ТЕМА ИССЛЕДОВАНИЯ:
РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ АНАЛИЗА И КОНТРОЛЯ РИСКОВ ИБ АИС

Выполнил: студент 957ом группы Ложкова А.А

Научный руководитель: Самохвалова С.Г. доцент, к.т.н

Статистика инцидентов информационной безопасности

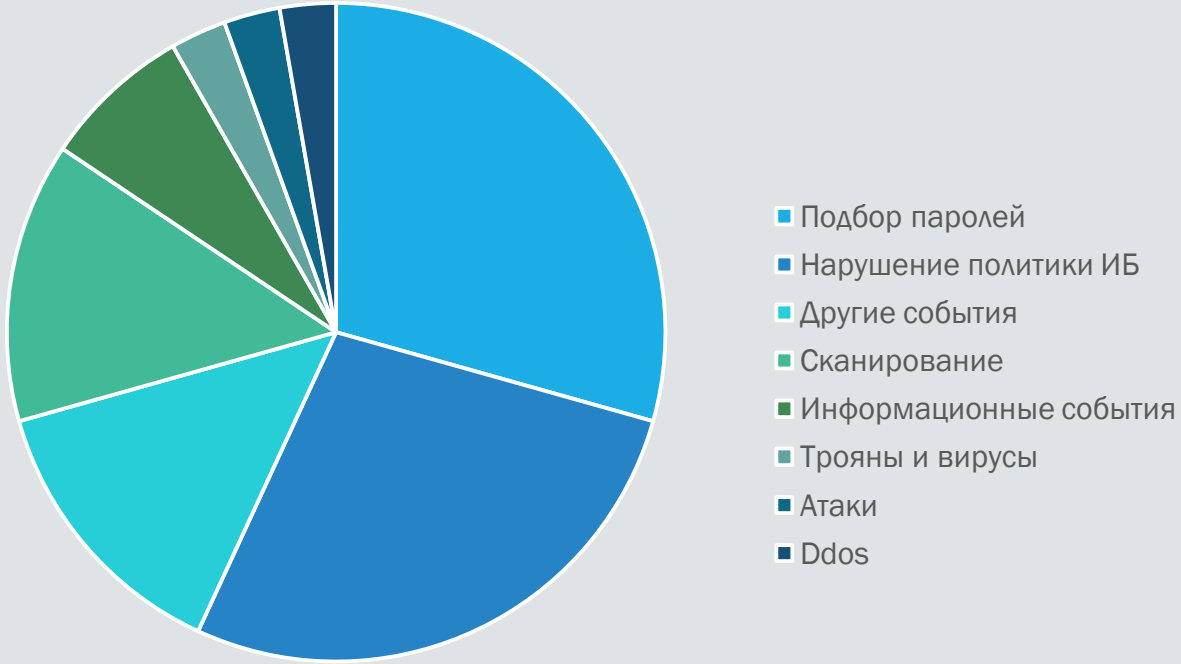


Рисунок 1 – Типы зарегистрированных событий

Статистика инцидентов информационной безопасности

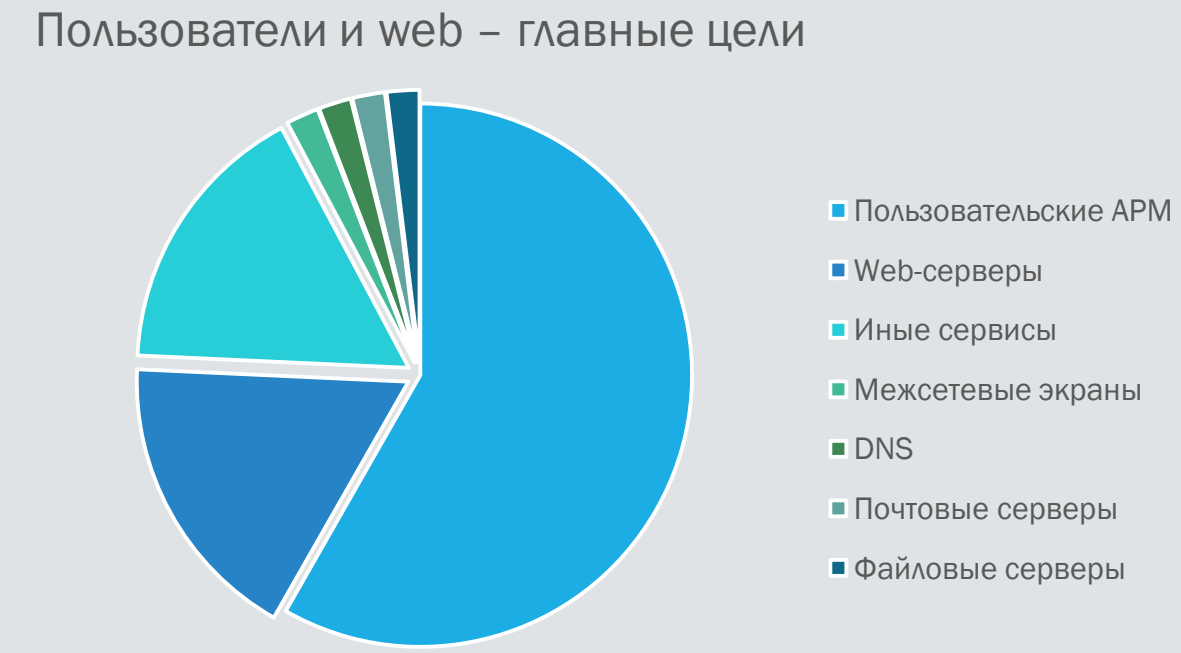
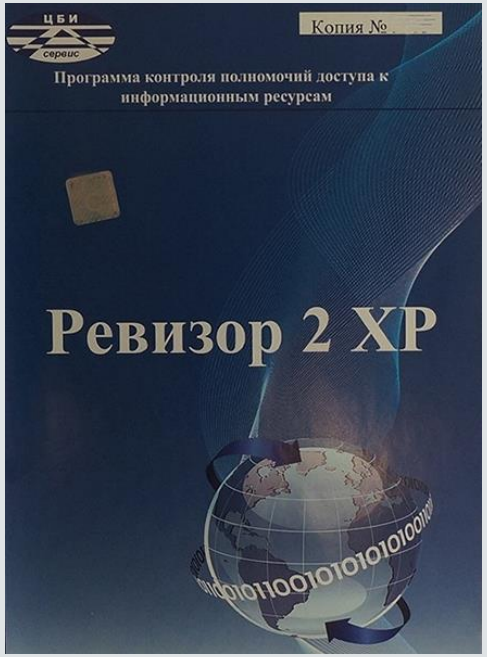


Рисунок 2 – Сегменты, подверженные инцидентам

Наиболее часто подвергаются нежелательному воздействию именно пользовательские АРМ. Это 60% от всех инцидентов на контролируемые ресурсы. На втором месте расположились атаки на web-серверы и иные сервисы.

Сравнительный анализ существующих программных средств



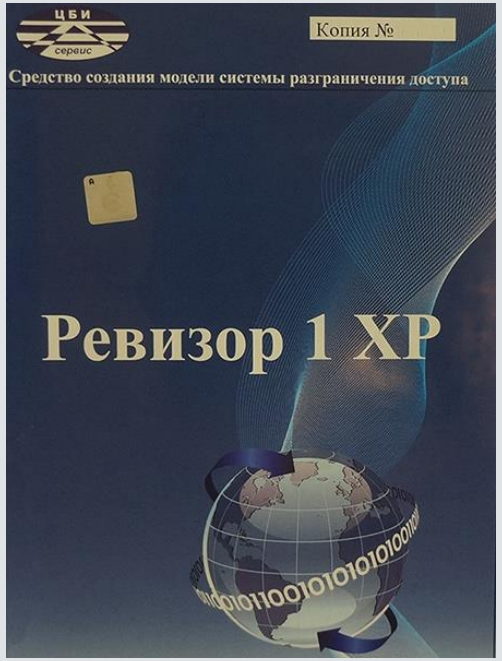


Рисунок 3 –Средства контроля защищенности от НСД

Анализ информационных ресурсов предприятия

Информационный ресурс	Общедоступная информация / Информация ограниченного доступа	Сотрудники каких подразделений допущены к информации	В каких помещениях предприятия обрабатывается (хранится) информация	На каких носителях распространяется (хранится) информация
Информация о закупках	Общедоступная	Нет ограничений	Отдел информационных технологий Бухгалтерский отдел	Бумажные Магнитные Оптические
Рабочие документы	Ограниченного характера	Циркулируют между всеми отделами	Циркулируют между всеми отделами	Бумажные
Сведения, составляющие государственную тайну	Ограничительного характера	Мобилизационный сектор	Режимно-секретное подразделение	Бумажные

Таблица 1 – Неполный список информационных ресурсов предприятия

Всю обрабатываемую на предприятии информацию необходимо разделить на общедоступную информацию, доступ к которой неограничен и предоставляется всем без исключения, и информацию, доступ к которой ограничен федеральными законами и регламентом предприятия.

