Курсовая работа на тему:

Совершенствование системы информационной безопасности в отделе продаж АО "Себряковцемент"

Выполнил: Вишняков К.А.
Преподаватель: Калашников В.Ю.

Цели и задачи:

- **Цель курсовой работы**: совершенствование системы информационной безопасности в отделе продаж АО «Себряковский цементный завод».
- **Задачи:**
- проанализировать состояние системы информационной безопасности;
- ознакомится с организационной структурой;
- проанализировать состав информационных ресурсов предприятия;
- выявить недостатки в системе защиты информации;
- предложить мероприятия по совершенствованию систему информационной безопасности;
- оценить эффективность предложенных мер;
- составить модель информационной системы

с позиции безопасности.

Характеристика предприятия

Служба по вопросам защиты информации

В АО «Себряковский цементный завод» за безопасность информации отвечает инженерно-технический отдел. В штате отдела имеется инженер по информационной безопасности, который включен в штатное расписание данного отдела.

Анализ и характеристика информационных ресурсов отдела

В отделе продаж АО «Себряковский цементный завод» хранятся и обрабатываются сведения, относящиеся к коммерческой тайне. Защищаемые сведения хранятся в базах данных 1С: Предприятие на сервере.

Угрозы информационной безопасности характерные для отдела

- отсутствие контроля нахождения в помещении посторонних лиц;
- разглашение сведений, относящихся к коммерческой тайне.

Методы и средства защиты информации на предприятии:

- Препятствие – метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.д.).
- Принуждение – метод защиты, при котором пользователи и персонал ИС вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.
- Побуждение – метод защиты, побуждающий пользователей и персонал ИС не нарушать установленные порядки за счет соблюдения сложившихся моральных и этических норм.

Недостатки в системе защиты информации:

- однообразность паролей доступа в систему;
- отсутствие паролей при работе программой с 1С: Предприятие, при изменении данных;
- отсутствует дополнительная защита файлов и информации;
- нерегулярное обновление баз программы антивируса и сканирование рабочих станций;
- большое количество документов на бумажных носителях в основном лежат в папках (иногда и без них) на рабочем столе сотрудника, что позволяет злоумышленникам без труда воспользоваться этим в своих целях;
- не производится регулярное обсуждение вопросов информационной безопасности на предприятии и возникающих проблем в этой области;
- не организована регулярная проверка работоспособности информационных систем;
- отсутствие политики информационной безопасности;
- отсутствие системного администратора;
- отсутствие средств предотвращения нанесения ущерба от стихийных природных явлений;
- кабинет с сервером легкодоступен;
- отсутствие видеонаблюдения.

Цель и задачи системы информационной безопасности

Цели системы безопасности отдела продаж АО «Себряковский цементный завод»:

- предотвращение ущерба ее деятельности за счет хищения финансовых и материально-технических средств;
- уничтожения имущества и ценностей;
- разглашения, утечки и несанкционированного доступа к источникам конфиденциальной информации;
- нарушения работы технических средств обеспечения производственной деятельности, включая и средства информатизации.

Задачи системы информационной безопасности:

