Методы и средства защиты информации

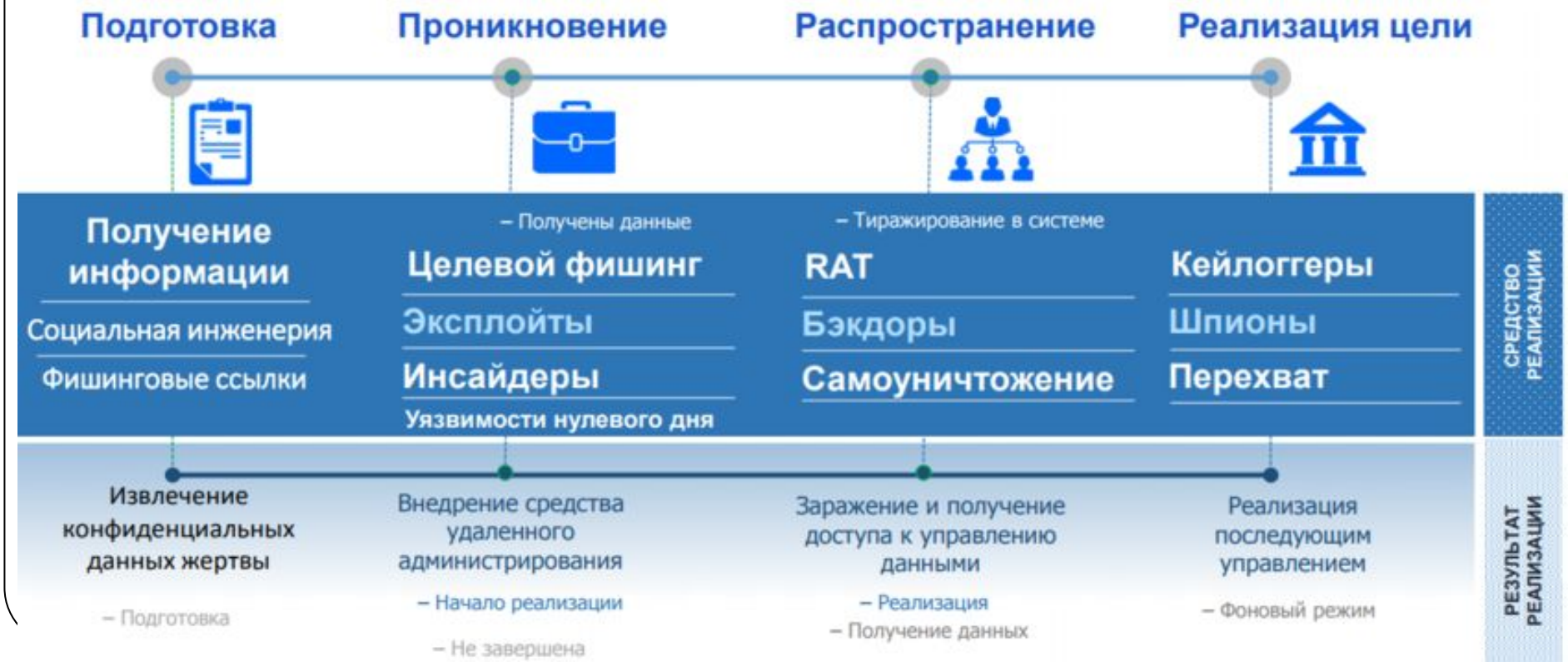
Атака на информационную систему

- - преднамеренные действия злоумышленника, использующие уязвимости информационной системы и приводящие к нарушению доступности, целостности и конфиденциальности обрабатываемой информации.

- **APT** (англ. ***a**dvanced **p**ersistent **t**hreat* — «развитая устойчивая угроза»; также **целевая кибератака**) — противник, обладающий современным уровнем специальных знаний и значительными ресурсами, которые позволяют ему создавать возможности для достижения целей посредством различных векторов нападения.

Этапы подготовки и реализации атаки

- Разведка на местности.
- Активная фаза.
- Изучение инфраструктуры изнутри.
- Финал APT-атаки.



Защита информации

- - это деятельность, которая направлена на предотвращение утечки защищаемых данных, непреднамеренных и несанкционированных воздействий на защищаемые данные.

Защита информации направлена на

- ***Обеспечение*** защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- ***Соблюдение*** конфиденциальности информации ограниченного доступа;
- ***Реализацию*** права на доступ к информации.

Обладатель информации, оператор информационной системы обязаны обеспечить

- предотвращение ;
- обнаружение ;
- предупреждение ;
- недопущение ;
- восстановления ;
- контроль ;
- размещение.