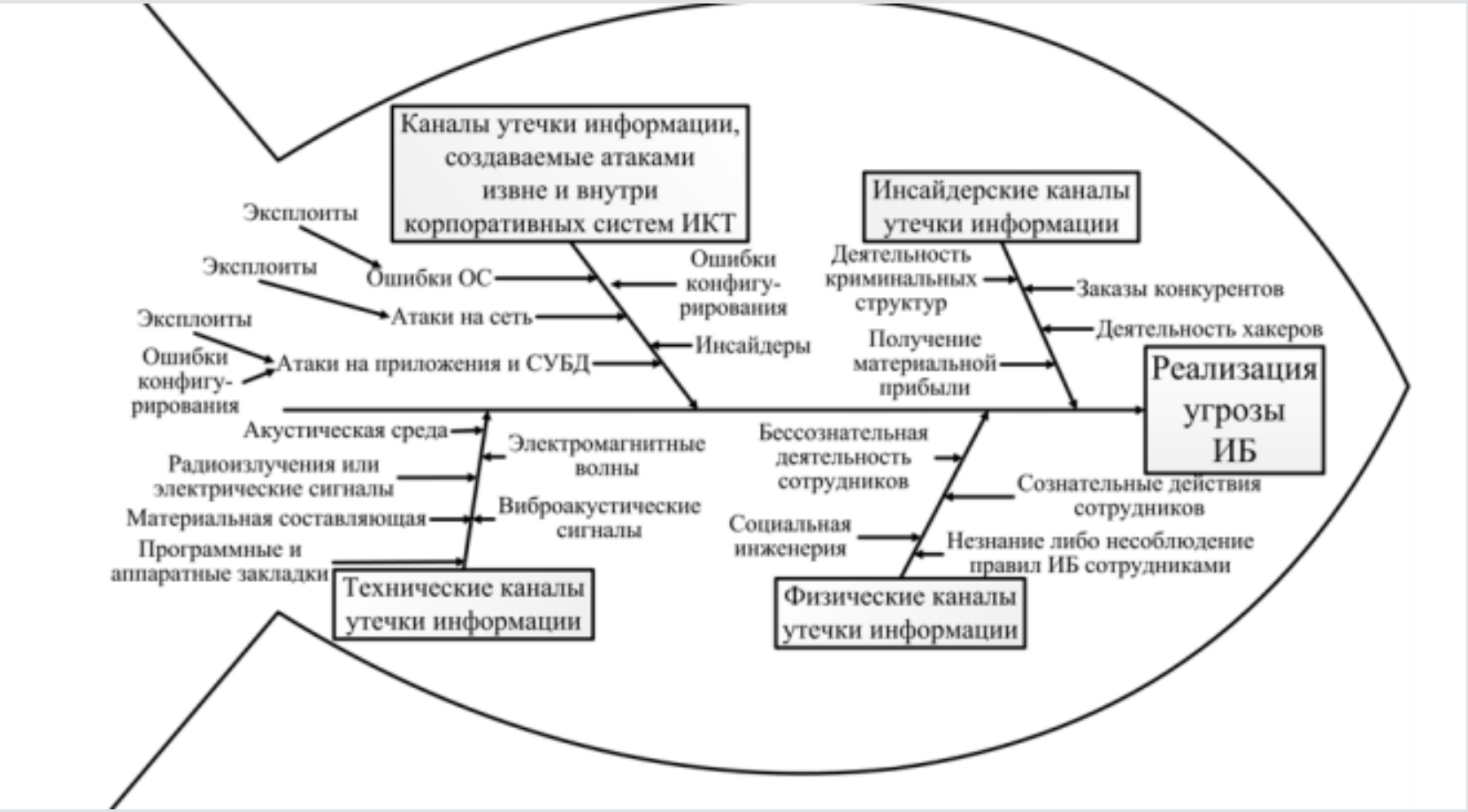


Рисунок 4 – Схема причинно-следственных связей

В результате анализа возможных угроз информационной безопасности предприятия и каналов утечки информации формируется схема причинно-следственных связей. Диаграмма позволяет определить главные факторы, оказывающие наиболее сильное влияние на снижение уровня информационной безопасности.

