*Задание 1. Разобрать кейс и дать развернутые аргументированные ответы на поставленные вопросы.*

На производстве было похищено дорогостоящее оборудование.

Его погрузили в ковш погрузчика и вывезли за территорию завода. На записи с камер видеонаблюдения было видно, как погрузчик подъехал к забору, в котором была заранее проделана дыра, а потом вернулся с пустым ковшом. Сам момент выемки похищенного из ковша на запись не попал, так как именно в этом месте обзор камерам слежения закрывал контейнер с отходами.

Водитель погрузчика свою вину отрицал, вел себя агрессивно, угрожал обращением в полицию и в суд с жалобами на оказываемое на него давление. Прямых доказательств вины не было, сотрудник был отпущен. Руководство требовало немедленно найти похищенное, так как оно содержало конфиденциальную информацию о структурном составе производимого на заводе продукта. Уже на следующий день по окончании работы подозреваемый в краже был задержан на проходной. В его шкафчике с рабочей одеждой были найдены конфиденциальные документы, принадлежащее его коллеге-конструктору. К данным документам подозреваемый не имел доступа по своим служебным обязанностям и функционалу.

Камеры в раздевалке оказались отключены, но три свидетеля готовы были подтвердить, что видели, как подозреваемый брал данные документы. Полицию не вызывали, похищенное днем ранее оборудование в течение двух часов было возвращено предприятию, сотрудник был немедленно уволен по соглашению сторон.

*Вопросы для решения:*

1. *Определите основную проблему кейса.*
2. *Какие ошибки были допущены руководителем завода?*
3. *Какие причины способствовали наличию ошибок?*
4. *Какие действия или мероприятия необходимо произвести, чтобы исправить сложившееся положение дел?*
5. *Какие дополнительные доработки помогли бы не допустить обозначенные ошибки?*

*Задание 2.*

1. Объясните понятия «политика безопасности компании» и «информационная безопасность», а также установите взаимосвязь данных понятий.
2. Дайте типовую структуру политики информационной безопасности. Обоснуйте свою точку зрения. Укажите, какие различия могут присутствовать в различных компаниях в контексте структуры и содержания политики информационной безопасности.
3. Укажите, какие функции руководства необходимо указывать в политике информационной безопасности. Поясните свой ответ.

*Задание 3.*

1. Составьте план мероприятий по проведению аудита информационной безопасности в компании (в качестве базы можно опираться на пример любой компании). Обоснуйте свою точку зрения.
2. Укажите, какой персонал будет задействован в составленном плане и почему необходимо задействовать выбранный вами персонал.

Литература

1. Информационная безопасность и защита информации: учеб. пособие для вузов / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова, Н.Г. Шахов. - Старый Оскол: ТНТ, 2015. – 383 с.
2. Управление персоналом: теория и практика. Кадровая политика и стратегия управления персоналом: учебно-практическое пособие для вузов / А.Я. Кибанов, Л.В. Ивановская; под ред. А.Я. Кибанова. – М.: Проспект, 2014. – 60 с.
3. Алавердов А.Р. Управление кадровой безопасностью организации: учебник. – М.: Маркет ДС, 2010.
4. Самоукина Н.В. Незаменимый сотрудник и кадровая безопасность. – М.: Вершина, 2008.
5. Грабс-Уэст Л. Сотрудники на всю жизнь. Уроки лояльности от Southwest Airlines. – М.: Манн, Иванов и Фербер, 2010.
6. Уэллс Дж.Т. Справочник по предупреждению и выявлению корпоративного мошенничества. – М. Инфра-М, 2011.
7. Шепард Г. Как управлять проблемными сотрудниками. – М.: Добрая книга, 2007.
8. Любавская Л.М., Беляйкин Д.В. Кадровая безопасность как фактор конкурентоспособности в сфере банковского предпринимательства: учеб. пос. – Новосибирск: НФ РГТЭУ, 2010.