Кафедра КИБЭВС

ТУСУР
Томский государственный университет систем управления и радиоэлектроники

Безопасность систем баз данных

Преподаватель: Сарин К. С.

Безопасность систем баз данных

4 семестр – зачет

5 семестр – экзамен

6 семестр – курсовая работа

Лекции

- Основные понятия защиты информации
- Защита информации в СУБД
- Управления доступом в СУБД
- Модели разграничения доступа в СУБД
- Управления целостностью данных
- Распределенные базы данных
- Механизм транзакций в СУБД

Безопасность систем баз данных

Практические работы

1. Использование команды select *.
2. Проектирование баз данных при сопровождении существующих продуктов.

Лабораторные работы

1. Установка и настройка MS SQL сервер.
2. Разграничения доступа к данным и объектам СУБД.
3. Безопасность на уровне строк.
4. Запросы и хранимые процедуры.
5. SQL инъекции.

Литература

- **Базы данных**. В 2-х кн.Кн. 1. Локальные базы данных: учебник / В.П. Агальцов. - 2-е изд., перераб. - М.:ИД ФОРУМ: ИНФРА-М, 2012. - 352 с.: ил.
- **Базы данных**: Учебник / Шустова Л.И., Тараканов О.В. - М.:НИЦ ИНФРА-М, 2016. - 304 с
- Култыгин, О. П. **Администрирование баз данных. СУБД MS SQL Server** [Электронный ресурс] : учеб. пособие / О. П. Култыгин. - М.: МФПА, 2012. - 232

Кафедра КИБЭВС

ТУСУР
Томский государственный университет систем управления и радиоэлектроники

Лекция №1

Основные понятия защиты информации

Безопасность информации [данных]: состояние *защищённости* информации [данных], при котором обеспечены её [их] *конфиденциальность*, *доступность* и *целостность*.

Информационная безопасность – все аспекты, связанные с определением, достижением и поддержанием *конфиденциальности*, *целостности*, *доступности*, *неотказуемости*, *подотчётности*, *аутентичности* и *достоверности* информации или средств её обработки.

Объект защиты информации

Объект защиты информации – *информация* или *носитель информации*, или *информационный процесс*, которые необходимо защищать в соответствии с целью защиты информации.

Информация, информационный процесс

Информация – сведения независимо от формы их представления.

Информационный процесс – процесс создания, сбора, обработки, накопления, хранения, поиска, распространения и использования информации.

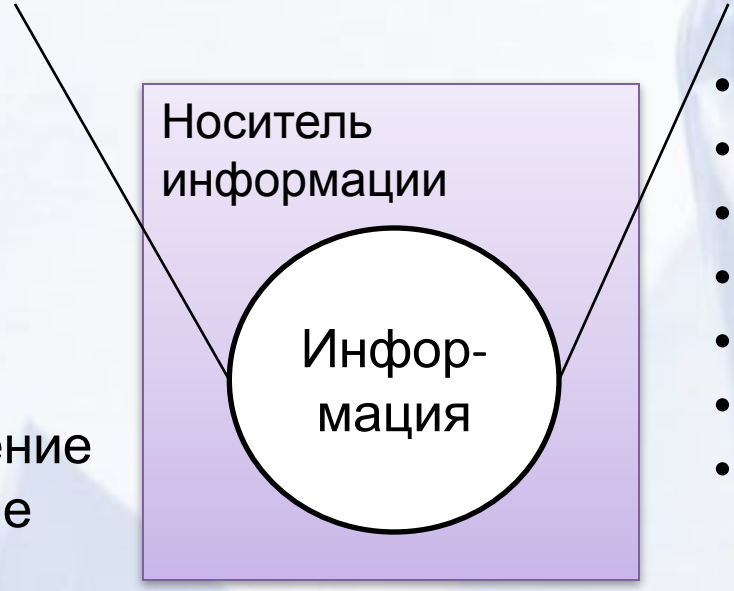
Носитель информации

Носитель защищаемой информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит своё отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Характеристики информации

Информационный процесс

- создание
- сбор
- обработка
- накопление
- хранение
- поиск
- распространение
- использование



Свойства информации

- конфиденциальность
- целостность
- доступность
- неотказуемость
- подотчётность
- аутентичность
- достоверность

Информационная безопасность при применении информационных технологий

Безопасность информации (при применении информационных технологий) – состояние защищённости информационной технологии, обеспечивающее безопасность информации, для обработки которой она применяется, и информационную безопасность *автоматизированной информационной системы*, в которой она реализована.

Информационные ресурсы АИС

Защищаемые информационные ресурсы (автоматизированной информационной системы) – информационные ресурсы автоматизированной информационной системы, для которых должен быть обеспечен требуемый уровень их защищённости.

Примечание – информационные ресурсы включают в себя документы и массивы документов, используемые в автоматизированных информационных системах.

