Задание 1

Вопрос 1

Примечание: в каждой категории может быть несколько объектов (более одного).

Охраняемая территория
Территория перед окнами офиса, выходящими на парковку и улицу. Данная территория не является контролируемой зоной организации, но напрямую прилегает к критичным объектам (окнам офиса). Это создает риски съема информации с мониторов, съема акустической информации через стекла, а также наблюдения за режимом работы и передвижениями ключевых сотрудников.
Здания, сооружения, помещения, сейфы
1. Офис организации. 2. Помещение отдела программирования. 3. Серверная. 4. Конференц-зал для совещаний. 5. Помещения отдела кадров и бухгалтерии. 6. Сейф генерального директора.
Информационные системы
1. Информационная система персональных данных (ИСПДн) «Зарплата и кадры». 2. Рабочие станции отдела программирования. 3. Автоматизированные рабочие места (АРМ) отдела кадров и бухгалтерии. 4. Компьютер отдела закупок, используемый для работы с ГИС «Торги». 5. Корпоративная локальная вычислительная сеть (ЛВС) организации.
Объекты информатизации, носители информации
1. USB-накопители с грифом «Коммерческая тайна» (с программным кодом BIOS). 2. Жесткие диски и твердотельные накопители (SSD) серверов и рабочих станций, обрабатывающих КТ и Пдн.

3. Резервные копии информационных систем (ИСПДн, исходного кода). 4. Архивы документов, содержащих коммерческую тайну и персональные данные.
Помещения для обсуждения конфиденциальной информации
Специально оборудованный конференц-зал.
Конфиденциальная информация, тайна, секрет производства, а также сотрудники, ознакомленные с конфиденциальной информацией
1. Секрет производства - исходный программный код, используемый для прошивки BIOS. 2. Коммерческая тайна (КТ) — техническая, деловая информация (алгоритмы, архитектура, спецификации, патенты, планы разработки, стратегии и т.д.) 3. Персональные данные (Пдн) - сведения о сотрудниках, обрабатываемые в ИСПДн «Зарплата и кадры» (состав сведений определяется в соответствии с 152-ФЗ). 4. Сотрудники, допущенные к конфиденциальной информации - сотрудники отдела программирования (допущены к КТ), сотрудники отдела кадров и бухгалтерии (допущены к ПД).

Вопрос 2

Примечание: для каждой техники может быть несколько способов реализации (более одного).

В чём заключается? (способ реализации)	**Цель применения**
Физическая защита	
Установка систем контроля и управления доступом (СКУД)	Не допустить физическое проникновение к компьютерам для их вскрытия.
Использование замков на корпусах системных блоков.	Заблокировать физический доступ к жестким дискам внутри компьютера.
Крепление компьютеров к столам/стойкам специальными замками (Kensington lock).	Затруднить хищение всего системного блока.

Техническая защита	
Настройка пароля на BIOS/UEFI и запрет загрузки с внешних устройств (USB, CD/DVD).	Заблокировать возможность загрузки нештатной операционной системы с постороннего носителя.
Включение функции Secure Boot в настройках UEFI.	Обеспечить загрузку только подписанной, доверенной операционной системы, блокируя неавторизованные ОС.
Аппаратное отключение портов (USB, SATA) на материнских платах критичных компьютеров.	Физически предотвратить подключение загрузочной флешки или другого жесткого диска.
Криптографическая защита	
Внедрение полного шифрования диска	Сделать данные на диске нечитаемыми при его извлечении и подключении к другому компьютеру. Защищает от кражи самих данных.
Использование аппаратных модулей TPM для безопасного хранения ключей шифрования.	Защитить ключи шифрования от извлечения и компрометации, повысив стойкость шифрования диска.
Обязательная строгая парольная политика (сложные пароли, регулярная смена) для доступа к операционной системе и расшифровки диска.	Не дать злоумышленнику подобрать пароль для доступа к зашифрованным данным.
Правовая защита, организационные меры	
Заполнять не нужно. Для каждой организации это политика безопасности, разработка регламентов, инструкций, приказов, регулирующих отношения субъектов по защите информации, применение этих документов (актов). Будет меняться только содержание данных документов	