ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

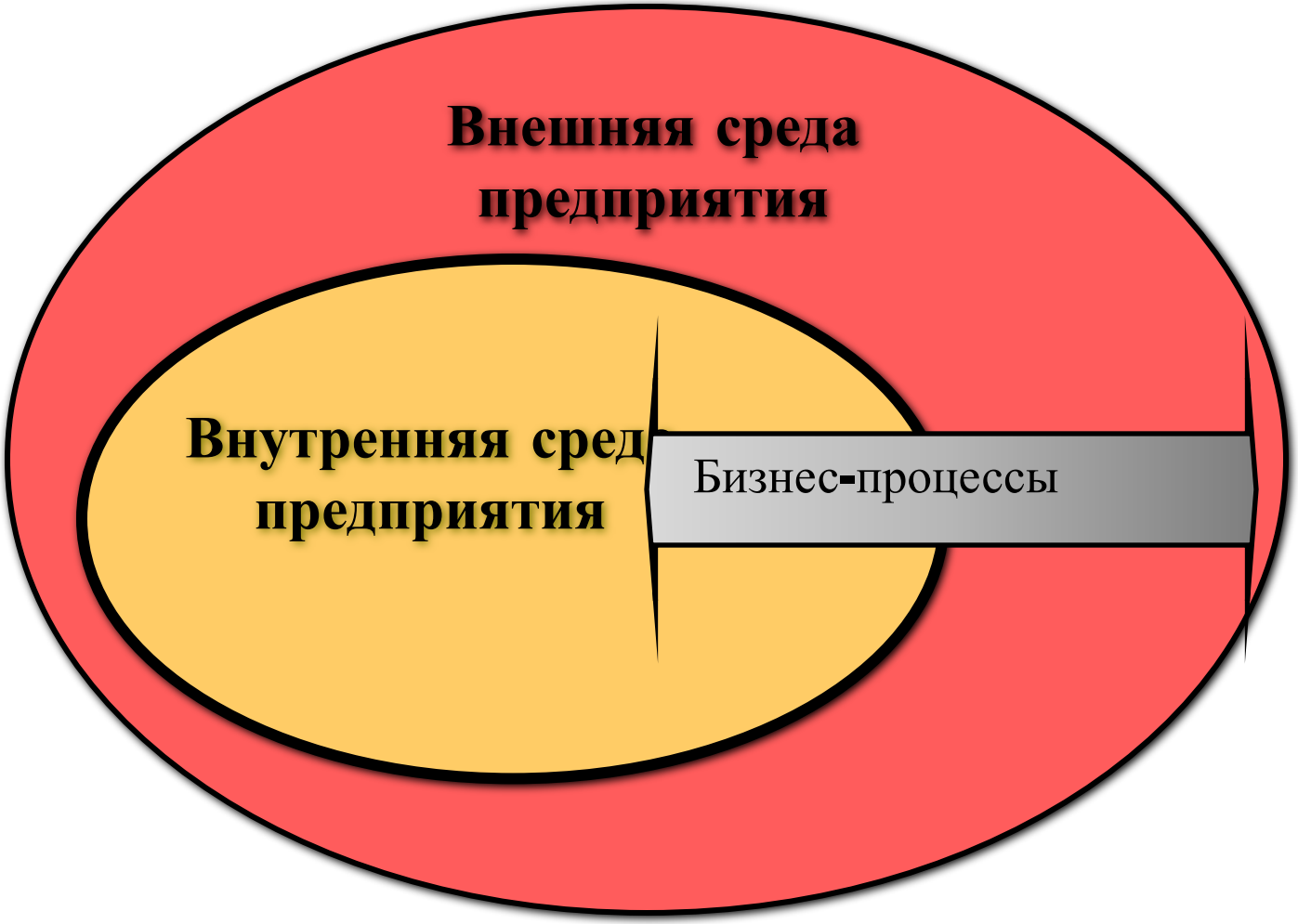
Лекция 1:

«Понятие и сущность информационной безопасности»

Вопросы:

1. Задачи обеспечения безопасности предприятия.
2. Основные понятия информационной безопасности.
3. Понятие и сущность информации ограниченного доступа.
4. Угрозы безопасности информации и их классификация.

Вопрос 1: «Задачи обеспечения безопасности предприятия»



Бизнес-процесс -

- устойчивая, целенаправленная совокупность взаимосвязанных видов деятельности, которая по определенной технологии преобразует входы в выходы, представляющие ценность для потребителя
- *(стандарт МС ИСО 9000:2000).*

Комплексная система защиты информации (КСЗИ) предприятия -

- совокупность методов и средств, объединенных единым целевым назначением и обеспечивающих необходимую эффективность защиты информации предприятия.
- **Главная цель КСЗИ – обеспечение устойчивого функционирования** предприятия и предотвращения угроз его безопасности.

Задачи КСЗИ:

- **отнесение информации к категории ограниченного доступа**, а других ресурсов — к различным уровням уязвимости (опасности), подлежащих сохранению;
- **прогнозирование, своевременное выявление и устранение угроз безопасности** персоналу и ресурсам коммерческого предприятия, причин и условий, способствующих нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развития;

- **создание механизма и условий оперативного реагирования на угрозы безопасности** проявления негативных тенденций в функционировании предприятия;
- **эффективное пресечение угроз персоналу и посягательств на ресурсы** на основе правовых, организационных и инженерно-технических мер и средств обеспечения безопасности;
- **создание условий для максимально возможного возмещения и локализации наносимого ущерба** неправомерными действиями физических и юридических лиц, ослабление негативного влияния последствий нарушения безопасности предприятия.

