНЕТИЧЕСКИХ АТАК НА КОРПОРАТИВНОМ УРОВНЕ



# МАСШТАБ УГРОЗ

**1994**
**1**
НОВЫЙ ВИРУС КАЖДЫЙ ЧАС

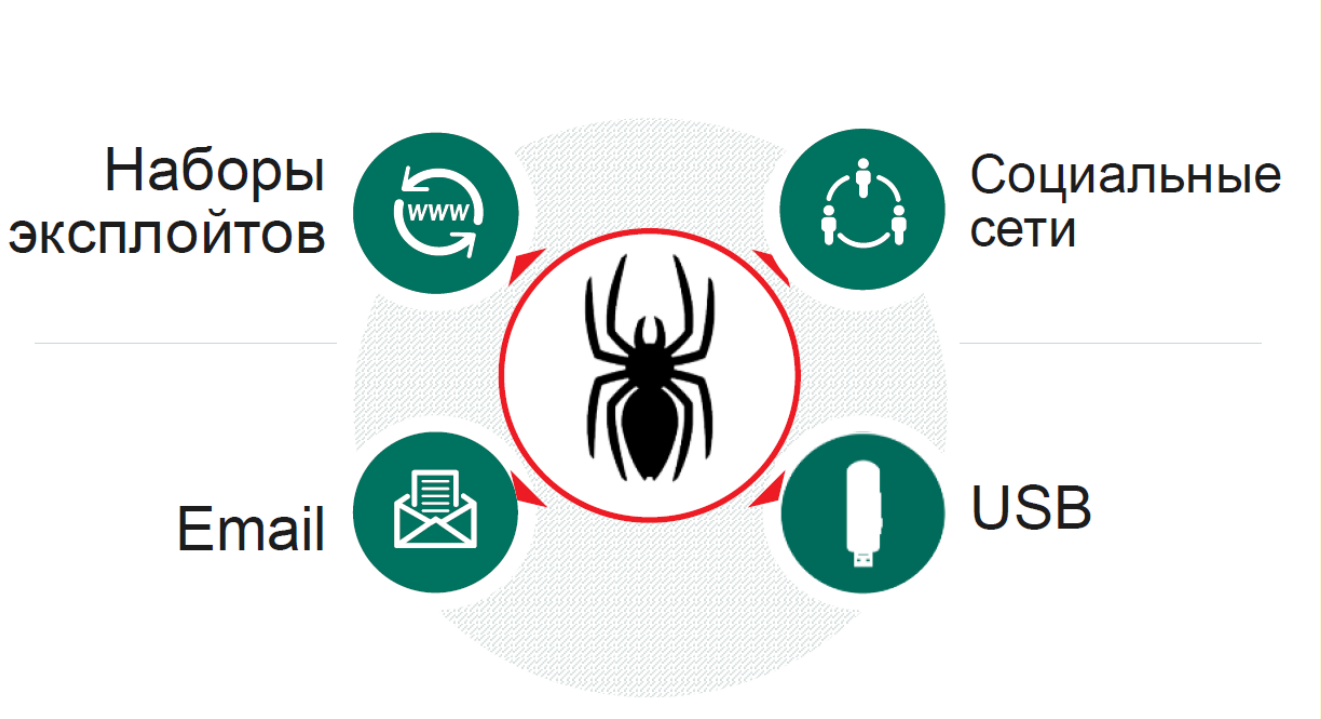
**2006**
**1**
НОВЫЙ ВИРУС КАЖДУЮ МИНУТУ

**2011**
**1**
НОВЫЙ ВИРУС КАЖДУЮ СЕКУНДУ

**2014**
**325 000**
НОВЫХ ВРЕДОНОСНЫХ ОБРАЗЦОВ В ДЕНЬ

*по данным лаборатории Касперского*

# КАК РАСПРОСТРАНЯЮТСЯ ВРЕДОНОСНЫЕ ПРОГРАММЫ




*по данным лаборатории Касперского*

# ОСНОВНЫЕ ВИДЫ СЕТЕВЫХ АТАК

***Почтовая бомбардировка***
***Атаки с подбором пароля***
***Вирусы, почтовые черви и "троянские кони"***

***Сетевая разведка***
Производится сканирование портов, запросы DNS, эхо-тестирование раскрытых с помощью DNS адресов и т. д

***Сниффинг пакетов***
Сниффер перехватывает все сетевые пакеты, которые передаются через атакуемый домен.

***IP-спуфинг*** - вид атаки, при которой хакер внутри организации или за ее пределами выдает себя за санкционированного пользователя.

***Атака на отказ в обслуживании***
*Основная защита:* трафик, предназначенный для переполнения атакуемой сети, необходимо "отсекать" у провайдера услуг Интернет.
Когда атака этого типа проводится одновременно через множество устройств, говорится о **распределенной атаке** DoS (Distributed Denial of Service — DDoS).

