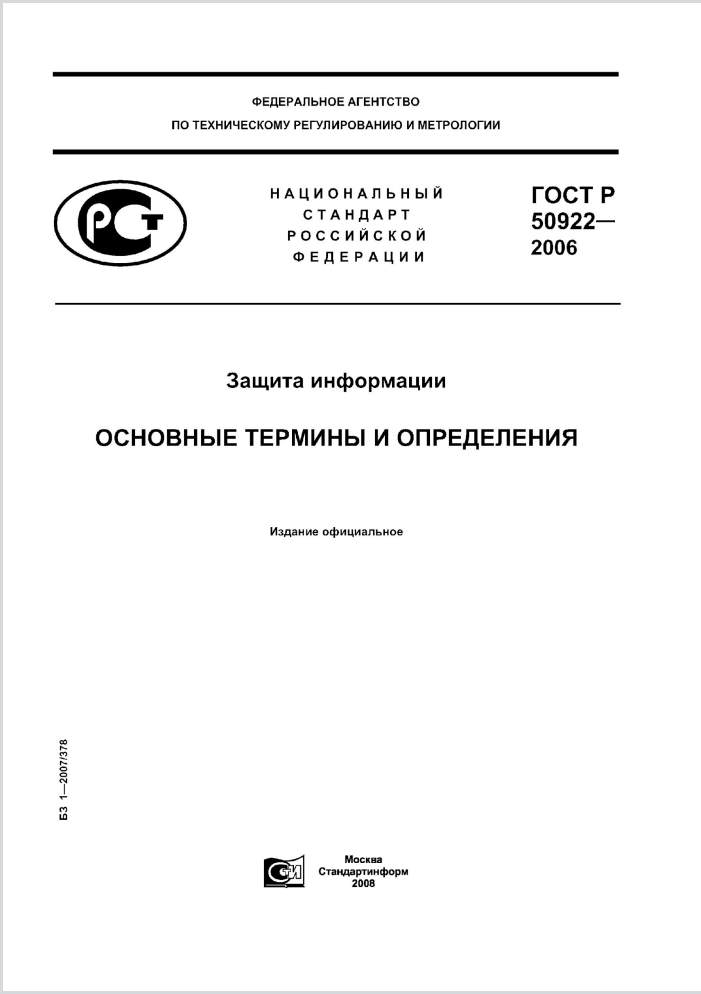
Российский государственный университет нефти и газа (НИУ) имени И.М. Губкина
ФАКУЛЬТЕТ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ТЭК

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КИБЕРБЕЗОПАСНОСТЬ

Выполнила:
студентки группы КС-19-04
Черевко Е.С.

Определение информационной безопасности

- Информационная безопасность – это состояние защищенности общества и государства, отдельного гражданина от информационно-технического воздействия на информационную инфраструктуру (Указ Президента РФ от 5 декабря 2016 г. № 646).
- Информационная безопасность - состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность (ГОСТ 50922-2006).



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 50922— 2006

Защита информации

ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Издание официальное

БЗ 1—2007/378

Москва
Стандартинформ
2008

Конфиденциальность, целостность и доступность

- **Конфиденциальность** – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.
- **Целостность** – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;
- **Доступность** – состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно.

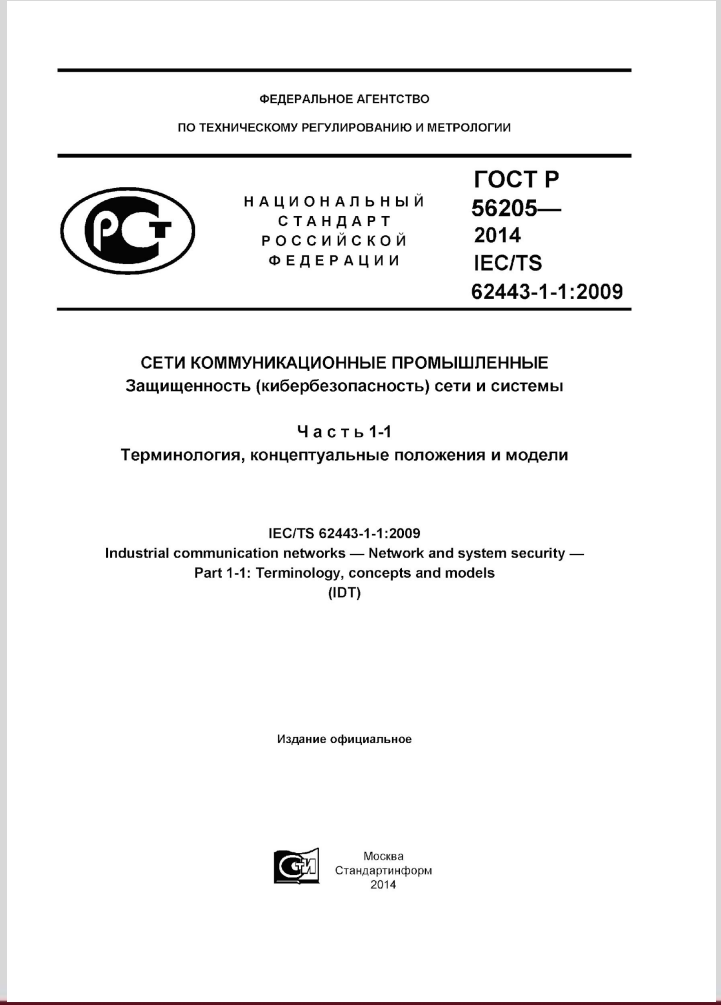
Способы достижения информационной безопасности

Для обеспечения информационной безопасности в информационной системе применяются четыре основных метода, актуальных для любого формата информации:

- ограничение или полное закрытие доступа к информации;
- шифрование;
- дробление на части и разрозненное хранение;
- скрытие самого факта существования информации.