Последовательность создания КСЗИ

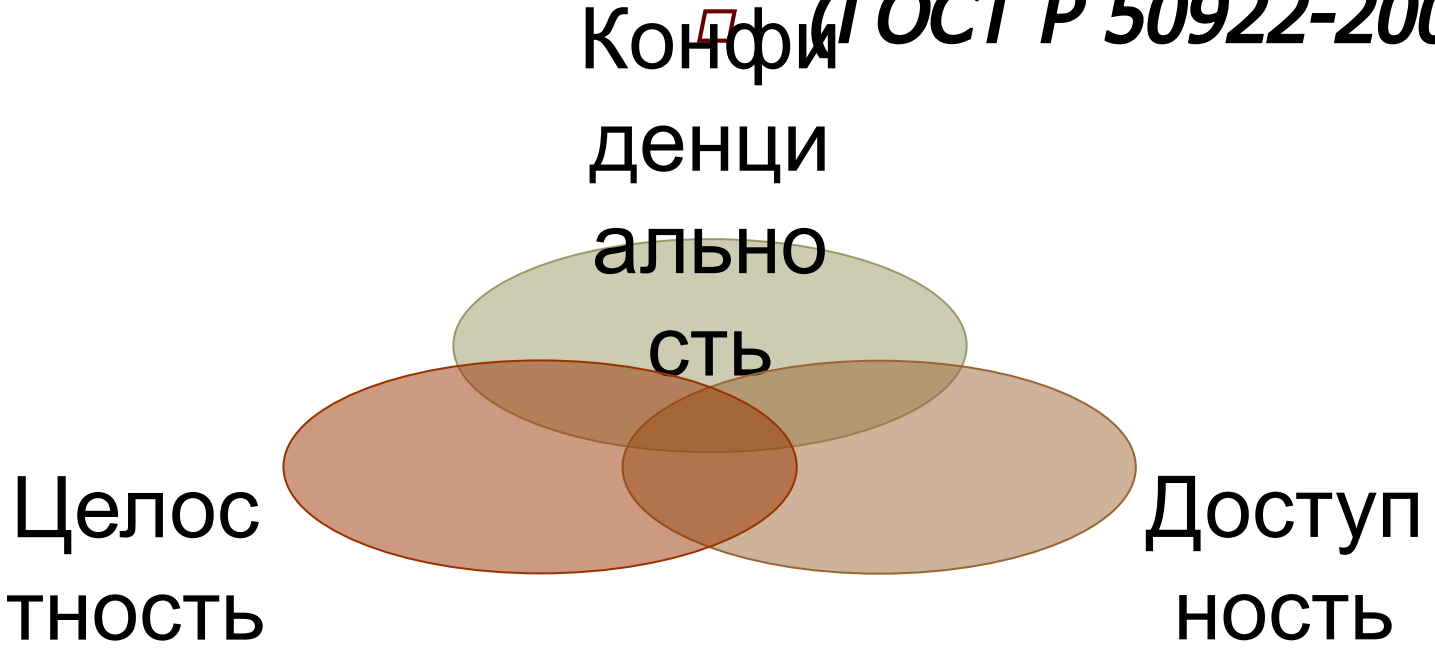
1. Определение состава защищаемой информации и объектов защиты информации.
2. Определение перечня актуальных угроз информационной безопасности.
3. Реализация необходимых способов защиты информации с использованием соответствующих средств.

Вопрос 2: «Основные понятия информационной безопасности»

- **Информация** - сведения (сообщения, данные) независимо от формы их представления.
  - ***ФЗ № 149 от 27 июля 2006 г. «Об информации, информационных технологиях и защите информации»***

- **Безопасность информации (данных):** Состояние защищенности информации (данных), при котором обеспечены ее (их) **конфиденциальность, доступность и целостность**.

(ГОСТ Р 50922-2006)



- **Защита информации** представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от **неправомерного доступа**, **уничтожения, модифицирования, блокирования, копирования, предоставления, распространения,** а также от иных неправомерных действий в отношении такой информации;
2) соблюдение **конфиденциальности** информации ограниченного доступа;
3) реализацию права на **доступ** к информации.

- **Конфиденциальность информации** - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Руководящий документ. Защита от несанкционированного доступа к информации Термины и определения

- **Целостность информации** (Information integrity) - способность средства вычислительной техники или АС обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения).

Рекомендации по стандартизации «Информационные технологии. Основные термины и определения в области технической защиты информации» (Р 50.1.053-2005).

- **Доступность** (информации (англ. availability) - состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать их беспрепятственно.
- **К правам доступа относятся:** право на чтение, изменение, копирование, уничтожение информации, а также права на изменение, использование, уничтожение ресурсов.

ГОСТ Р 50922-2006 Государственный стандарт Российской Федерации. Защита информации. Основные термины и определения

- **Защита информации** (ЗИ) - деятельность, направленная на предотвращение:
- **утечки защищаемой информации**,
- **несанкционированных и непреднамеренных воздействий** на защищаемую информации.

- **Несанкционированное воздействие на информацию:** Воздействие на защищаемую информацию **с нарушением установленных прав** и (или) правил доступа, **приводящее к утечке**, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

- **Система защиты информации** - совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области защиты информации.

- **Средство защиты информации** - техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.
- **Способ защиты информации** - порядок и правила применения определенных принципов и средств защиты информации.