Уровни защиты информации

1. Правовой уровень
2. Организационный уровень
3. Технический уровень

- ***Средства защиты информации***
  - **нормативные (неформальные)**
  - **технические (формальные)**

КЛАССИФИКАЦИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Классификация средств защиты


Теоретические методы
Формализация процессов, связанных с обеспечением ИБ
Обоснование корректности и адекватности систем обеспечения ИБ
Организационные методы
Управление ИБ на предприятии
Методы обеспечения информационной безопасности
Сервисы сетевой безопасности
Идентификация и аутентификация
Разграничение доступа
Протоколирование и аудит
Средства защиты периметра
Криптографические средства защиты
Инженерно-технические методы
Защита информации от утечки по техническим каналам
Правовые методы
Ответственность
Работа с гостайной
Защита авторских прав
Лицензировани и сертификация

Организационно-технические методы

- создание и совершенствование системы обеспечения информационной безопасности Российской Федерации;
- выявление, изобличение и привлечение к ответственности лиц, совершивших преступления и другие правонарушения в этой сфере;
- разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;
- создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;
- выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите информации;
- сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;
- контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности Российской Федерации;
- формирование системы мониторинга показателей и характеристик информационной безопасности Российской Федерации в наиболее важных сферах жизни и деятельности общества и государства.

Организационно-технические методы информационной безопасности

- систему обеспечения информационной безопасности;
- разработку (создание новых), эксплуатацию и усовершенствование уже имеющихся средств защиты информации;
- перманентный контроль над действенностью принимаемых мер в области обеспечения информационной безопасности.

Организационная защита информации

- состоит в своде правил, составленных на основе правовых актов РФ, призванных предотвратить неправомерное овладение конфиденциальными данными.

К организационным методам и средствам защиты информации относятся:

- охрана серверов;
- тщательно организованный подбор персонала;
- исключение таких случаев, когда все особо важные работы выполняются одним человеком;
- разработка плана, как восстановить работоспособность сервера в ситуации, когда он выйдет из строя;
- универсальные средства защиты от любого пользователя.

Составляющие организационного метода обеспечения ИБ

- создание режима охраны информации;
- разработка правил взаимоотношений между сотрудниками;
- регламентация работы с документами;
- правила использования технических средств в рамках существующего правового поля РФ;
- аналитическая работа по оценке угроз информационной безопасности.

Правовой фактор безопасности

- лицензирование деятельности в части обеспечения информационной безопасности;
- сертификация технических средств информационной защиты;
- аттестация объектов информатизации согласно соответствию нормам информационной безопасности РФ.

Законы, регулирующие порядок работы с конфиденциальной информацией

- Федеральный закон «О защите персональных данных»
- Федеральный закон «О коммерческой тайне»
- Закон «Об архивном деле»
- Стандарт Банка России
- Соглашение Basel II
- Закон HIPAA
- Закон SOX
- Правило 17a-4 Комиссии по ценным бумагам США
- Федеральный закон «О связи»
- Доктрина информационной безопасности
- Федеральный закон «Об информации, информационных технологиях и о защите информации»
- Федеральный закон «О противодействии неправомерному использованию инсайдерской информации»
- Федеральный закон «О банках и банковской деятельности»
- Федеральный закон «Об электронной подписи»

Экономические методы

- разработка и составление программ по обеспечению информационной безопасности РФ;
- определение источников их финансового обеспечения;
- разработка порядка финансирования;
- создание механизма страхования информационных рисков.

Технические методы и средства защиты информации

- защита от несанкционированного доступа к компьютерной системе;
- резервирование всех важных компьютерных подсистем;
- организация сетей с последующей возможностью перераспределить ресурсы, если возникнет нарушение работоспособности отдельных сетевых звеньев;
- установка оборудования по обнаружению и тушению пожаров;
- установка оборудования по обнаружению воды;
- принятие комплекса мер по защите от хищений, диверсий, саботажа, взрывов;
- установка резервной системы электропитания;
- оснащение помещения замками;
- установка сигнализации и др.

Информационная безопасность

- это всегда комплексная система, все составляющие которой призваны не допустить утечки конфиденциальных сведений по техническим каналам, а также воспрепятствовать стороннему доступу к носителям информации.

Способы защиты информации

- Препятствие
- Управление
- Маскировка
- Регламентация
- Принуждение
- Побуждение

Средства защиты информации

- Физические средства
- Аппаратные средства
- Программные средства
- Организационные средства
- Законодательные средства
- Морально-этические средства

Сопоставление способов и средств защиты информации