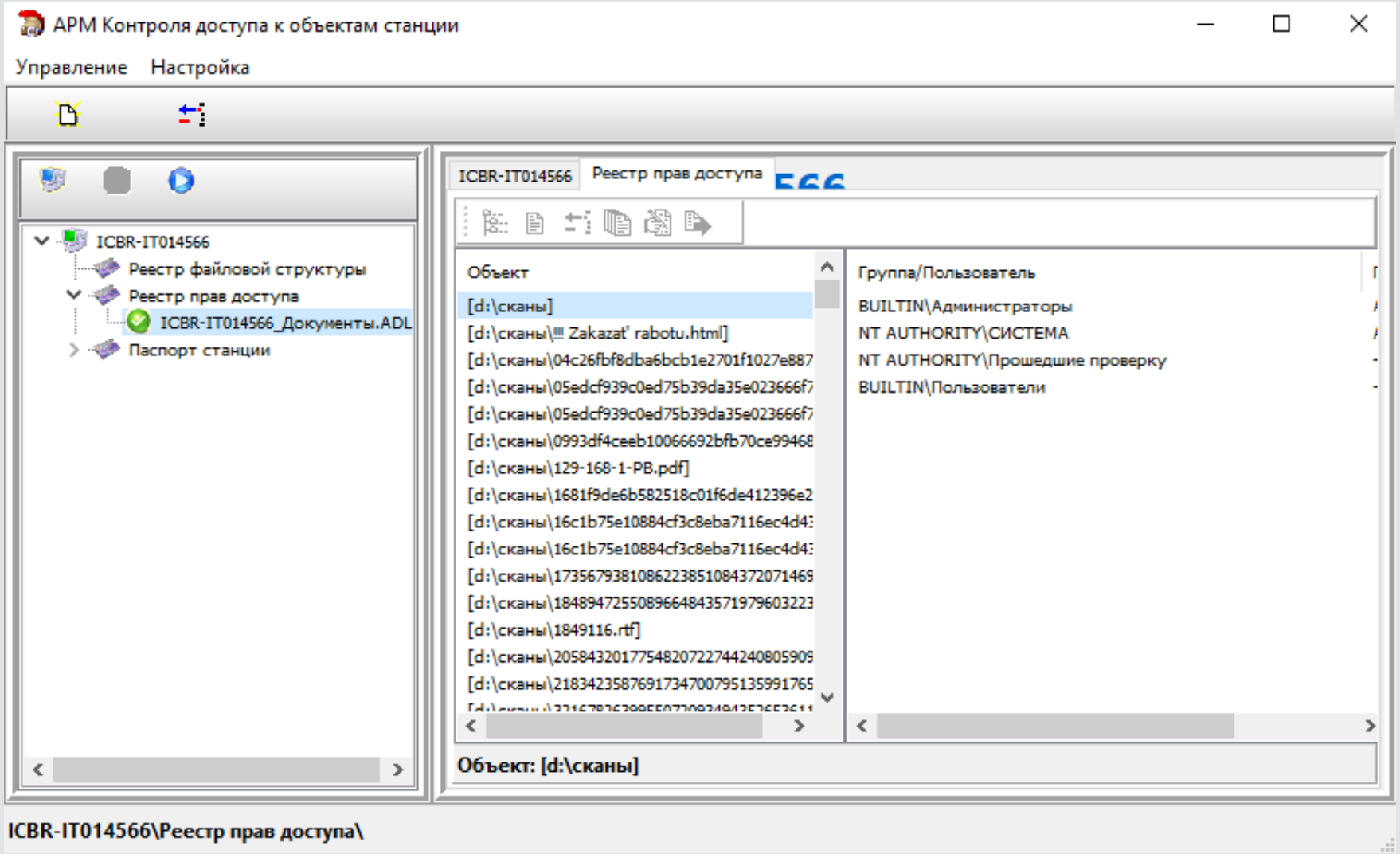


Рисунок 5 – Средство контроля доступа к объектам станций

Заключение

Проведен анализ угроз и каналов утечки информации предприятия, занимающегося научно-исследовательской и производственной деятельностью. По результатам анализа построены диаграмма Исикавы, отражающая влияние различных факторов на информационную безопасность предприятия, и модель угроз информационной безопасности, описывающая источники возможных угроз информационной безопасности, каналы утечки и компоненты системы защиты информации на предприятии. В ходе работы были проанализированы информационные ресурсы предприятия, сформирован перечень информации ограниченного доступа, проведен анализ информационных потоков предприятия.

Считаю, что тема обеспечения информационной безопасности на предприятиях является актуальной в настоящее время.