***Атаки типа Man-in-the-Middle***

***Использование "дыр" и "багов" в ПО***

# ОСНОВНАЯ СХЕМА КИБЕРАТАК С ИСПОЛЬЗОВАНИЕМ ИНТЕРНЕТ БАНК-КЛИЕНТОВ

1. **Хаотичное заражение большого количества ПК вредоносным программным обеспечением, использую незакрытые уязвимости в браузерах или др. прикладном ПО (часто используются незакрытые дыры в ПО Adobe, Microsoft, Mozilla и др.)**

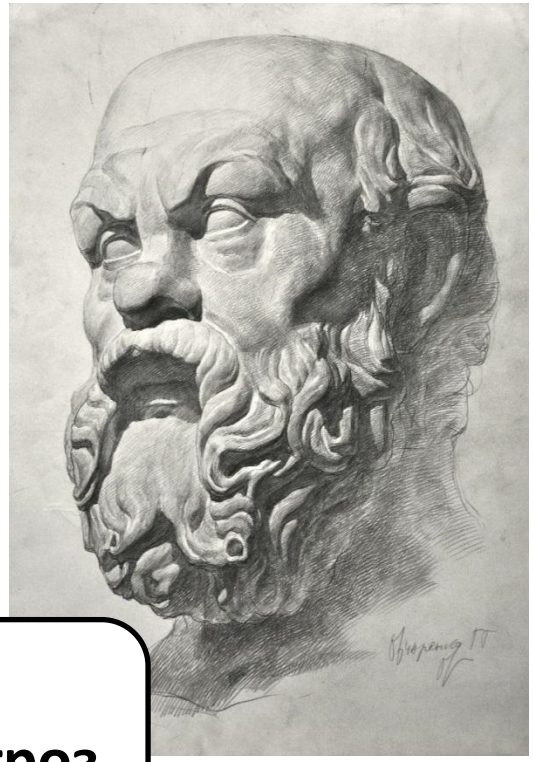
2. **Если в список зараженных ПК попадает машина, с которой осуществляются банковские операции, данный факт регистрируется, и на нее закачиваются дополнительные модули, необходимые для кражи электронных ключей и аутентификационной информации. Часто применяются различные кейлоггеры, средства удаленного управления (Teamviewer, VNC, Remote Admin), вредоносные модули, предназначенные специально для извлечения ключей из реестра и внешних носителей.**

3. **Как только необходимая информация собирается, она передается злоумышленникам, которые проверяют возможность авторизации и проведения платежных поручений.**

4. **Как только вся необходимая информация для проведения мошенничества готова, злоумышленники прилагают усилия для того, чтобы скрыть следы преступления от жертвы. Применяются различные методы, начиная от нарушения функционирования ПК, с которого были похищены ключи, заканчивая DDoS-атаками на сервер банк-клиента. Цель данных действий – максимально отсрочить момент обнаружения факта преступления, чтобы деньги успели перевестись на подставные фирмы.**

5. **Деньги выводятся через цепочку счетов подставных компаний или пластиковые карточки физических лиц. Наиболее часто обналичивание производится в районе Урала и Западной Сибири, регулярно мелькают такие города, как Екатеринбург, Челябинск и др.**

# Причины изменения ландшафта киберугроз



Сократ, мудрец

# ПРИЧИНЫ ПОЯВЛЕНИЯ НОВЫХ УГРОЗ

Мобильность

Совместная работа

Виртуализация и облака

**изменения среды ведения бизнеса**

# ЭВОЛЮЦИЯ КИБЕРУГРОЗ

# ЭВОЛЮЦИЯ ТАКТИКИ РЕАЛИЗАЦИИ КИБЕРУГРОЗ

# СМЕНА ЛАНДШАФТА КИБЕРУГРОЗ

# УГРОЗЫ СЕГОДНЯ

Устойчивые, сложные, мутирующие

Каждый экземпляр атаки может отличаться от другого

Домены меняются ежедневно, даже ежечасно

Контент мутирует и маскируется под легальный трафик

80% спама исходит от инцифицированных клиентов

70% «зомби» используют динамические IP-адреса

Угрозы из легальных доменов растут на сотни процентов в год

Спам составляет более 180 миллиардов сообщений в день

# ЗАЧЕМ ЭТО НАДО ЗЛОУМЫШЛЕННИКАМ?

# НЕУЖЕЛИ ЭТО ВЫГОДНО?

- Партнерская сеть по продаже scareware
- Партнеры загружают scareware на зараженные компьютеры и получают комиссию 60% с продаж
- Объем продаж за десять дней $147K (154 825 установки и 2 772 продажи)
- $5M в год

| Loader | Сетапы | Покупки | Покупки |
|---|---|---|---|
| 37943 | 19989 | 667 | 29853.86 |
| 39895 | 19722 | 74 | 5420.64 |
| 41687 | 18619 | 384 | 28148.96 |
| 38059 | 16038 | 249 | 13908.24 |
| 39160 | 15335 | 176 | 9726.17 |
| 29968 | 12076 | 207 | 11672.71 |
| 13293 | 6866 | 129 | 6920.81 |
| 18055 | 8915 | 157 | 7557.25 |
| 29642 | 14802 | 265 | 12852.29 |
| 50457 | 22463 | 464 | 21055.29 |
| 338159 | 154825 | 2772 | 147116.22 |
| Loads | Installs | Purchases | Total |

