Вопрос 2. Угрозы безопасности: понятие и классификация.

История проблем защиты информации, представленной в цифровой форме, тесно связана с появлением технических средств ее обработки и возможностью передачи сообщений с помощью электрических сигналов и электромагнитных полей. И если в начале развития таких средств спектр угроз был связан с **защитой от технических каналов утечки информации**, то создание современных средств вычислительной техники, автоматизированных систем и в целом информатизация общества особенно с 1960-х гг. расширили диапазон угроз. Возникает проблема защиты **от несанкционированного доступа и получения информации**.

Комплексное решение вопросов безопасности называется архитектурой безопасности, которая включает: угрозы безопасности, службы безопасности и механизмы (методы) обеспечения безопасности.

Появление **сетевых технологий**, развитие глобальных компьютерных сетей, изменило характер проблем защиты, привело к распространению новых угроз безопасности.

По данным различных исследований в области компьютерных преступлений, в качестве основных опасностей информационной безопасности выделяют следующие: кража финансовых данных и подделка финансовых документов, кража критичной информации уволенными сотрудниками, саботаж сотрудников, извещенных о предстоящем увольнении, кражи переносных компьютеров и их компонентов.6

Угроза безопасности — потенциально возможное событие, действие, процесс, явление, которое может привести к нанесению материального морального и иного ущерба защищаемому объекту системы.

Классификация угроз может быть различной. Так, исследователи Гайкович В.Ю. и Ершов Д.В. все множество потенциальных угроз **по природе их возникновения** разделяют на два класса:

-естественные угрозы — угрозы, вызванные воздействиями на КИС и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека;

-искусственные угрозы — угрозы, вызванные деятельностью человека. Среди них, исходя из мотивации действий, выделяют:

— **непреднамеренные (случайные)** угрозы, вызванные ошибками в проектировании системы и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала;

— **преднамеренные (умышленные)** угрозы, связанные с корыстными устремлениями людей.

По целям, преследуемым злоумышленником (Романец Ю.В, Тимофеев П.А):

● угрозы конфиденциальности данных и программ;

● угрозы целостности данных, программ, аппаратуры;
● угрозы доступности данных;
● угрозы отказа от выполнения транзакций (действий).

Относительно объекта защиты (классификация Теплякова А.А.):
● внешние;
● внутренние.

На основе **объектов КИС,** на которые направлены угрозы (Дж.Уорленд):

-угрозы компьютерам или серверам;

— физическое вмешательство;
— заражение вредоносными программами (вирусы);
— несанкционированное внедрение в систему.

- угрозы пользователям;

— подмена персоналий;
— нарушение приватности;

- угрозы электронным документам

— нарушение целостности документа;
— искажение аутентичности отправителя документа (незаконное присвоение идентификатора, повторная передача сообщения, искажение реквизитов документа);
— непризнание участия (отказ от факта формирования документа, от получения информации или заявление ложных сведений о времени ее получения, утверждение, что получателю в определенное время была
послана информация, которая на самом деле не посылалась или посылалась в другое время).

По отношению к сети Итернет (Касперский Е.):

● **вредоносное программное обеспечение** (вирусные и троянские программы, сетевые пакеты, используемые в хакерских атаках);
● **спам,** (массовая неперсонифицированная рассылка с использованием специальных программ коммерческой, политической и иной рекламы или иного вида сообщений людям, не выразившим желания их получать);
● **глобальные сетевые атаки** (результат запланированных действий хакеров или неконтролируемого распространения сетевых вирусов-червей).