Определение кибербезопасности

Кибербезопасность - действия, необходимые для предотвращения неавторизованного использования, отказа в обслуживании, преобразования, рассекречивания, потери прибыли, или повреждения критических систем или информационных объектов (ГОСТ Р 56205-2014).



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 56205— 2014 IEC/TS 62443-1-1:2009

СЕТИ КОММУНИКАЦИОННЫЕ ПРОМЫШЛЕННЫЕ
Защищенность (кибербезопасность) сети и системы

Часть 1-1
Терминология, концептуальные положения и модели

IEC/TS 62443-1-1:2009
Industrial communication networks — Network and system security —
Part 1-1: Terminology, concepts and models
(IDT)

Издание официальное

Москва
Стандартинформ
2014

Цель кибербезопасности

Цель— уменьшить персональный риск травмирования или риск угрозы здоровью населения, риск потери доверия общественности или потребителей, разглашения информации о важных объектах, незащищенности бизнес-объектов или несоответствия нормативам.

Кибербезопасность можно разделить на три основные категории: анализ рисков, обнаружение и реагирование, а также защита.

Анализ рисков, обнаружение и защита

- Анализ рисков включает в себя определение потенциальных рисков для сетей и систем вашей организации, чтобы вы могли определить приоритетные направления расходования бюджета на кибербезопасность.
- Обнаружение включает в себя мониторинг активности в вашей сети для обнаружения любой несанкционированной активности или активности, которая может указывать на нарушение.
- Защита подразумевает защиту ваших информационных систем от атак хакеров с помощью различных методов, таких как брандмауэры и системы обнаружения вторжений (IDS).

Информационная безопасность и кибербезопасность: Различия

1. ***Сфера безопасности.***

Кибербезопасность - это процесс защиты информации в киберпространстве.

Информационная безопасность - это более широкий термин, который включает все методы, используемые для защиты информации от несанкционированного доступа, использования, раскрытия, модификации или уничтожения в любой форме.

2. Защита от угроз.

Кибербезопасность связана с защитой компьютерных сетей и технологий от кибератак, кибертерроризма и других видов атак, использующих компьютеры или сети в качестве средств.

Информационная безопасность фокусируется на защите данных в любом формате, в котором они хранятся.

Информационная безопасность и кибербезопасность: Различия

3. Подход к нарушению безопасности.

При борьбе с кибербезопасностью выделяют два основных вида нарушения: кибепреступность и кибермошенничество.

Борьба с информационной безопасностью может быть выражена как несанкционированный доступ, модификация с целью раскрытия информации и нарушение работы.

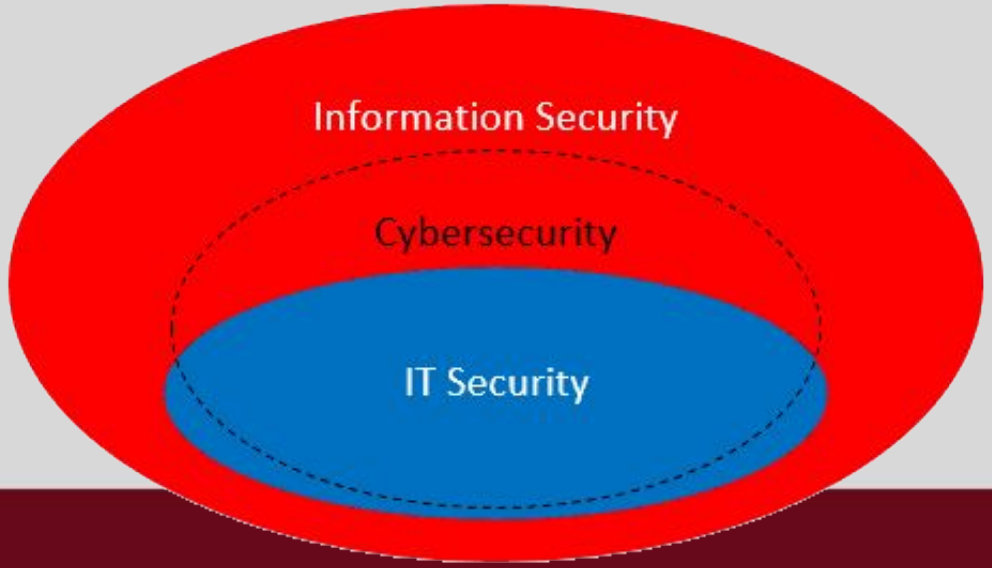
4. Активация защиты.

Кибербезопасность - это первая линия обороны от киберугроз. Она пытается предотвратить проникновение хакеров в компьютер или кражу вашей личной информации.

Информационная безопасность - это то, что происходит, когда кибербезопасность дает сбой - когда она нарушена и вредоносный код проникает через брандмауэр в систему.

Информационная безопасность и кибербезопасность: Пересечения

- обе области рассматривают угрозы безопасности данных, которые могут исходить из любого источника (включая человеческий фактор);
- обе области рассматривают защиту данных в процессе их прохождения через сети или устройства;
- обе области рассматривают защиту устройств, чтобы они не были уязвимы для атак хакеров или других злоумышленников.



Спасибо за внимание!