Статистика продаж Bakasoftware за 10 дней

# ДЕЯТЕЛЬНОСТЬ ЛИЦ ПО НАНЕСЕНИЮ УЩЕРБА КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ

**Популярный пример жизненного цикла киберпреступности**

1. Разработка и тестирование вредоносного кода
2. Вредоносный код объявляется к продаже
3. Вредоносный код размещается на различных сайтах
   - Сайты могут быть как специально подготовленные, так и общепопулярные, но взломанные
4. Вредоносный код загружается на компьютеры пользователей при посещении зараженных сайтов
   - В случае специально подготовленных сайтов используются партнерские схемы pay-per-install
5. Вредоносный код собирает информацию для продажи (учетные записи, персональные данные, ключи электронной подписи и т.д.)
6. Собранная информация используется или продается

**Ключевые виды деятельности**

- Производство
- Разрешение проблем
- Платформы/сети

**Ключевые партнеры**

- Оптимизация и экономия в сфере производства
- Снижение риска и неопределенности
- Поставки ресурсов и совместная деятельность

- Типы партнеров
  - Abuse-хостеры
  - Гаранты
  - Владельцы ботнетов
  - Владельцы анонимных прокси
  - Владельцы Fast-Flux-хостинга
  - Продавцы трафика
  - И т.д.

**ПЕРСОНАЛ**

**У каждого своя роль**

- Менеджер по продажам
- Кассир
- Маркетолог
- Логист
- Водитель
- HR
- Генеральный директор
- Айтишник
- Охранник
- Инженер
- Разработчик
- Дроп (разводной / неразводной)
- Дроповод
- Обнальщик
- Заливщик / Даунлоадер
- Селлер
- Abuse-хостер
- Гарант
- Кодер

# МОТИВЫ КИБЕРПРЕСТУПЛЕНИЙ

## Деньги играют важную роль, но есть и другие мотивы

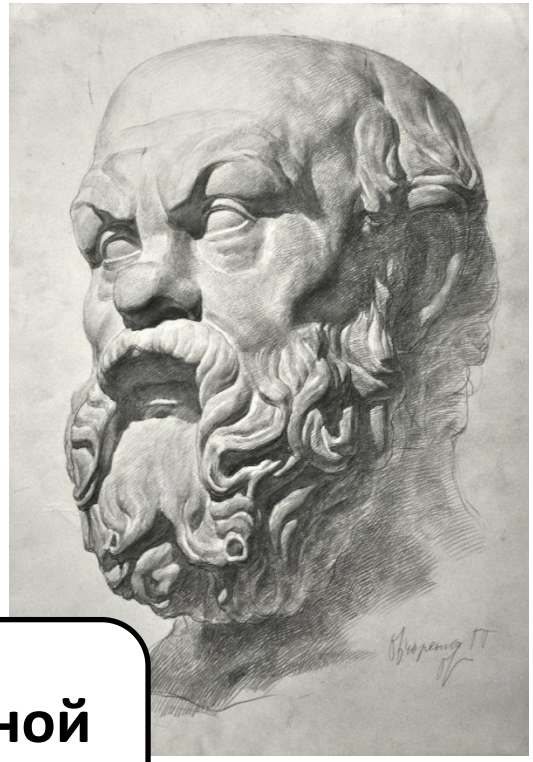
| | Кибер-террористы | Кибер-воины | Хактивисты | Писатели malware | Старая школа | Фрикеры | Самураи | Script kiddies | Warez D00dz |
|---|---|---|---|---|---|---|---|---|---|
| Сложность | | | | + | + | + | + | | + |
| Эго | | | | + | + | + | | | + |
| Шпионаж | | + | | + | | | | | |
| Идеология | + | + | + | | + | | | | + |
| Шалость | | | | + | | + | | + | |
| Деньги | | + | | + | | + | + | | + |
| Месть | + | | + | + | | | | + | |

Источник: Furnell, S. M

- Отсутствие желания заработать не означает отсутствие бизнес-модели киберпреступности