Вопрос 3: «Понятие и сущность информации ограниченного доступа»

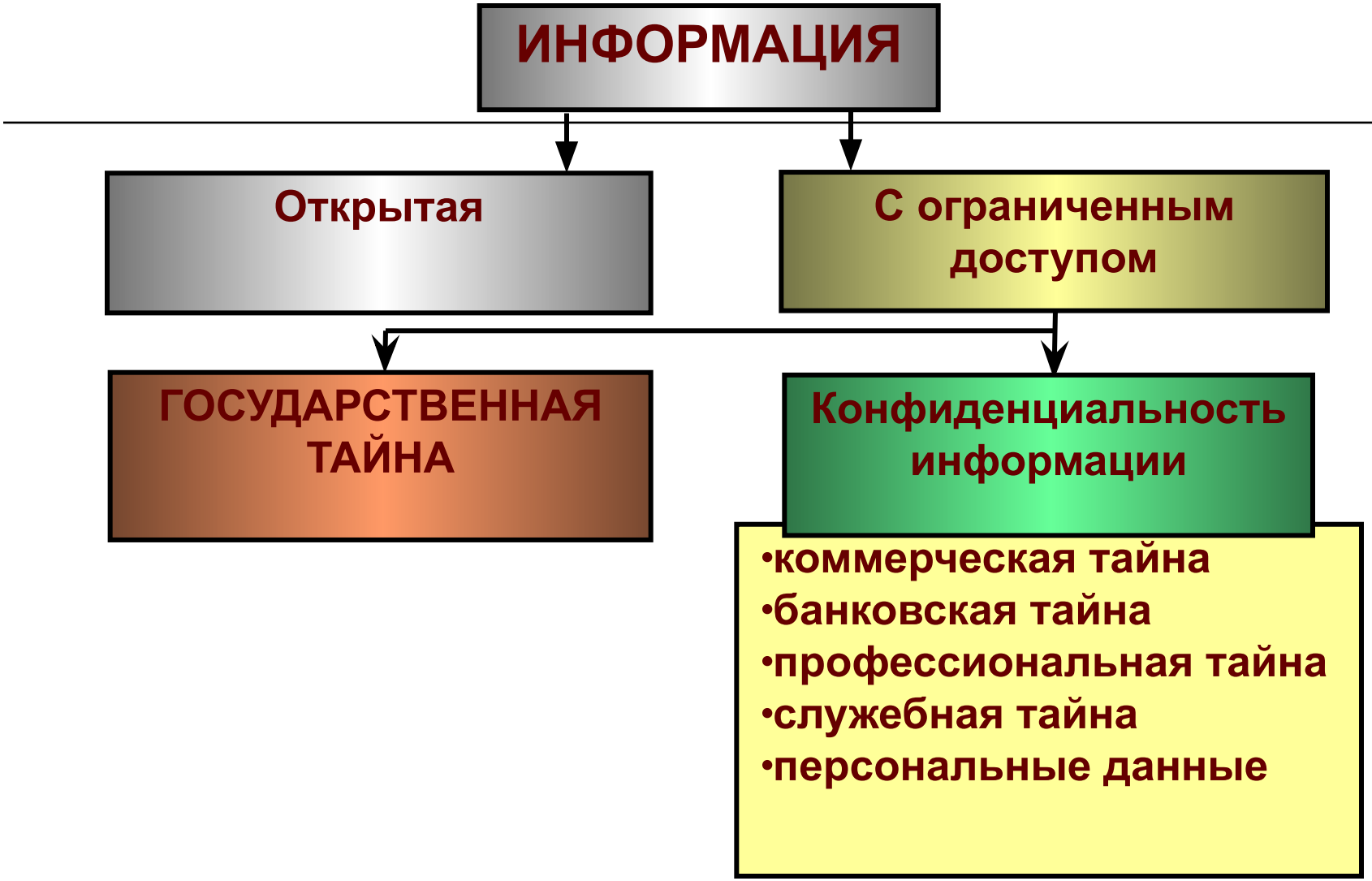
- **Информация ограниченного доступа** - информация, доступ к которой ограничен федеральными законами.
  - ***ФЗ № 149-ФЗ от 27.07. 2006 г. «Об информации, информационных технологиях и защите информации»***

Обладатель информации обязан:

1. Соблюдать права и законные интересы иных лиц.
2. Принимать меры по защите информации.
3. Ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Особенности доступа к информации

- Информация **в зависимости от категории доступа** к ней подразделяется на:
  - общедоступную информацию;
  - информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).


ИНФОРМАЦИЯ
Открытая
С ограниченным доступом
ГОСУДАРСТВЕННАЯ ТАЙНА
Конфиденциальность информации
•коммерческая тайна
•банковская тайна
•профессиональная тайна
•служебная тайна
•персональные данные

Государственная тайна

- **Государственная тайна** — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.
  - ***Закон РФ «О государственной тайне»***

ПЕРЕЧЕНЬ СВЕДЕНИЙ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА

(Указ Президента РФ от 6 марта 1997 г.
С изменениями и дополнениями от ред. от 13.07.2015г.)

1. **Персональные данные.**
2. **Тайна следствия и судопроизводства.**
3. **Служебная тайна.**
4. **Профессиональная тайна.**
5. **Коммерческая тайна.**
6. **Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.**
7. **Сведения, содержащиеся в личных делах осужденных.**

Коммерческая тайна

- **Коммерческая тайна** - конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду
  - ***Закон РФ «О коммерческой тайне»***

ИНФОРМАЦИЯ, СОСТАВЛЯЮЩАЯ КОММЕРЧЕСКУЮ ТАЙНУ

концептуальная:
- новые идеи
- стратегии
- концепции развития

организационная:
- деловые связи
- управленческие решения
- планы производства

технологическая:
- управление предприятием
- управление финансами
- технологии

параметрическая:
- расчеты эффективности
- структура цены
- издержки

эксплуатационная:
- эксплуатация оборудования
- утилизация оборудования
- сведения о системе безопасности

Банковская тайна

- **Банковская тайна** — защищаемые банками и иными кредитными организациями сведения о банковских операциях по счетам и сделкам в интересах клиентов, счетах и вкладах своих клиентов и корреспондентов, а также сведения о клиентах и корреспондентах, разглашение которых может нарушить право последних на неприкосновенность частной жизни.