Защищаемая автоматизированная информационная система – автоматизированная информационная система, предназначенная для сбора, хранения, обработки, передачи и использования защищаемой информации с требуемым уровнем её защищённости.

Свойства информации, обеспечиваемые при её защите

Конфиденциальность (информации [ресурсов автоматизированной информационной системы]) – состояние информации [ресурсов автоматизированной информационной системы], при котором доступ к ней [к ним] осуществляют только субъекты, имеющие на него право.

Целостность (информации [ресурсов автоматизированной информационной системы]) – состояние информации [ресурсов автоматизированной информационной системы], при котором её [их] изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Свойства информации, обеспечиваемые при её защите

Доступность (информации [ресурсов автоматизированной информационной системы]) – состояние информации [ресурсов автоматизированной информационной системы], при котором субъекты, имеющие право доступа, могут реализовать их беспрепятственно.

Примечание - К правам доступа относятся: право на чтение, изменение, копирование, уничтожение информации, а также права на изменение, использование, уничтожение ресурсов.

Свойства информации, обеспечиваемые при её защите

- **Неотказуемость** – способность удостоверять имевшее место действие или событие так, чтобы эти события или действия не могли быть позже отвергнуты.
- **Подотчётность (ресурсов автоматизированной информационной системы)** – состояние ресурсов автоматизированной информационной системы, при котором обеспечиваются их идентификация и регистрация.

Свойства информации, обеспечиваемые при её защите

- **Аутентичность** – свойство, гарантирующее, что субъект или ресурс идентичны заявленным.

Примечание – аутентичность применяется к таким субъектам, как пользователи, к процессам, системам и информации.

- **Достоверность** – свойство соответствия предусмотренному поведению и результатам.

Нарушение информационной безопасности организации

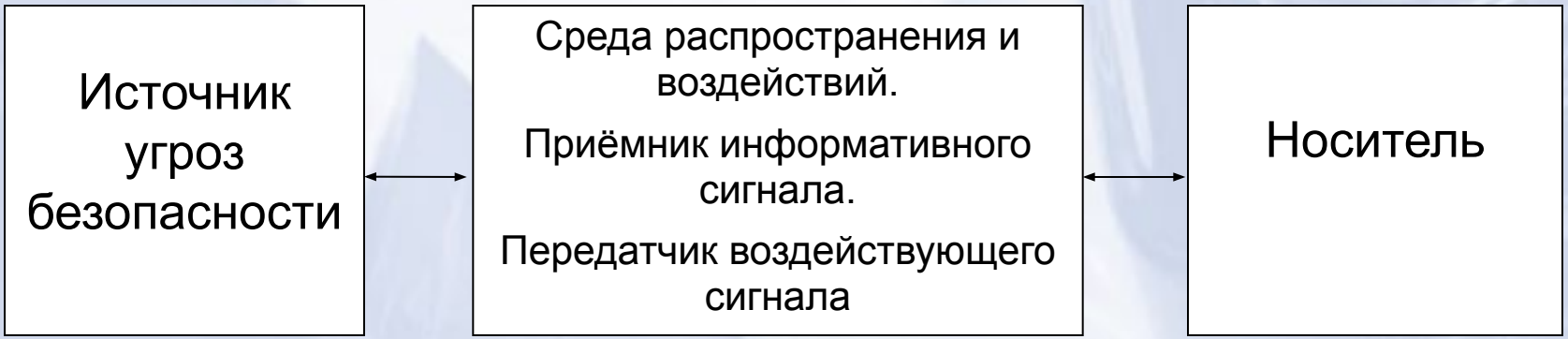
Нарушение информационной безопасности организации – случайное или преднамеренное неправомерное действие физического лица (субъекта, объекта) в отношении активов организации, следствием которых является нарушение безопасности информации при её обработке техническими средствами в информационных системах, вызывающее негативные последствия (ущерб/вред) для организации.

Угроза информационной безопасности

- **Угроза (безопасности информации)** – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.
- **Источник угрозы безопасности информации** – субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.

Каналы реализации угроз

Угроза безопасности реализуется в результате образования канала реализации угрозы безопасности между *источником угрозы* и *носителем* (информации), что создает условия для нарушения безопасности (несанкционированный или случайный доступ).