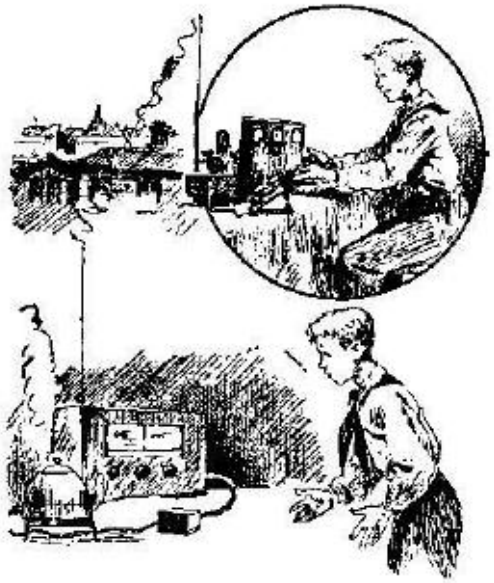
  Anonymous, Lulzsec демонстрируют это в полной мере

# Кибератаки на объекты критически важной инфраструктуры



Сократ, мудрец

# КИБЕРАТАКИ НА ОБЪЕКТЫ КРИТИЧЕСКИ ВАЖНОЙ ИНФРАСТРУКТУРЫ



*Можно по радио включать и выключать чайник. Но зачем это нужно?*

1956 год

1990 год

## ПРОБЛЕМЫ РЕАЛИЗАЦИИ МЕР КИБЕРБЕЗОПАСНОСТИ ДЛЯ АСУ ТП

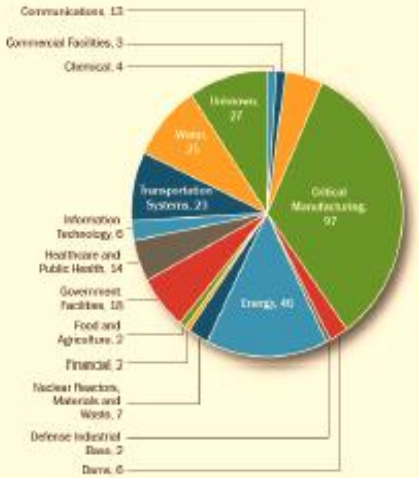
- **Защита от атак DoS и DDoS**
- **Плохая реализация сетевых протоколов в устройства АСУ ТП**
- **Не установленные обновления ОС и приложений**
- **Отсутствие антивирусов**
- **Плохая аутентификация и авторизация**
- **Плохой аудит и регистрация событий**
- **Не целевое использование ресурсов АСУ ТП**
- **Требования по удаленному доступу/интеграции**
- **Человеческий фактор**