Информация, отнесенная к банковской тайне:

Ст. 857 ГК РФ	Ст. 26 Банковского закона
Гарантируется тайна:	
• банковского счета; • банковского вклада; • операций по счету; • сведений о клиенте.	• об операциях; • о счетах о вкладах своих клиентов и корреспондентов; • о иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону.

Профессиональная тайна

- **Профессиональная тайна** — защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной или муниципальной службой, распространение которой может нанести ущерб правам и законным интересам другого лица (доверителя), доверившего эти сведения, и не являющаяся государственной или коммерческой тайной.
  - ***Закон РФ «Об информации, информационных технологиях и защите информации»***

Объекты профессиональной тайны:

- Нотариальная тайна (тайна завещания)
- Врачебная тайна
- Адвокатская тайна
- Тайна страхования
- Аудиторская тайна
- Тайна связи (тайна переписки, почтовых, телеграфных и иных сообщений)
- Тайна ломбарда
- Тайна усыновления
- Тайна исповеди

Служебная тайна

- **Служебная тайна** — защищаемая по закону конфиденциальная информация, ставшая известной в государственных органах и органах местного самоуправления только на законных основаниях и в силу исполнения их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости.
  - ***ГОСТ 34.003–90. Автоматизированные системы Термины и определения***

Персональные данные

- **Персональные данные** - любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).
  - ***Федеральный закон «О персональных данных»***

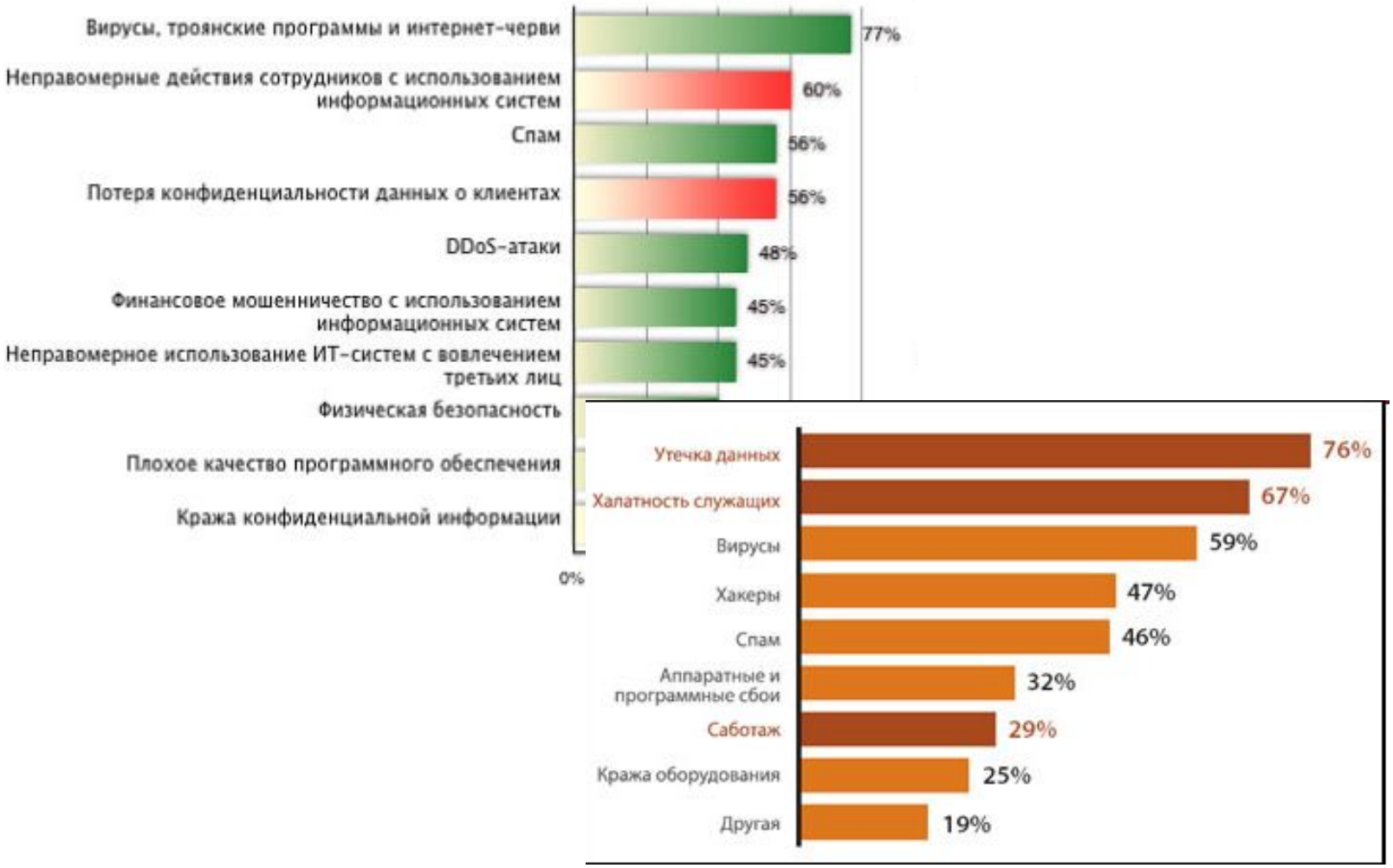
Вопрос 5: «Угрозы безопасности информации и их классификация»

- **Угроза (безопасности информации)** - совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.
  - ***ГОСТ Р 50922-2006 Национальный стандарт РФ. Защита информации. Основные термины и определения***

