**Практическая работа 1**

1. **Под защитой информации в системе и сетях** понимается защищенность системы от вмешательства в нормальный процесс ее функционирования, от попыток хищения информации, модификации или физического разрушения ее компонентов.
2. **ИБ КИС** расшифровывается как «информационная безопасность корпоративных информационных систем».
3. **Угрозы информации** подразделяются на *естественные* и *человеческие*. Человеческие в свою очередь делятся на *умышленные (преднамеренные) угрозы* и *неумышленные (случайные) угрозы.*
4. **Основным направления реализации информационных угроз :**

• непосредственное обращение к объектам доступа;

• обращение к объектам доступа в обход средств защиты, с помощью созданных программ;

•изменение средств защиты

•внедрение в АС программных или технических механизмов, нарушающих предполагаемую структуру и функции.

**Основные методы реализации угроз информационной безопасности :**

•определение злоумышленником типа и параметров носителей информации;

•получение злоумышленником информации о программно-аппаратной среде, типе и параметрах средств вычислительной техники, типе и версии операционной системы, составе прикладного программного обеспечения.

•получение злоумышленником детальной информации о функциях, выполняемых АС;

•получение злоумышленником данных о применяемых системах защиты;

•определение способа представления информации;

•хищение (копирование) машинных носителей информации, содержащих конфиденциальные данные;

•хищение (копирование) носителей информации;

•несанкционированный доступ пользователя к ресурсам АС в обход или путем преодоления систем защиты с использованием специальных средств, приемов, методов;

1. **Информационная система (ИС)** — это система сбора, хранения и передачи информации. Можно сказать, что это взаимодействие людей и компьютеров для обработки и интерпретации неких данных или какой либо информации.
2. **Информационные ресурсы** – документы, содержащиеся в информационных системах (библиотеках, архивах, фондах, банках данных, информационных системах других видов).
3. **Основу политики безопасности** составляет способ управления доступом, который определяет порядок доступа субъектов системы к объектам системы.
4. **Механизмы защиты информации:**

*формирование и опознание подписи;*

*контроль и разграничение доступа;*

*система регистрации и учета информации;*

*обеспечение целостности данных;*

*обеспечение аутентификации;*

*подстановка трафика;*

*управление маршрутизацией;*

*арбитраж или освидетельствование.*

Проанализировав все механизмы защиты информации я могу сказать, что хоть они и имет большие различия , почти все механизмы построенны на «проверке» и «контроле».

**Свойства защиты информации:**

-Конфиденциальность. Свойство, позволяющее ограничить круг субъектов, имеющих доступ к информации, и сохранить информацию от субъектов, не имеющих прав на доступ к такой информации.

-Целостность. Свойство, позволяющее существовать данной информации в неискаженном виде .

-Доступность. Свойство, позволяющее обеспечить своевременный доступ субъектов к информации, когда в этом возникает необходимость.

1. **Объект защиты информации** - информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью. К объектам защиты информации могут быть отнесены: охраняемая территория, здание , выделенное помещение, информация и информационные ресурсы объекта информатизации.
2. **В целом, любые действия**, выполняемые с информацией, называются информационными процессами. Среди информационных процессов, можно выделить получение, обработку, передачу, хранение, поиск, кодирование и защиту информации.
3. **Информационная система (ИС**) — система, предназначенная для хранения, поиска и обработки информации. ИС предназначена для своевременного обеспечения надлежащих людей надлежащей информацией, то есть для удовлетворения конкретных информационных потребностей.
4. . **Информационные ресурсы**- являются источником информации, представляют собой отдельные документы и массивы документов в информационных системах.
5. Одним из примеров ПАК является «СЕРГЕК», которая выполняет следующие функции: Распознавание автомобильных номеров, фиксация нарушений ПДД (превышение скорости на рубеже контроля, превышение скорости на участке дороги, проезд на красный сигнал светофора, пересечение сплошной линии, выезд на встречную полосу и т.д.

Следующий пример – ПАК «Соболь» предназначенный для предотвращения несанкционированного доступа посторонних лиц.

ПАК имеют следующие преимущества:

* Система сбора данных имеет большее быстродействие, лучшие характеристики по точности измерения и возможность подключения большего количества датчиков, что позволяет проводить более сложные опыты.
* Датчики имеют лучшие технические характеристики и точность измерения параметров.
* Программное обеспечение имеет большие возможности обработки и визуализации информации, позволяет вывести на экран всю необходимую информацию по подготовке, проведению и интерпретации опытов.
* Программно-аппаратный комплекс выполнен в современном дизайне, имеет наименьшие габариты и вес, надежную систему подключения датчиков, что дает большую надежность.