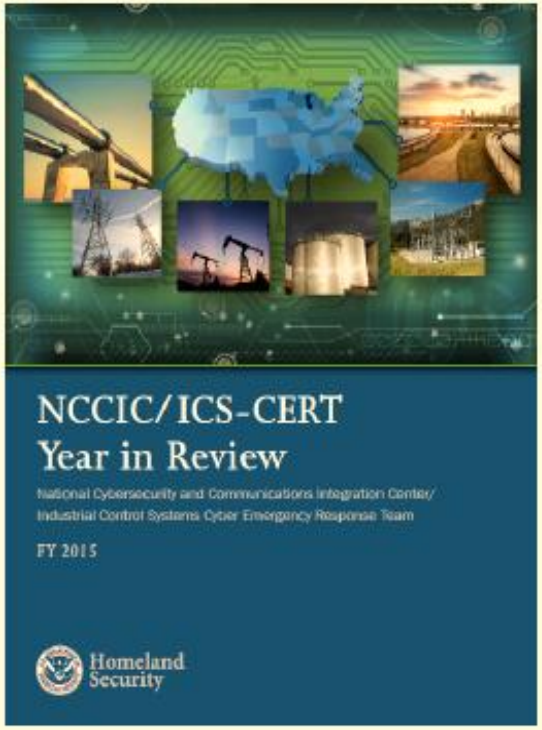
# КИБЕРАТАКИ НА ОБЪЕКТЫ КРИТИЧЕСКИ ВАЖНОЙ ИНФРАСТРУКТУРЫ

## Отчет ICS-CERT за 2015 год

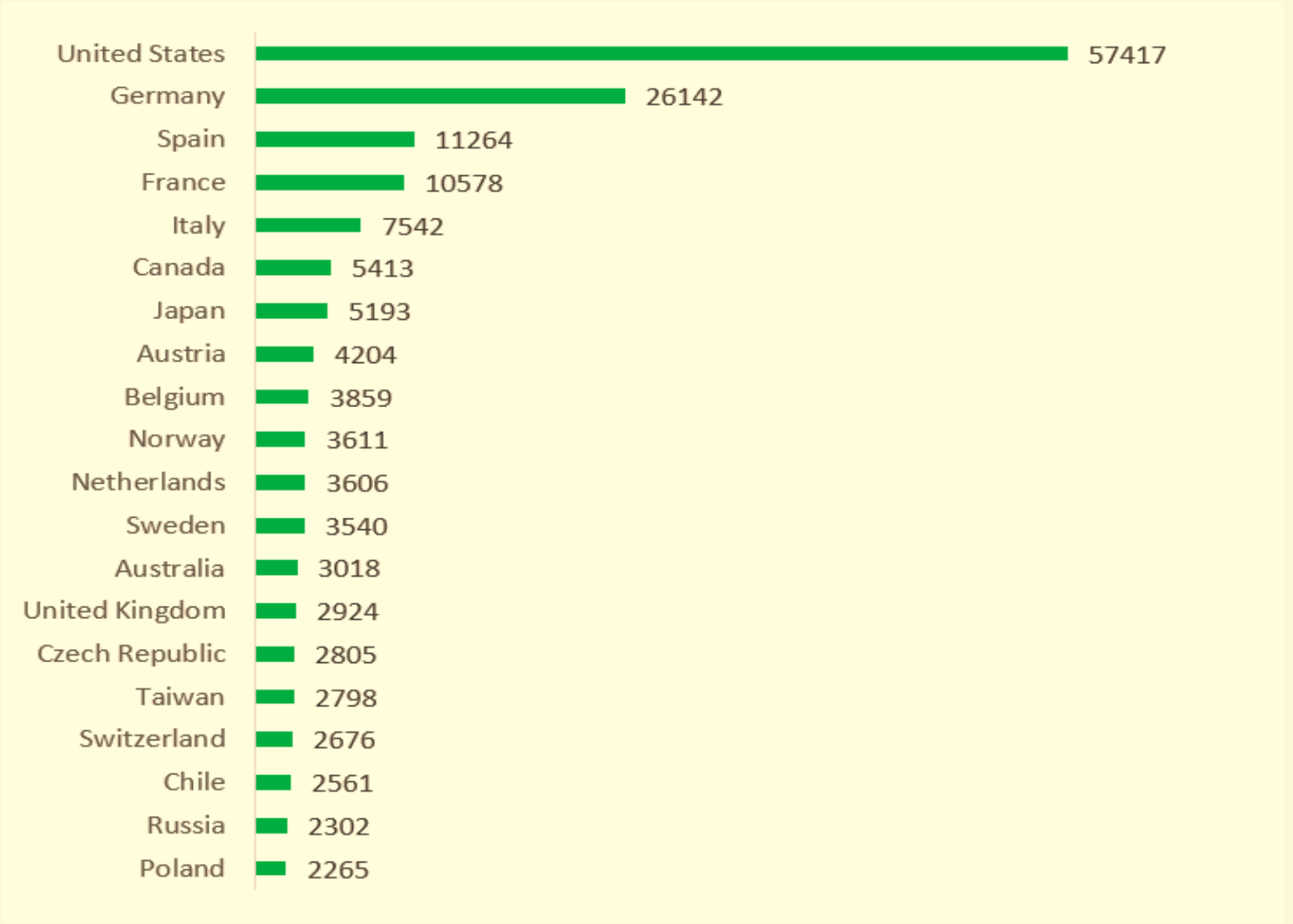
- 295 инцидентов (рост 20%)
- 486 уязвимостей
  - Снижение времени на устранение уязвимости с 108 до 55 дней

FY 2015 Incidents by Sector (295 total)