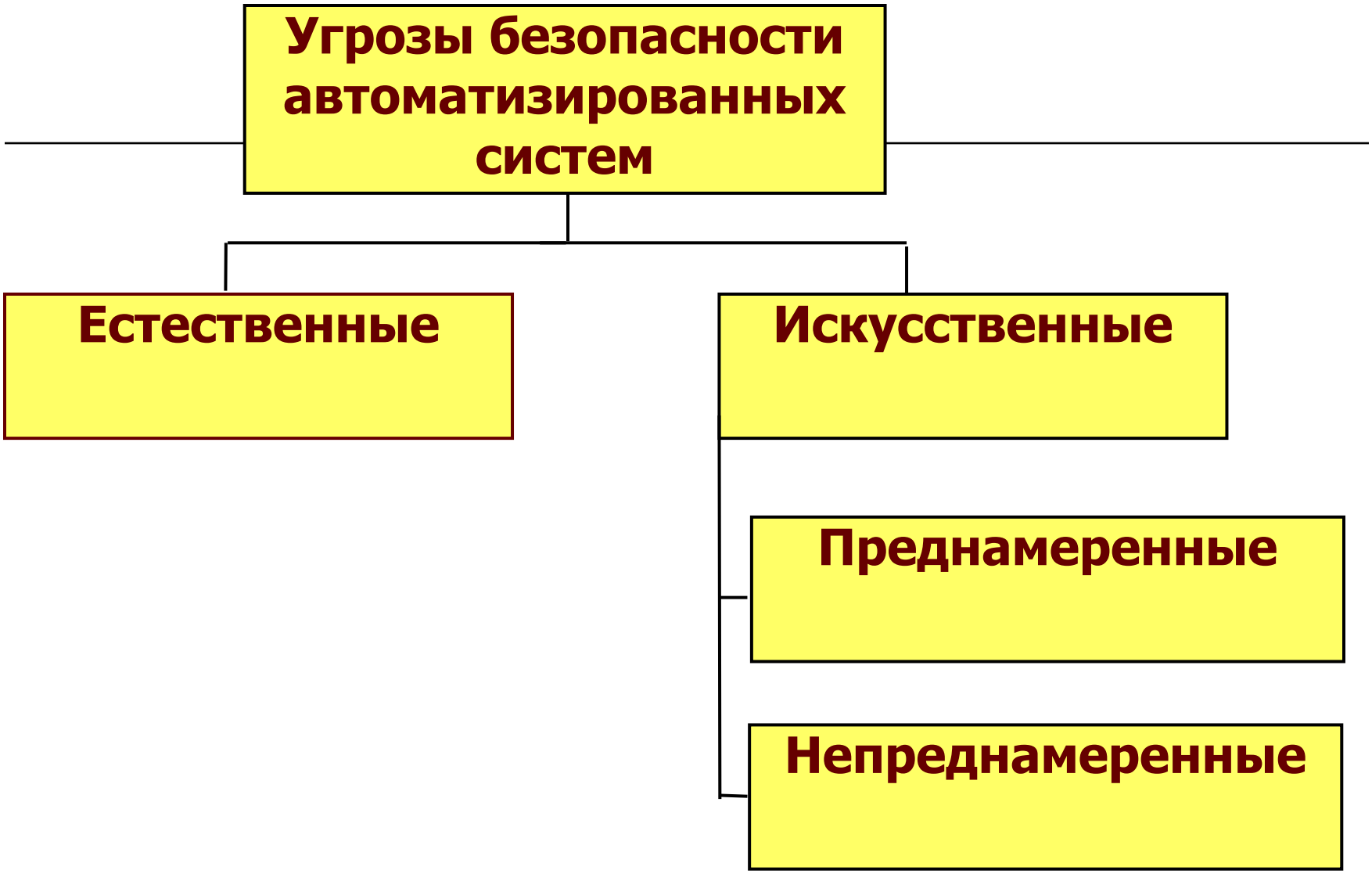
Угрозы современной России

- распространение оружия массового уничтожения и его попадания в руки террористов;
- Противоправная деятельность **в кибернетической и биологической областях, в сфере высоких технологий;**
- **усиление глобального информационного противоборства;**
- **развитие националистических настроений, ксенофобии, сепаратизма и насильственного экстремизма;**
- обострение мировой демографической ситуации;
- проблемы окружающей природной среды;
- угрозы, связанные с неконтролируемой и незаконной миграцией, наркоторговлей и торговлей людьми;
- распространение эпидемий, вызываемых новыми, неизвестными ранее вирусами;
- последствия мировых финансово-экономических кризисов могут стать сопоставимыми с масштабным применением военной силы.

Рейтинг угроз ИБ



- Угроза реализуется в виде **атаки**, в результате чего и происходит нарушение безопасности информации.
- **Основные виды нарушения безопасности информации:**
- нарушение **конфиденциальности**;
- нарушение **целостности**;
- нарушение **доступности**.


Угрозы безопасности автоматизированных систем
Естественные
Искусственные
Преднамеренные
Непреднамеренные

Угрозы безопасности

внешние угрозы:

- недобросовестные конкуренты;
- криминальные группы и формирования;
- противозаконные действия административного аппарата.

