Контрольная работа 19.11.2020

- *Вопрос №1*: Аспекты угроз нарушения ИБ: **Угроза нарушения конфиденциальности.** Заключается в том, что секретная информация становится доступна лицам, у которых нет доступа к ней (у личности нет полномочий на доступ к информации). Может произойти во время передачи информации от одной ИС к другой или во время ее хранения. **Угроза нарушения целостности.** Заключается в преднамеренном изменении информации злоумышленниками во время ее хранения в ИС или передачи из одной системы в другую (данные могут быть удалены, или изменены). **Угроза нарушения доступности.** Возникает в результате преднамеренных действий злоумышленника или пользователя, из-за которых блокируется доступ к некоторому ресурсу в ИС.
- *Вопрос №2*: **Политика информационной безопасности** – это совокупность правил, процедур, практических методов и руководящих принципов в области информационной безопасности, которыми руководствуется компания или организация в своей деятельности. **Система защиты информации** — это комплекс организационных и технических мер, направленных на обеспечение ИБ предприятия. Главным объектом защиты являются данные, которые обрабатываются в автоматизированной системе управления (АСУ) и задействованы при выполнении бизнес-процессов. **Модель безопасности** - формальное выражение политики безопасности.
- *Вопрос №3*: **Авторизация** - это разграничение полномочий субъектов(пользователей) по отношению к объектам и обязательная проверка полномочий любых процессов над данными. Авторизация является вторым после идентификации / аутентификации рубежом обеспечения безопасности данных в многопользовательских ИС. **Способы аутентификации субъектов информационных систем**: **по знаниям** – некоторой информации, которая должна хранится в секрете(пароль, кодовое слово) и которую может знать только определённый субъект, **по собственности** – физическим предметам, которыми субъект владеет (смарт-карта, чип и тд), **по биометрии** - анатомическим или поведенческим характеристикам субъекта(сетчатка глаза, отпечатки, черты лица и тд), **по информации, ассоциированной с субъектом –** по его местонахождению (например через GPS).
- *Вопрос №4:* **Контролируемой зоной** - помещения или территория, в которой расположены основные и вспомогательные технические средства системы, используемые для получения доступа к защищенным данным или для проведения переговоров, инструктажей, совещаний и

т.п, которые нуждаются в особой защите. Такие помещения обязательно должны включать в себя средства технической и информационной защиты, контролируются пропускной системой. В такие помещения могут быть скрытно внедрены технические средства разведки (аппаратные закладки), которые представляют собой электронные устройства, осуществляющие перехват информации по различным техническим каналам утечки информации и ее передачу в приемные пункты технической разведки. **Опасная зона** – пространство вне КЗ, но в непосредственной близости с ней, в которой располагаются активные ТСР, посторонние проводники, с которых имеется возможность снять сигнал, случайные антенны, на которых могут наводиться информационные сигналы выше допустимого уровня.

- *Вопрос* №5: Классификация информационных ресурсов **по принадлежности**: правовая информация, научно-техническая информация, политическая информация, финансово-экономическая информация, статистическая информация и тд. **Информационные ресурсы по категориям доступа:** открытая информация, информация ограниченного доступа (гос. Тайна, конфиденциальная информация, коммерческая тайна, профессиональная тайна, служебная тайна, персональные данные). **Классификация по режиму использования**: Традиционные формы(массивы документов, архивы), автоматизированные формы (интернет, банк данных, автоматихированная информационная система, база знаний).