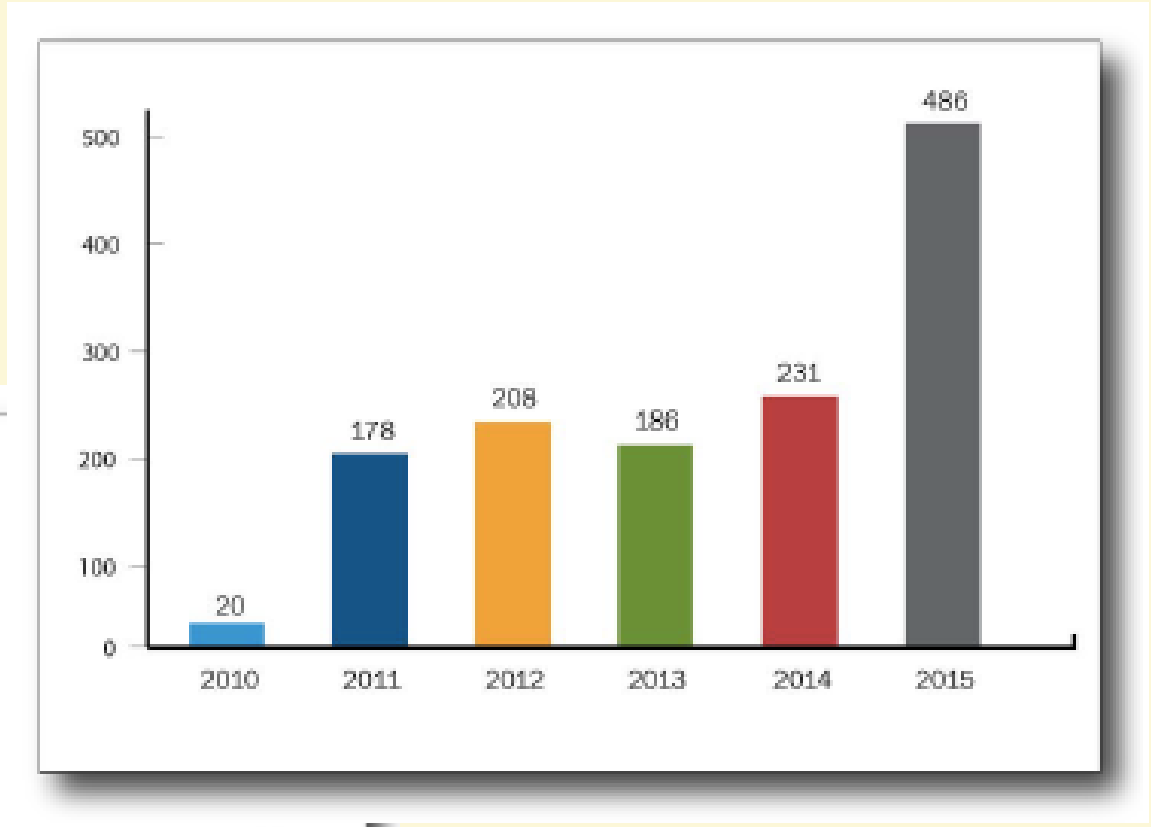


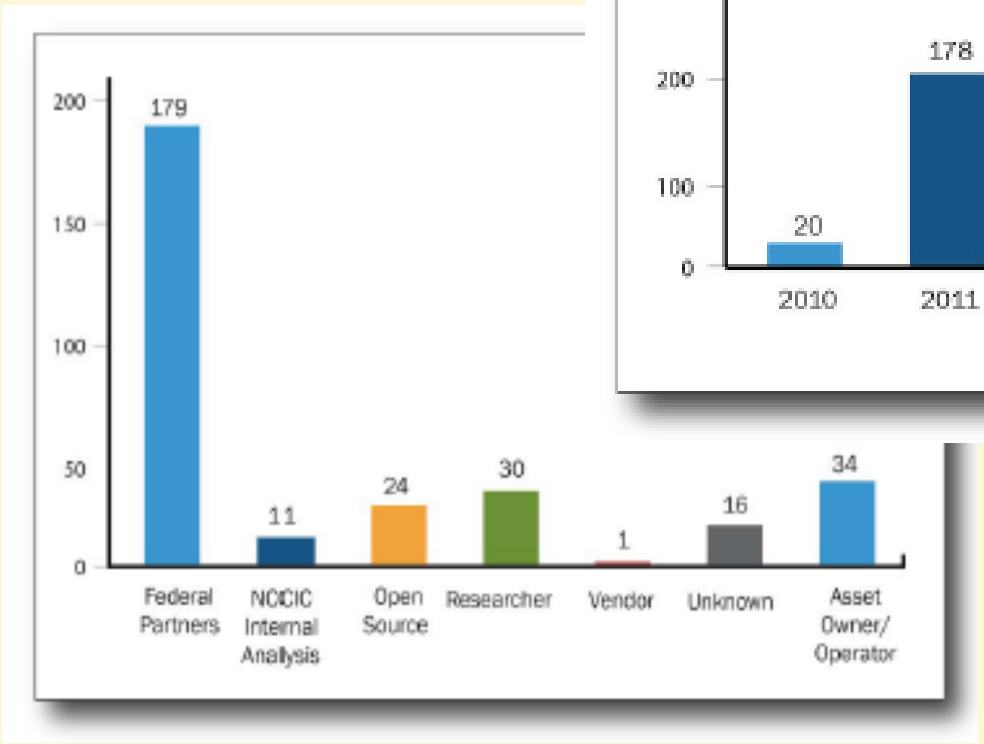



# РЕЙТИНГ 20 СТРАН С НАИБОЛЬШИМ ЧИСЛОМ АСУ, ДОСТУПНЫХ ЧЕРЕЗ ИНТЕРНЕТ



# РАСПРЕДЕЛЕНИЕ ИНЦИДЕНТОВ И УЯЗВИМОСТЕЙ



# ПОСЛЕДНИЕ ИНЦИДЕНТЫ ПО КИБЕРБЕЗОПАСНОСТИ

- Атака на АЭС в Японии в 2015-м году (стало известно только сейчас)
- Неправильное позиционирование зеркал на Ivanpah Solar Electric System привело к пожару (возможно ли сделать со злым умыслом?)
- Столкновение поездов в Казахстане и Баварии (киберпричина?)
- Атака на электроэнергетическую систему Украины с последующим обвинением России
- Атака на аэропорт «Борисполь»
- Обвинение иранцев в DDoS-атаке и взломе плотины около Нью-Йорка
- Регулярные демонстрации взломов автомобилей
- Атака на систему электроэнергетики Израиля