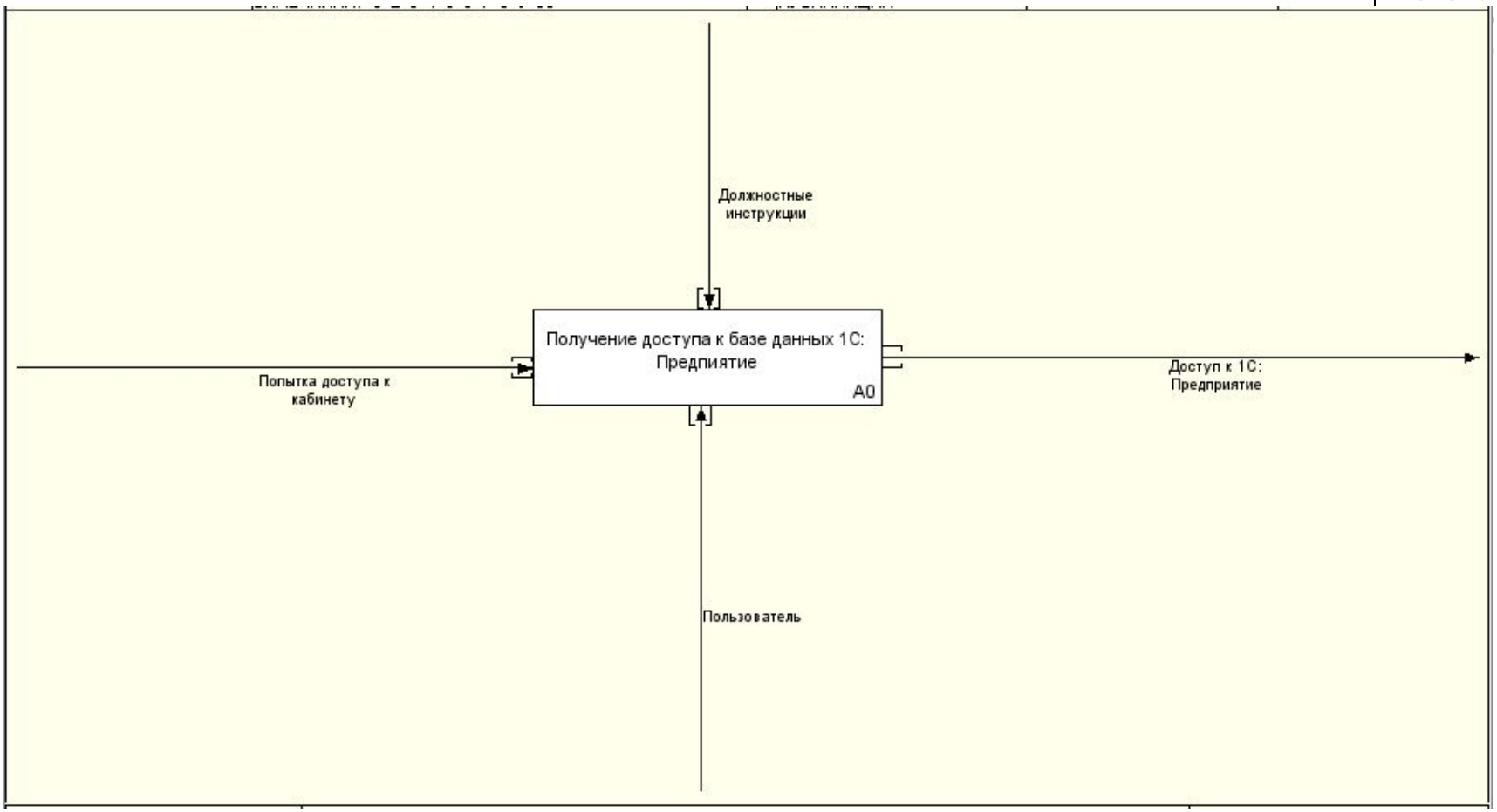
- обеспечить защиту от вмешательства в процесс функционирования предприятия посторонних лиц;
- обеспечить защиту от несанкционированных действий с информационными ресурсами предприятия посторонних лиц и сотрудников, не имеющих соответствующих полномочий;
- обеспечить физическую сохранность технических средств и программного обеспечения предприятия и защитить их от действия техногенных и стихийных источников угроз;
- создать и сформировать целенаправленную политику безопасности информации предприятия.