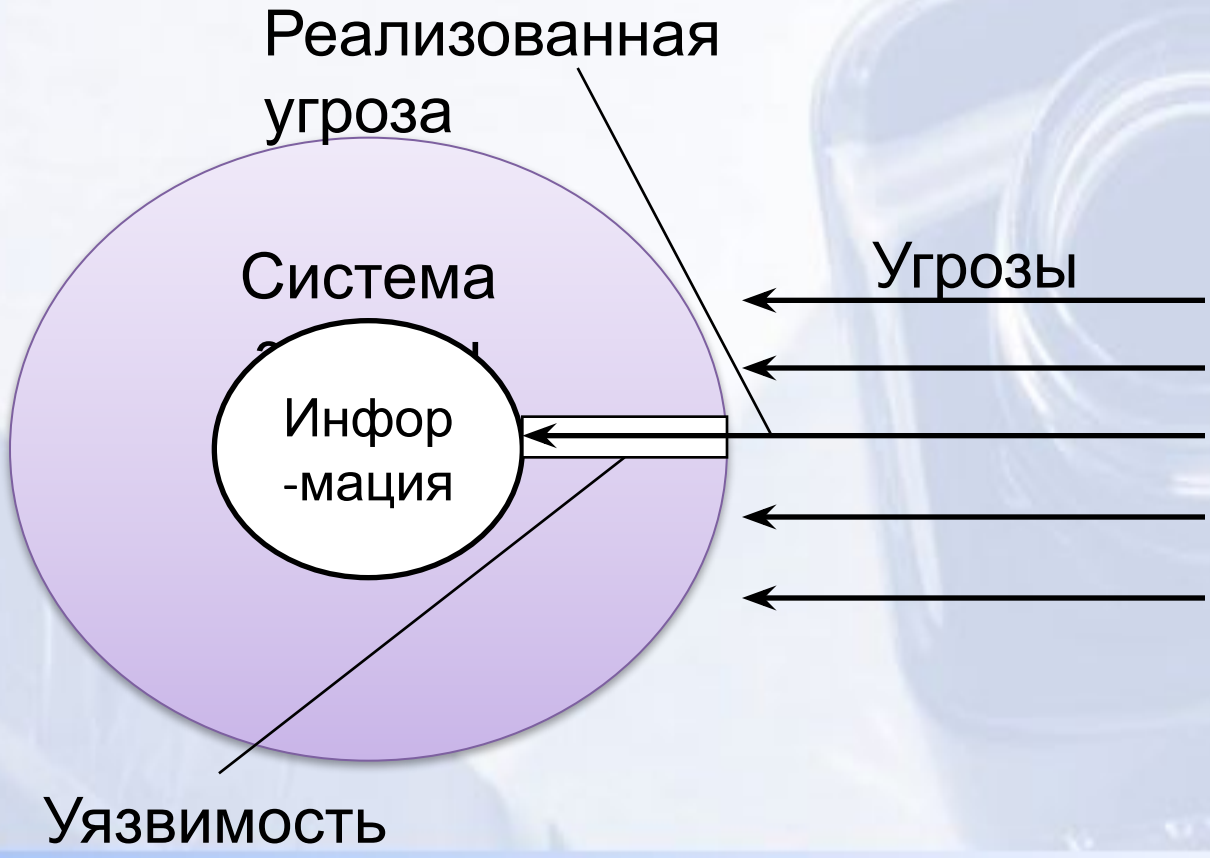
Система защиты информации

Система защиты информации (СЗИ)– совокупность *органов и (или) исполнителей*, используемой ими *техники* защиты информации, а также *объектов* защиты информации, организованная и функционирующая *по правилам и нормам*, установленным соответствующими документами в области защиты информации.

Угрозы системе защиты информации

- Угрозы конфиденциальности – угрозы утечки информации, описывающей структуру и порядок работы СЗИ.
- Угрозы целостности – угрозы несанкционированного изменения (отключения) элементов СЗИ и (или) их настроек.

Нарушение информационной безопасности



Уязвимость

Уязвимость (информационной системы); брешь – свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации.

Примечания

- *Условием реализации угрозы безопасности обрабатываемой в системе информации может быть недостаток или слабое место в информационной системе.*
- *Если уязвимость соответствует угрозе, то существует риск.*

Классификация уязвимостей программного обеспечения

- Уязвимости системного программного обеспечения (в том числе протоколов сетевого взаимодействия).
- Уязвимости прикладного программного обеспечения (в том числе средств защиты информации).

Причины возникновения уязвимостей

- Ошибки при проектировании и разработке программного (программно-аппаратного) обеспечения.
- Преднамеренные действия по внесению уязвимостей в ходе проектирования и разработки программного (программно-аппаратного) обеспечения.
- Неправильные настройки программного обеспечения, неправомерное изменение режимов работы устройств и программ.
- Несанкционированное внедрение и использование неучтенных программ с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях).

Причины возникновения уязвимостей

- Внедрение вредоносных программ, создающих уязвимости в программном и программно-аппаратном обеспечении.
- Несанкционированные неумышленные действия пользователей, приводящие к возникновению уязвимостей.
- Сбои в работе аппаратного и программного обеспечения (вызванные сбоями в электропитании, выходом из строя аппаратных элементов в результате старения и снижения надежности, внешними воздействиями электромагнитных полей технических устройств и др.).

Кафедра КИБЭВС

ТУСУР
Томский государственный университет систем управления и радиоэлектроники

Спасибо за внимание!!!