1) В данном случае работники теряют своё время на работу, а также имеют риск поймать вирусы, сидя на разных сайтах.

Перекладывая свои обязанности на других, они усложняют работу другим, по итогу не делая ничего, такие работники не приносят никакой пользы в компанию.

Копирование конфиденциальной информации - прямое нарушение 2-ух аспектов Информационной Безопасности - целости и конфиденциальности.

Если сотрудник работает на конкурента или пытается создать конкурентную компанию, то он сможет и будет брать как можно больше информации из данной компании, что не сулит ничего хорошего.

Распространение государственной тайны уголовно наказуем

Чтобы предотвратить потерю информации нужно:

1. делать хороший отбор сотрудников
2. заблокировать на компьютерах доступ к посторонним сайтом и конфиденциальной информации.

Для устранения нарушений необходимо уволить сотрудников

2) Использование любого несанкционированного ПО - нарушение Информационной Безопасности

Передача паролей также является одним из нарушений Информационной Безопасности - нарушение конфиденциальности.

То, что администраторы сделали бреши для удобства может оказаться удобством для взлома злоумышленникам.

Любое самописная закладка должна быть запрещена, даже если она безопасная, потому что это недопустима, а также это закладка может быть проводником ко всей информации.

Для предотвращения и устранения этого нужно:

* Блокировать посторонние ПО
* Блокировать передачу конфиденциальной информации
* Применить различные наказа ния для сотрудников

Для предотвращения этого нужно:

1. Блокировать посторонние ПО
2. Блокировать передачу конфиденциальной информации
3. Наказывать работников разносящих секретную информацию

Контрольные вопросы:

1. Информационная Безопасность- это совокупность средств защиты информации от случайного или преднамеренного воздействия.

2. Целостность, конфиденциальность, доступность

3. Владелец информации понесет убытки