Электронный документооборот - это взаимодействие с внешними сторонами: клиентами, контрагентами, партнёрами. Защита безопасности электронного документооборота - это элемент поддержания доверия и безопасность успешных взаимоотношений.

Соблюдение законодательства и нормативных требований является важным вопросом в обеспечении безопасности персональных данных, в том числе в рамках электронного документооборота.

Недостаточная безопасность электронного документооборота может привести к серьёзным последствиям:

- утечке конфиденциальных данных,
- нарушению доверия партнёров и клиентов,
- финансовым убыткам,
- репутационным потерям.

Риски информационной безопасности в сфере электронного документооборота:

Вот некоторые из угроз, с которыми может столкнуться электронный документооборот:

1. **DDoS-атаки**

   Атаки на инфраструктуру электронного документооборота могут привести к временной недоступности системы, что может негативно повлиять на бизнес-процессы. Кроме того, злоумышленники могут попытаться проникнуть в систему электронного документооборота, чтобы получить несанкционированный доступ к конфиденциальным данным с помощью вирусов или вредоносных программ.

2. **Фишинг и социальная инженерия**

   Атаки, направленные на пользователей, могут включать в себя попытки обмана с целью получения конфиденциальной информации, такой как пароли или персональные данные.

3. **Утечки данных**

   Недостаточная защита данных может привести к случайным или преднамеренным утечкам конфиденциальной информации. Это может нанести ущерб репутации компании и нарушить законодательство о защите данных.

4. **Недостаточная аутентификация и авторизация**

   Из-за слабой системы управления доступом к данным посторонние могут получить доступ к конфиденциальной информации или проводить операции от имени других пользователей.

5. **Нарушение целостности данных**

Изменение или подделка данных в электронных документах может создать недоверие к системе и повредить доверие сторон, участвующих в документообороте.

6. **Недостаточная надёжность шифрования**

   Отсутствие надежного шифрования может привести к тому, что конфиденциальная информация становится уязвимой для перехвата и несанкционированного доступа.

7. **Внутренние угрозы**

   Сотрудники с доступом к системе могут стать источниками угроз, если у них плохие намерения или если они недостаточно осведомлены о безопасности.

Это не полный перечень рисков, с учетом внешних и внутренних факторов он может меняться.