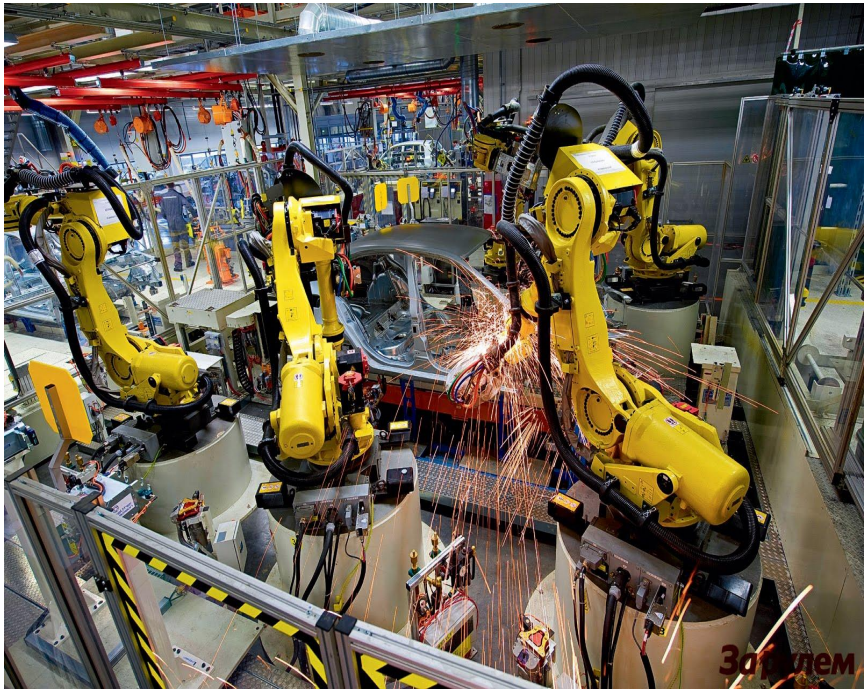
внутренние угрозы:

- преднамеренные и непреднамеренные действия персонала;
- отказ оборудования, технических средств;
- сбои программного обеспечения.

Угрозы критически важным объектам

- **Критически важный объект** - объект, нарушение (или прекращение) функционирования которого приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению (или разрушению) экономики страны, субъекта РФ, либо административно-территориальной единицы или существенному ухудшению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный срок.

Основной признак КВО - наличие на объекте экологически опасного или социально значимого производства или технологического процесса, нарушение штатного режима которого приводит к ЧС.

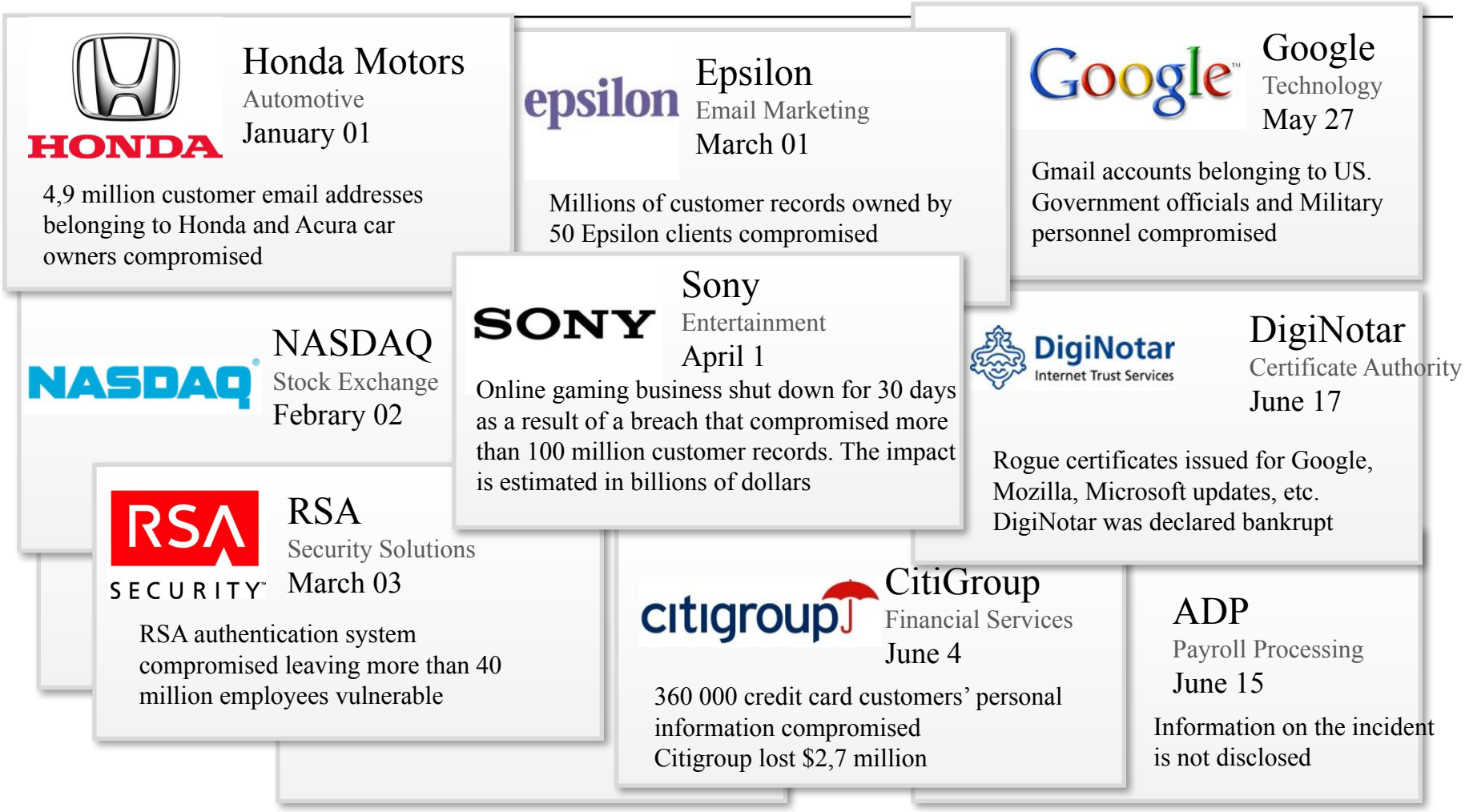


Актуальные угрозы безопасности КСИИ

- **Stuxnet** (воздействие на программы ПЛК Siemens Simatic S7);
- **Duqu** (кража информации);
- **Wiper** (удаление информации с жестких дисков ПК);
- **Flame** (бэкдор, шпионаж);
- **Gauss** (перехват cookie-файлов, паролей, данных по учетным записям в социальных сетях, почтовых сервисах).

