Лекция 6. Автоматизированная система как объект информационного воздействия

1.Основные компоненты автоматизированной систе-мы (АС). Субъекты информационных отношений в АС, их безопасность.

2.Уязвимость структурно-функциональных элементов АС.

3.Угрозы безопасности информации, АС и субъектов информационных отношений. Основные источники угроз.

1.Основные компоненты автоматизированной системы (АС). Субъекты информационных отношений в АС, их безопасность.

- АС - система, состоящая из персонала, комплекса средств автоматизации его деятельности и регламентов работы, реализующая информационную технологию выполнения установленных функций.
- АС - это организованная совокупность средств, методов и мероприятий, используемых для регулярной обработки информации для решения задачи.

АС=Железо+ПО (ОПО+СПО)+Персонал (люди), организованные для выполнения определенных функций.

Персонал АСУ : оперативный и эксплуатационный.

Оперативный персонал - лица, непосредственно участвующие в принятии решений по процессу управления и в выполнении функций системы.

Эксплуатационный персонал - лица, обеспечивающие нормальные условия функционирования АСУ в соот-ветствии с Инструкцией по эксплуатации (выполняю-щие работу по техническому обслуживанию системы).

Ремонтный персонал - выполняет ремонт отказавших технических средств, устраняет ошибки ПО АСУ [из п. 11 таблицы Приложения 1 ГОСТ 24.701-86]

2.Уязвимость структурно-функциональных элементов АС

Требования по ЗИ - конфиденциальность, целостность, доступность.

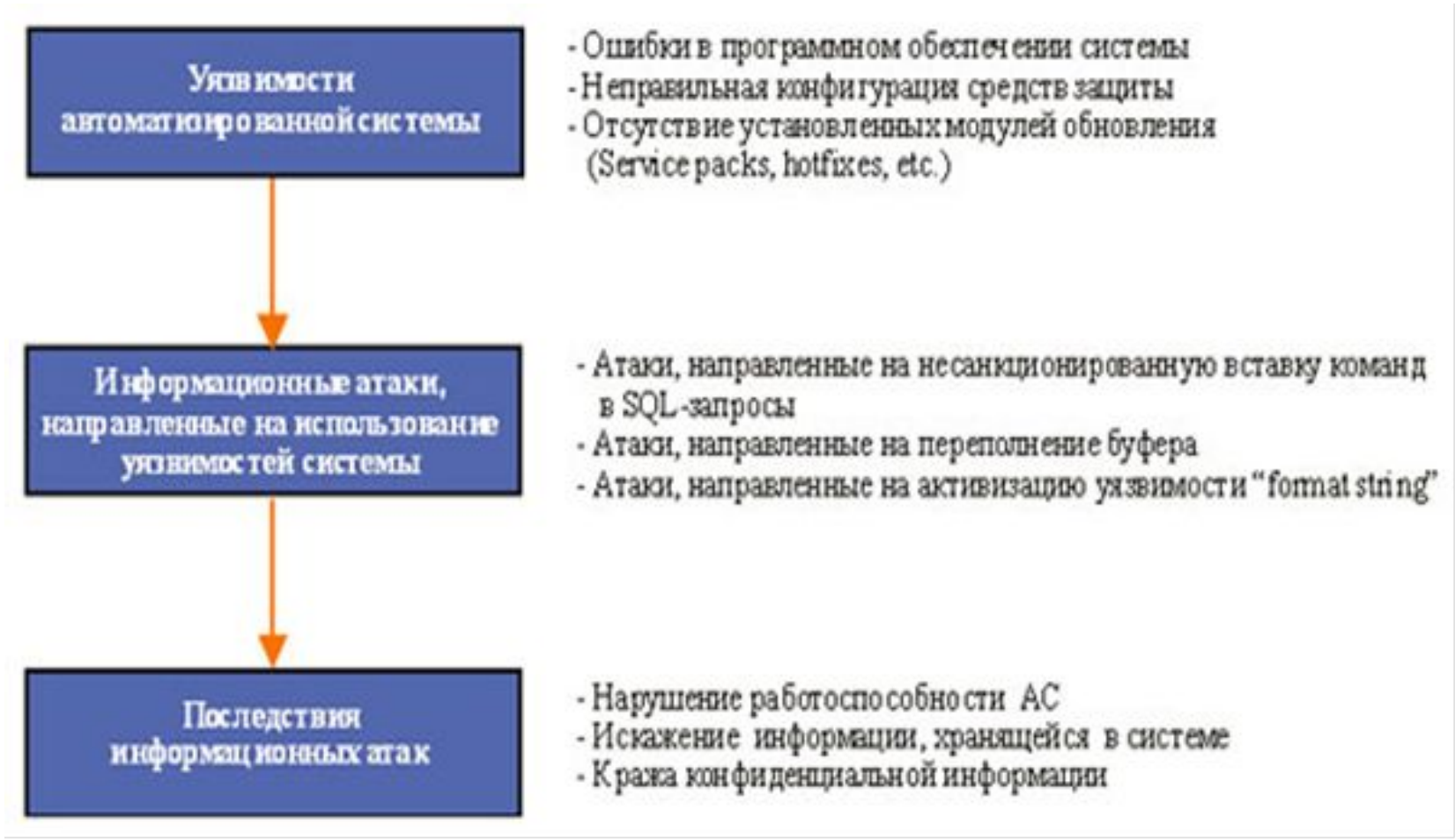
Конфиденциальность – исключение доступа посторонних лиц к информации или нераскрытие ее неполномочными лицами, логическим объектам или процессам (кража, ….).