- Операция Dust Storm по атаке японских объектов ТЭК, транспорта, финансов и т.п.
- Создание первого червя для PLC Siemens, распространяемого без ПК
- Обнаружение на немецкой АЭС вируса
- Атака на ЖКХ-компанию Lansing Board of Water & Light в США
- Атака на CMS управления данными о содержимом и местонахождении кораблей (взлом пиратами контейнеров с бриллиантами)
- Атака на водоочистную систему Kemuri Water Company
- КНДР атаковало почтовые ящики сотрудников ж/д Южной Кореи
- Атаки на АСУЗ (СКУД) и медицинские системы/датчики

# ГЕОПОЛИТИКА И КИБЕРБЕЗОПАСНОСТЬ

# Кейс

## ВИРУС «Stuxnet»

**Вирус был разработан спецслужбами США и Израиля специально для атаки на ядерные объекты Ирана. Данный вирус, занесенный извне в изолированную от внешнего мира систему управления заводом по обогащению урана в иранском городе Натанз, вывел из строя около тысячи центрифуг, что привело к существенному снижению объема производства обогащения урана, используемого в ядерной программе Ирана.**

*Это первый в истории случай, когда мы имеем дело с злоумышленным воздействием на ядерную инфраструктуру извне, которое привело к желаемому результату, продемонстрировав не только возможность, но и всю серьезность кибератак на атомные, да и на вообще на критически важные объекты. Более того, Stuxnet стал первым примером вредоносного кода, разработанного специально для атаки на атомный объект.*

*При этом применялась специализированная вредоносная программа, аналогов которой с тех пор обнаружено не было (или нам о них пока неизвестно).*

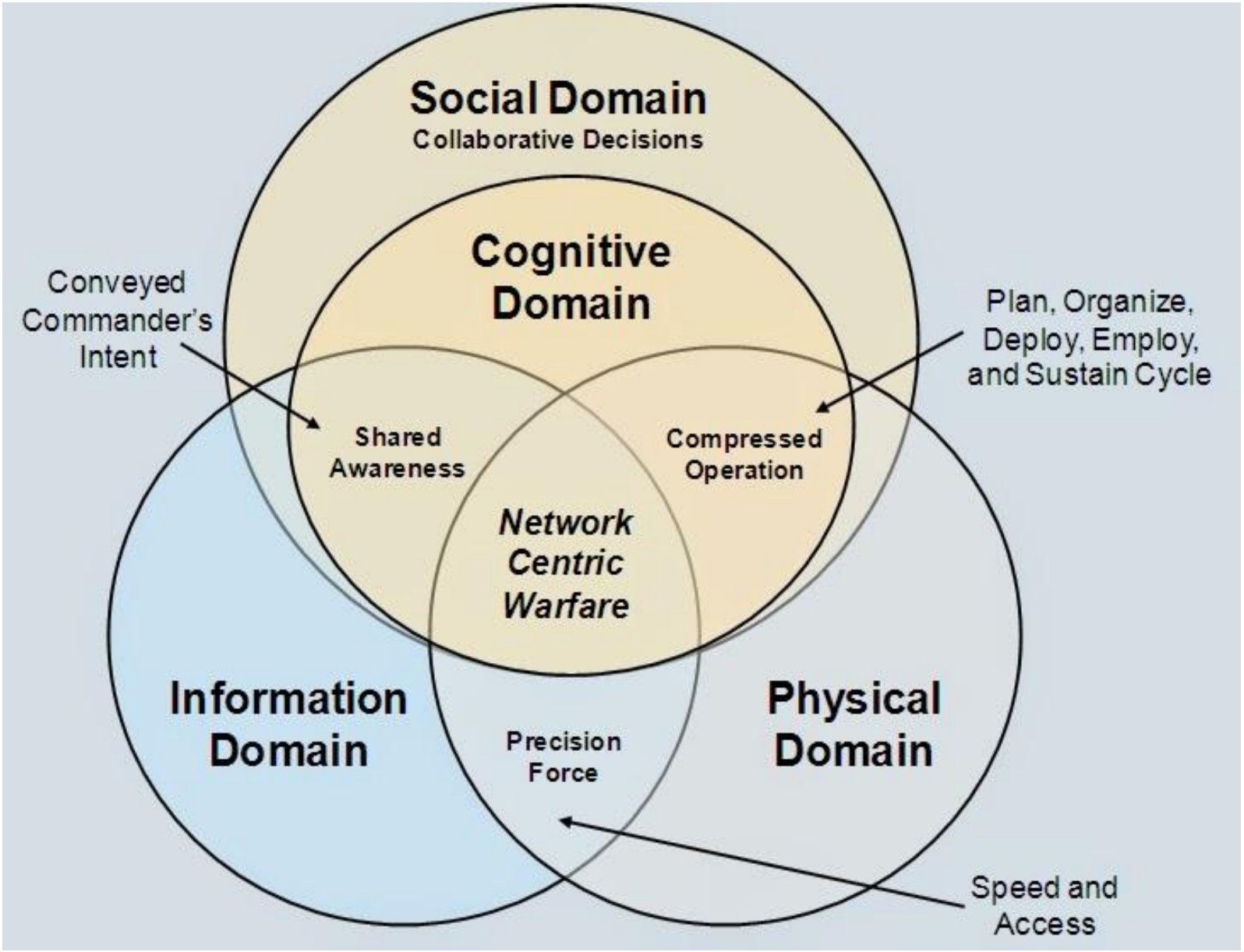
***Вопрос:** возможна ли применение подобных программ в будущем?*