Мероприятия и средства по совершенствованию системы информационной безопасности

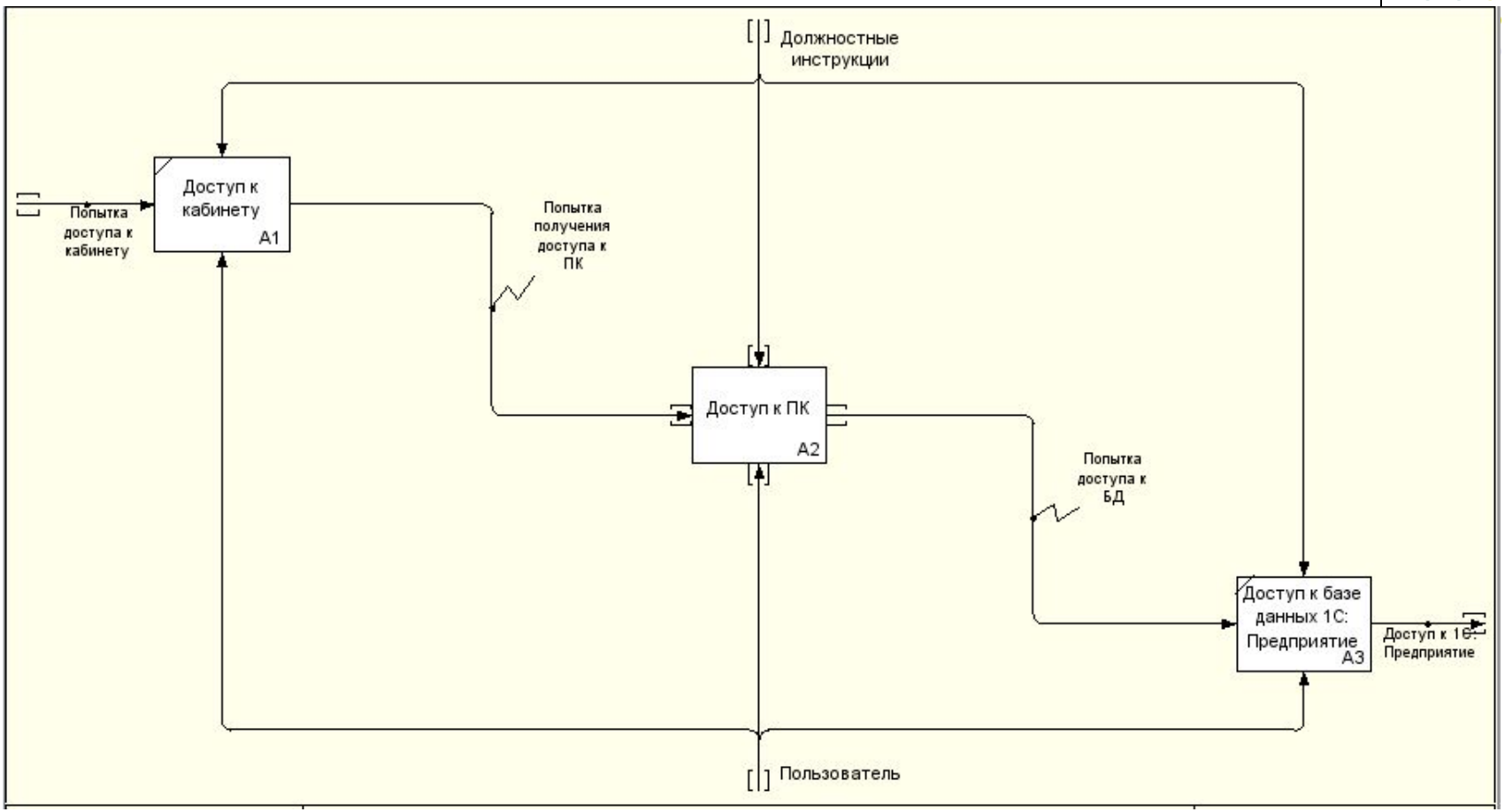
- организация работ по обучению персонала навыкам работы с новыми программными продуктами при участии квалифицированных специалистов;
- строгий контроль соблюдения сотрудниками правил работы с конфиденциальной информацией;
- контроль соблюдения правил хранения рабочей документации сотрудников предприятия;
- плановое проведение собраний, семинаров, обсуждений по вопросам информационной безопасности предприятия;
- регулярная (плановая) проверка и обслуживание всех информационных систем и информационной инфраструктуры на работоспособность.
- введение паролей пользователей;
- регулярное сканирование рабочих станций и обновление баз антивирусной программы;
- установка сейфов и шкафов для хранения информации на бумажных носителях;
- установка огнетушителей, систем пожарного оповещения и громоотводов.