Информационное воздействие

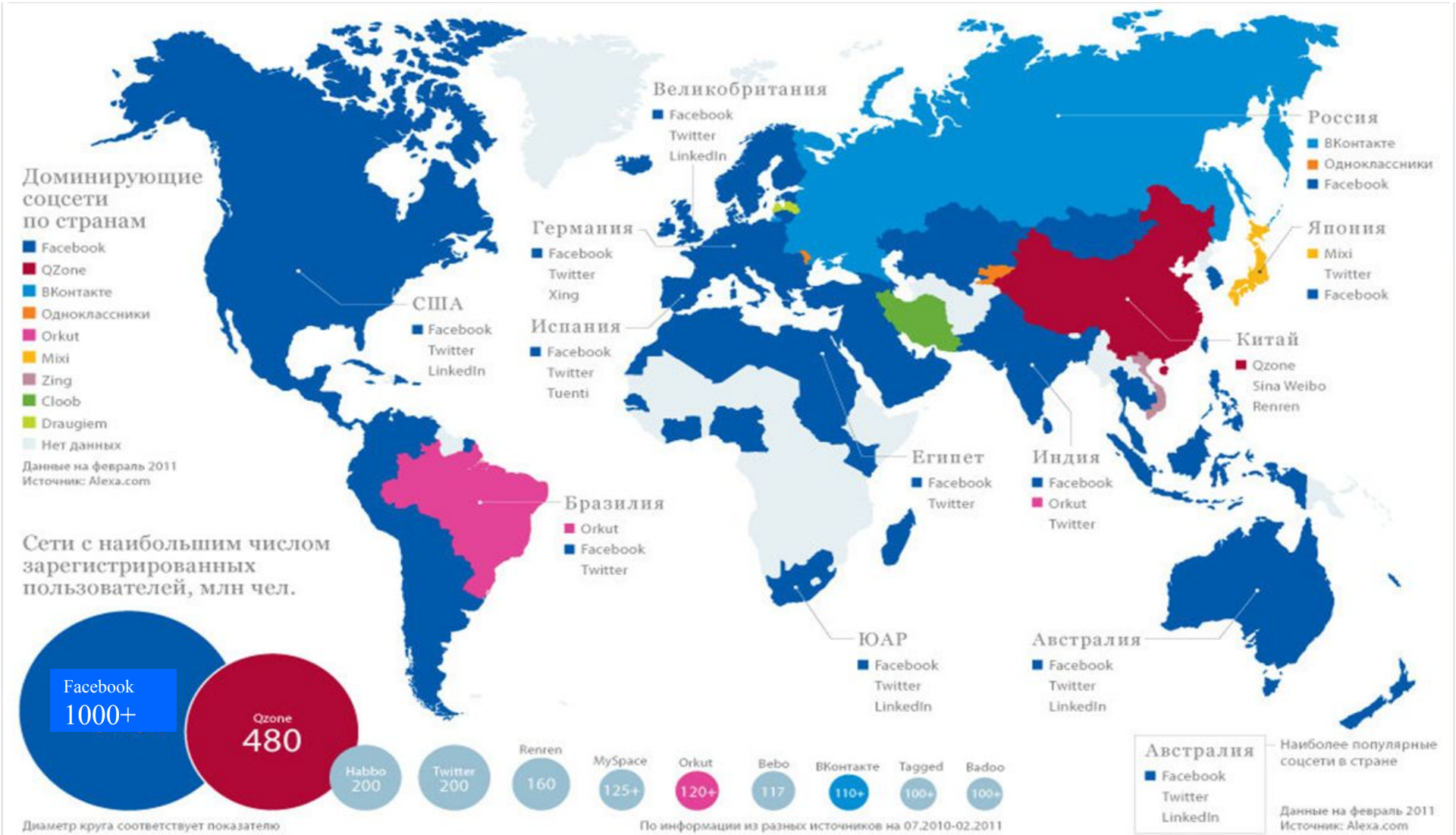
Взлом крупной компании – обычное дело



Использования социальных сетей в информационных войнах

- В сентябре 2010 г. Госдепом США был разработан **«Стратегический план развития информационных технологий в 2011–2013 гг.: цифровая дипломатия».**
- Ключевой инструмент в дипломатической практике правительства США - применение социальных сетей

СОЦИАЛЬНЫЕ СЕТИ В МИРЕ



Тендер ФБР (FBI) о разработке ПО контент-анализа соцсетей

Social Media Application

Solicitation Number: SocialMediaApplication

Agency: Department of Justice

Office: Federal Bureau of Investigation

Location: Procurement Section

Notice Type:
Modification/Amendment

Original Posted Date:
January 19, 2012

Posted Date:
January 20, 2012

Response Date:
Feb 10, 2012 11:59 pm Eastern

Original Response Date:
Feb 07, 2012 11:59 pm Eastern

Archiving Policy:
Automatic, on specified date

Original Archive Date:
February 16, 2012

Archive Date:
February 16, 2012

Original Set Aside:
N/A

Set Aside:
N/A

Classification Code:
70 -- General purpose information technology equipment

NAICS Code:
519 -- Other Information Services/519130 -- Internet Publishing and Broadcasting and Web Search Portals

---

Synopsis:

Added: Jan 19, 2012 4:14 pm Modified: Jan 20, 2012 3:34 pm Track Changes

Please review the Request for Information (RFI) that is attached. The Federal Bureau of Investigations is