# ВАЖНЫЕ ОТКРЫТИЯ «ЛАБОРАТОРИИ КАСПЕРСКОГО»

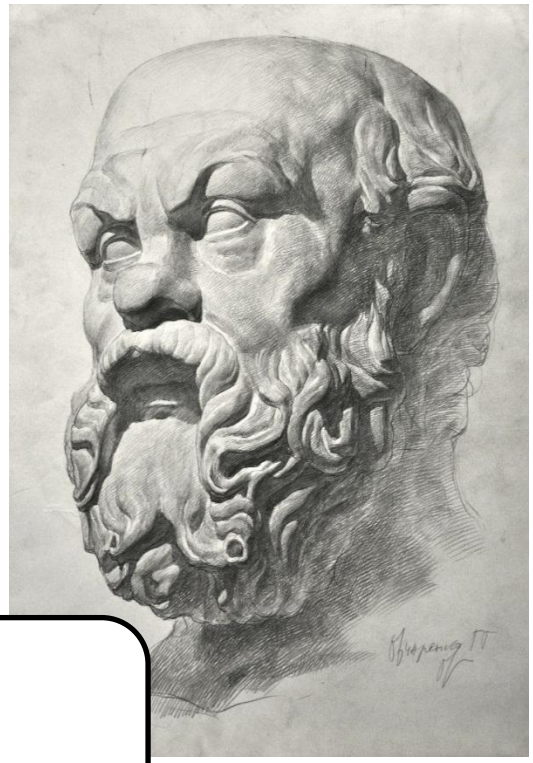
| Угроза | Duqu | Flame | Gauss | miniFlame | Red October | NetTraveler | Careto/The Mask |
|---|---|---|---|---|---|---|---|
| Классификация | Кибершпионское вредоносное ПО | Кибершпионское вредоносное ПО | Кибершпионское вредоносное ПО | Кибершпионское вредоносное ПО | Кампания кибершпионажа | Серия кампаний кибершпионажа | Наиболее сложная кампания кибершпионажа |
| Обнаружение | Сентябрь 2011 | Май 2012 | Июль 2012 | Октябрь 2012 | Январь 2013 | Май 2013 | Февраль 2014 |
| Активность | С 2010 | С 2007 | С 2011 | С 2012 | С 2007 | С 2004 | С 2007 |
| Факты | • Сложный троянец<br>• Ведет себя в системе как бэкдор<br>• Помогает красть частную информацию | • Более 600 конкретных объектов в качестве целей<br>• Может распространяться по локальной сети или через USB<br>• Делает скриншоты, записывает аудиофайлы, отслеживает нажатие клавиш на клавиатуре и сетевой трафик | • Сложный набор модулей выполняет различные функции<br>• Большинство жертв находились в Ливане | • Небольшой, но полнофункциональный модуль для кибершпионажа<br>• Используется для точечных атак<br>• Функционирует отдельно или в качестве дополнительного модуля Flame | • Одна из первых кибершпионских кампаний мирового масштаба<br>• Нацелена на дипломатические и государственные учреждения<br>• Использование русского языка в коде | • 350 жертв высокого уровня в 40 странах<br>• Использование известных уязвимостей в ПО<br>• Нацелена на частные компании, промышленные и исследовательские центры, государственные учреждения | • Более 10000 жертв в 31 стране<br>• Сложный набор инструментов, включая вредоносное ПО, руткиты и буткиты<br>• Версии для Windows, Mac OS X, Linux<br>• Считается одной из самых сложных атак в истории |

KASPERSKY lab

# ОСНОВНЫЕ СОСТАВЛЯЮЩИЕ СЕТЕЦЕНТРИЧЕСКОГО ПРОТИВОБОРСТВА



# «УМНЫЕ СИСТЕМЫ» НЕ УМНАЯ БЕЗОПАСНОСТЬ



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. Шаньгин В.Ф. Информационная безопасность и защита информации. – М.: ДМК-пресс. – 2014. – 702с.


**Нормативные акты**


4. ФЗ от 27 июля 2006 г. 149-ФЗ «Об информации, информационных технологиях и о защите информации».

5. Доктрина Информационной безопасности РФ (утверждена Президентом Российской Федерации В. Путиным 9 сентября 2000 г., № Пр-1895)