# Практическая работа № 4

**Тема** Анализ примеров нарушений информационной безопасности. Выявление значимых составляющих информационной безопасности и характеристик информационной системы в конкретных ситуациях

**Цель** проводить анализ нарушений информационной безопасности

**Теоретические сведения**

Информационная безопасность в самом широком смысле – это совокупность средств защиты информации от случайного или преднамеренного воздействия. Независимо от того, что лежит в основе воздействия: естественные факторы или причины искусственного характера – владелец информации несет убытки.

Принципы информационной безопасности

Целостность информационных данных означает способность информации сохранять изначальный вид и структуру как в процессе хранения, как и после неоднократной передачи. Вносить изменения, удалять или дополнять информацию вправе только владелец или пользователь с легальным доступом к данным.

Конфиденциальность – характеристика, которая указывает на необходимость ограничить доступа к информационным ресурсам для определенного круга лиц. В процессе действий и операций информация становится доступной только пользователям, который включены в информационные системы и успешно прошли идентификацию.

Доступность информационных ресурсов означает, что информация, которая находится в свободном доступе, должна предоставляться полноправным пользователям ресурсов своевременно и беспрепятственно.

Достоверность указывает на принадлежность информации доверенному лицу или владельцу, который одновременно выступает в роли источника информации.

Обеспечение и поддержка информационной безопасности включают комплекс разноплановых мер, которые предотвращают, отслеживают и устраняют несанкционированный доступ третьих лиц. Меры ИБ направлены также на защиту от повреждений, искажений, блокировки или копирования информации. Принципиально, чтобы все задачи решались одновременно, только тогда обеспечивается полноценная, надежная защита.

**Методические указания**

1. Проанализируйте данные нарушения?
2. Укажите угрозы, уязвимости и т.д.
3. Нарушение каких аспектов ИБ можно увидеть?
4. Как предотвратить потерю информации?
5. Что следует предпринять для устранения данных нарушений?

Ответ можно оформить в виде таблицы

1. Сотрудники сидят в интернете на развлекательных сайтах по 4 часа. Играют в игры на работе. Перекладывают свои обязанности на других. Сотрудники копируют конфиденциальные данные компании. Сотрудники одновременно работают на другой работе. Сотрудники работают на конкурента. Сотрудник хочет создать собственную конкурентную компанию. Сотрудники распространяют государственную тайну.
2. Используется потенциальное опасное ПО, содержащее уязвимости, позволяющие скрытую передачу данных, дающие возможность деструктивного влияния на ИТ инфраструктуру компании. Выясняется, что административные пароли передаются по открытым каналам. Сотрудники используют средства удаленного управления. Администраторы сделали бреши в межсетевом периметре компании для удобства. Оставлены закладки в самописном программном обеспечении.

**Контрольные вопросы**

1. Что называют информационной безопасностью?
2. Какие составляющие информационной безопасности должны быть соблюдены?
3. Что будет если одна из составляющих информационной безопасности будет нарушена?