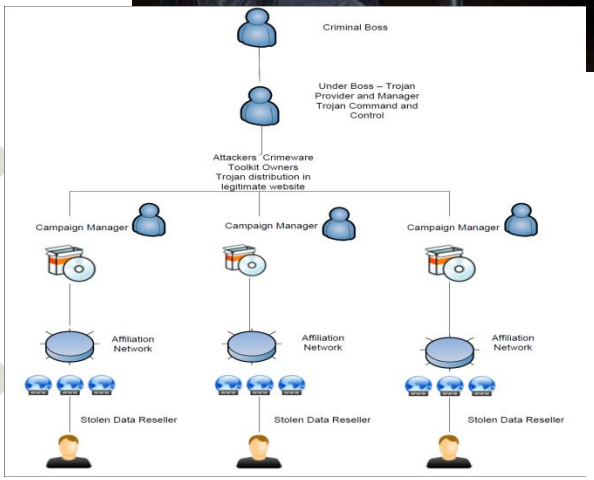
Не смотря на то, что:

- ИБ строится десятилетиями
- Вкладываются серьезные средства
- Актуальны угрозы информационной безопасности

Причина 1. Новые цели – новые хищники

APT

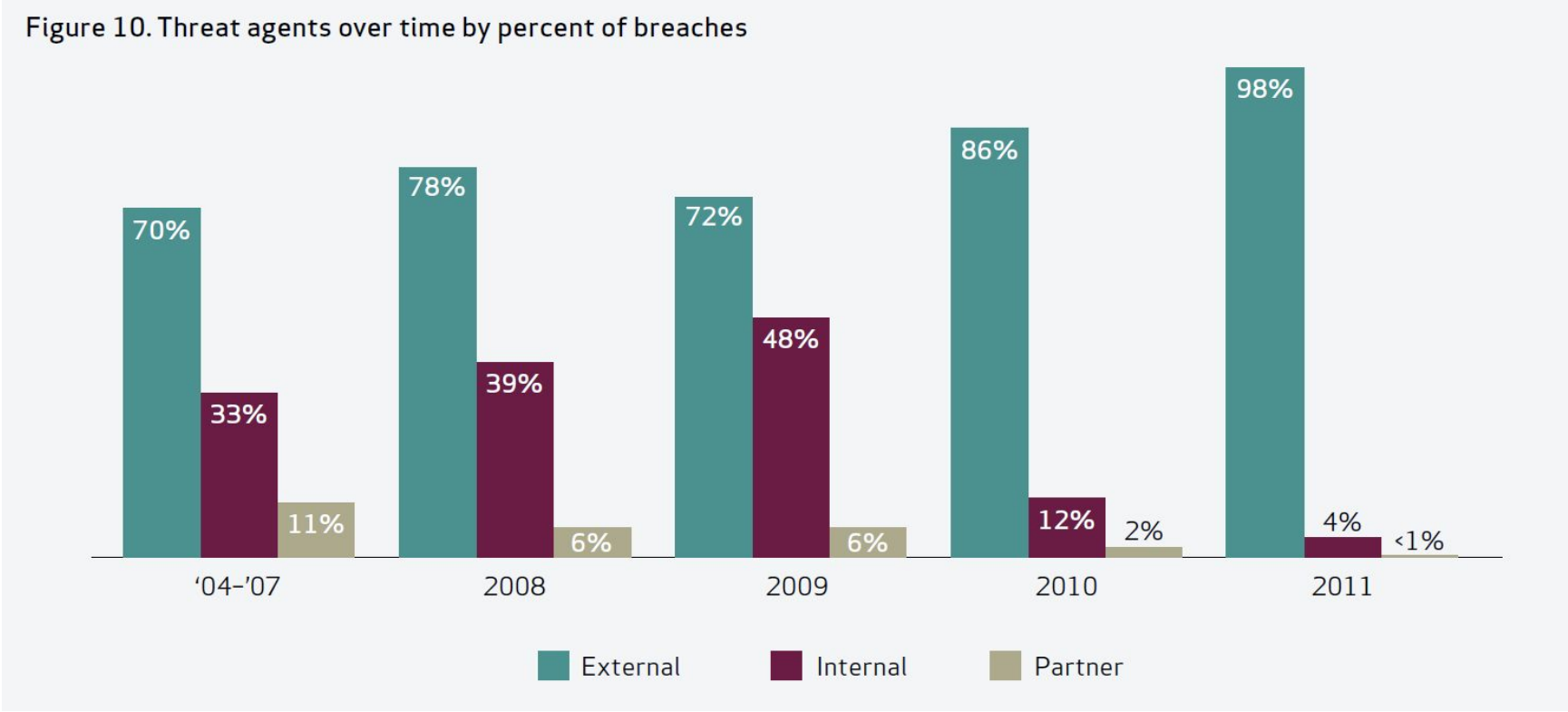
Hooligans	Interest	Low damage
Organized crime	Money	Banking and retail damage
Cyber troops	Cyber War	Serious damage
Underground Community	Ideology	Unpredictable



Причина 2. Бумажная безопасность

Отчет: Verizon Data Breach Investigations 2012

96% атак были квалифицированы как не сложные!



Причина 3. Отсутствие культуры информационной безопасности

Причина 4. Технологии нападения - впереди

- СЗИ обеспечивают безопасность защищаемой информации;
- Межсетевые экраны, VPN, антивирусы, ААА – защита от внешнего нарушителя;
- DLP, средства защиты от НСД – от внутреннего нарушителя.

0-day

BYOD

Иллюзии о SCADA системах

- Сети АСУ ТП **изолированы** и никто не сможет соединиться с ними;
- MES/SCADA/PLC **используют специализированные платформы** и поэтому «взломоустойчивы»;
- HMI это просто **устройство для отображения** информации.

«Социальный инжиниринг»