Дементьев Н.А.
Научный руководитель: Р. А. Штыков
Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»
602264, г. Муром, Владимирская обл., ул. Орловская, 23
nik.dementev1996@mail.ru

Организация защиты информации отдела производства промышленного предприятия

Последние годы наблюдается тенденция повсеместной информатизации. Цифровые устройства встречаются на каждом шагу: домашние компьютеры, компьютеризированные кассы в магазине, рабочие станции сотрудников различных профессий на производствах и многое другое. В данном случае была выбрана сфера деятельности: отдел производства промышленного предприятия, которое занимается изготовлением и выпуском продукции на котором необходимо обеспечить безопасную передачу информации.

С целю организации защиты необходимо рассмотреть угрозы, которые могут быть созданы относительно применяемой информационной системы:

- «Получение учетной записи пользователя»
- «Получение персональных данных заказчиков»
- «Захват сведений об оформленных заказах»
- Получение платежных документов с данными заказчика

Современные системы электронного документооборота стали разрабатываться с массовым появлением доступа в сеть интернет.

Основные требования, которым должна соответствовать система электронного документооборота:

- «Надежное хранение и удобный поиск документации»
- «Своевременный контроль за исполнением документов и их маршрутизация»
- «Создание аналитических отчетов»
- «Обеспечение информационной безопасности»

Наиболее оптимальным решением в данной ситуации является разработка собственной информационной системы, которая бы позволяла решать задачи по обеспечению информационной безопасности при учете и обработке поступающих заказов.

В ходе анализа были выявлены возможные угрозы и необходимо выявить решения для защиты этой информации.

Первая угроза заключается в хищении учетной записи пользователя. Наиболее надежным является применение ключевых носителей, которые должны всегда находиться у пользователя и в случае компрометации ключа применять административные меры в отношении владельца учетной записи и администратор закрывает доступ к этой учетной записи.

Второй и третьей угрозой является получение текстовой информации из базы данных в случае получения прямого доступа к ней. Для того, чтобы защитить данные наиболее оптимальным решением является шифрование данных одним из криптографических алгоритмов.

Последней угрозой является получение платежных документов, которые хранятся в виде сканированных образов документов. В данном случае удобно применять файловое шифрование, ключ от которого будет генерироваться лишь клиентским приложением на лету.

В итоге были проанализированы угрозы для данной системы и основные потоки информации, так же удалось выявить решения для защиты этой информации и данной системы.