# Основные понятия и определения предмета защиты информации

- **Доступ к информации** − ознакомление с информацией, ее обработка (копирование, модификация или удаление).
- **Защита информации (ЗИ)** − это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

# *Несанкционированный доступ (НСД) к информации*

- характеризуется нарушением установленных правил разграничения доступа.

# *Санкционированный доступ к информации (доступ, согласованный с правообладателем)*

- — это доступ к информации, не нарушающий установленные правила разграничения доступа. Правила разграничения доступа служат для регламентации права доступа к компонентам системы.

- **Защита от НСД к информации** – это деятельность, направленная на предотвращение несанкционированного доступа к защищаемой информации.
- **Защищаемая информация** – это информация, являющаяся предметом собственности и подлежащая защите в соответствие с требованиями нормативных документов или требованиями, устанавливаемыми собственниками информации.

- **Субъект доступа к информации** — участник правоотношений в информационных процессах.
- **Объект доступа –** это единица информационного ресурса, доступ к которой регламентируется правилами разграничения доступа.

- **Нарушитель (субъект атаки) –** это лицо или инициируемый им процесс, осуществляющий НСД.

# Анализ угроз информационной безопасности

# *По природе возникновения* различают:

- *естественные угрозы,* вызванные воздействиями на ИС объективных физических процессов или стихийных природных явлений;
- *искусственные угрозы* безопасности ИС, вызванные деятельностью человека.

# *По степени преднамеренности* проявления различают:

- *угрозы, вызванные ошибками или халатностью* персонала, например некомпетентное использование средств защиты; ввод ошибочных данных ит. п.;
- *угрозы преднамеренного действия,* например действия злоумышленников.

# основные каналы несанкционированного доступа

- штатные каналы доступа к информации (терминалы пользователей, оператора, администратора системы; средства отображения и документирования информации; каналы связи) при их использовании нарушителями, а также законными пользователями вне пределов их полномочий;
- технологические пульты управления;
- линии связи между аппаратными средствами ИС;

# способы и приемы несанкционированного доступа

- *Перехват паролей* осуществляется специально разработанными программами.
- При попытке законного пользователя войти в систему программа-перехватчик имитирует на экране дисплея ввод имени и пароля пользователя, которые сразу пересылаются владельцу программы-перехватчика,

- после чего на экран выводится сообщение об ошибке и управление возвращается операционной системе. Пользователь предполагает, что допустил ошибку при вводе пароля. Он повторяет ввод и получает доступ в систему. Владелец программы-перехватчика, получивший имя и пароль законного пользователя, может теперь использовать их в своих целях. Существуют и другие способы перехвата паролей.

*Маскарад* — это выполнение каких-либо действий одним пользователем от имени другого пользователя, обладающего соответствующими полномочиями.

Целью маскарада является приписывание каких-либо действий другому пользователю либо присвоение полномочий и привилегий другого пользователя.

Примерами реализации маскарада являются:

- вход в систему под именем и паролем другого пользователя (этому маскараду предшествует перехват пароля);
- передача сообщений в сети от имени другого пользователя. Маскарад особенно опасен в банковских системах электронных платежей, где неправильная идентификация клиента из-за маскарада злоумышленника может привести к большим убыткам законного клиента банка.

# *Незаконное использование привилегий.*

- Большинство систем защиты устанавливают определенные наборы привилегий для выполнения заданных функций.
- Каждый пользователь получает свой набор привилегий: обычные пользователи — минимальный, администраторы — максимальный.
- Несанкционированный захват привилегий возможен  при наличии ошибок в системе защиты, либо из-за халатности администратора при управлении системой и назначении привилегий.

- Несанкционированный захват привилегий, например посредством маскарада, приводит к возможности выполнения нарушителем определенных действий в обход системы защиты.
- Следует отметить, что незаконный захват привилегий возможен либо при наличии ошибок в системе защиты, либо из-за халатности администратора при управлении системой и назначении привилегий.

- Фишинг
- Фарминг
- Вредоносные программы
- Вирусы