Целостность информации - способность не подвергаться изменению или уничтожению в результате НСД .

Доступность информации - свойство быть доступной и испо-льзуемой по запросу со стороны уполномоченного пользо-вателя (СПАМ).

Итак, в результате нарушения конфиденциальности, целост-ности или доступности информации злоумышленник мо-жет нарушить бизнес-процессы

Связь уязвимости, атаки и её возможных последствий



- **Уязвимости АС могут быть внесены** как на техноло-гическом, так и на эксплуатационном этапах жизне-нного цикла АС. На технологическом этапе наруши-телями могут быть ИТР, участвующие в процессе проектирования, разработки, установки и настрой-ки программно-аппаратного обеспечения АС.
- **Внесение эксплуатационных уязвимостей** может иметь место при неправильной настройке и исполь-зовании программно-аппаратного обеспечения АС. В отличие от технологических, устранение эксплуатационных уязвимостей требует меньших усилий, поскольку для этого достаточно изменить конфигурацию АС.

Примеры уязвимостей, наличие :

- слабых, не стойких к угадыванию паролей доступа к ресурсам АС (длина и сложность пароля);
- незаблокированных встроенных учётных записей пользователей (удаление после увольнения работни-ка);
- неправильным образом установленные права досту-па пользователей к информационным ресурсам АС;
- в АС неиспользуемых, но потенциально опасных се-тевых служб и программных компонентов (удаление лишних функций);
- неправильная конфигурация средств ЗИ, приводящая к возможности проведения сетевых атак.

3.Угрозы безопасности информации, АС и субъектов информационных отношений. Основные источники угроз.

Стадии атаки:

- **Рекогносцировка**: сбор данных об объекте атаки (тип и версия ОС, список пользователей, зарегистрированных в системе, сведе-ния об используемом прикладном ПО и др. При этом в качестве объектов атак могут выступать рабочие станции пользователей, серверы, а также коммуникационное оборудование АС);
- **Вторжение в АС:** НСД к ресурсам тех узлов АС, по отношению к которым совершается атака;
- **Атакующее воздействие на АС:** направлено на достижение це-лей, ради которых предпринималась атака (нарушение работоспо-собности АС, кража КИ, хранимой в системе, удаление или моди-фикация данных системы и др., действия на удаление следов присутствия в АС);
- **Дальнейшее развитие атаки:** выполнение действий, которые направлены на продолжение атаки на ресурсы других узлов АС.

Основные виды технических средств защиты:

- средства криптографической защиты информации;
- средства разграничения доступа пользователей к ресурсам АС;
- средства межсетевого экранирования;
- средства анализа защищённости АС;
- средства обнаружения атак;
- средства антивирусной защиты;
- средства контентного анализа;
- средства защиты от спама.

Процедура входа пользователя в автоматизированную систему

Комплекс мер по ЗИ:

- меры по выявлению и устранению уязвимостей, на основе которых реализуются угрозы (позволяет иск-лючить причины возможного возникновения инфор-мационных атак);
- меры, направленные на своевременное обнаруже-ние и блокирование информационных атак;
- меры, обеспечивающие выявление и ликвидацию последствий атак (направлены на минимизацию ущерба, нанесённого в результате реализации угроз безопасности).

Основные направления обеспечения информационной безопасности

- **Нормативно-методическое обеспечение ИБ:** создание сбалансированной правовой базы в области защиты от угроз (комплекс внутрен-них нормативных документов и процедур, обеспечивающих процесс эксплуатации систе-мы ИБ: политика ИБ (руководство) ИБ организации.
- **Кадровое обеспечения ИБ**: выделение подра-зделения (службы ИБ), обучение сотрудников по вопросам противодействия информацион-ным атакам (теоретические, так и практичес-кие аспекты ИБ).

КОНЕЦ