Эффективность предложенных мероприятий

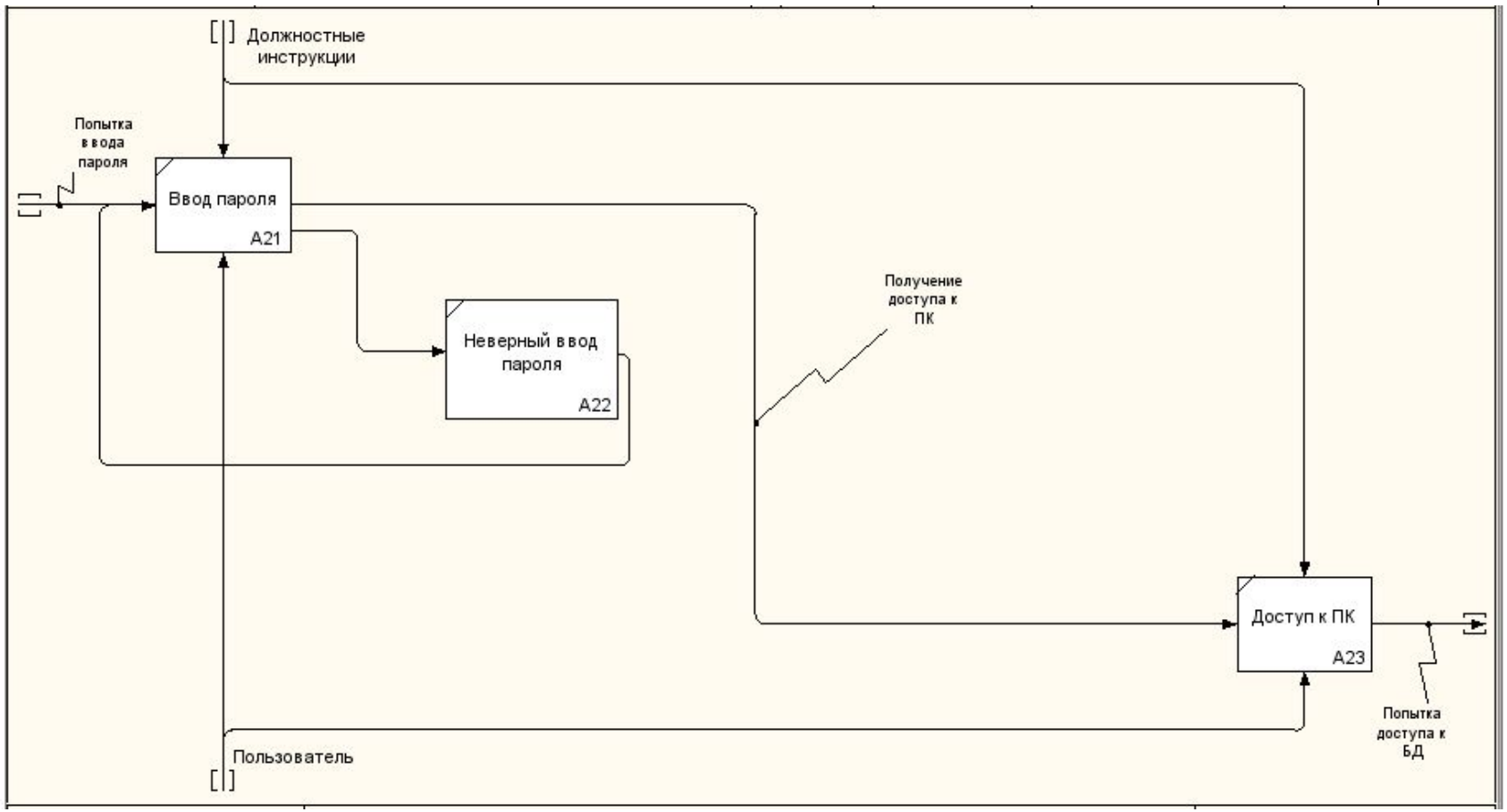
- уменьшить вероятность утери, удаления или изменения информации;
- повысить уровень доступа к серверной комнате;
- разработать и внедрить политику информационной безопасности, которая будет направлена на защиту информации и ассоциированных с ней ресурсов;
- повысить уровень защиты рабочих станций;
- повысить уровень защиты от пожаров.



Получение доступа к БД



Получение доступа к БД (2 уровень)



Получение доступа к ПК

Выводы по курсовой работе