# Анализ политики безопасности предприятия ООО «Ромашка»

Павел Смоляков, гр. 21214

21 декабря 2023 г.

## 1 Введение

Данная работа представляет собой анализ политики безопасности предприятия ООО «Ромашка». Анализ будет производиться по главам, в соответствующем порядке.

## 2 Глава “Политика информационной безопасности”

В данном разделе описывается общий подход к обеспечению информационном безопасности, используемый в ООО «Ромашка». В целом, на абстрактном уровне упомянуты решения для осуществления защиты от большей части возможных внешних и внутренних угроз. Впрочем, часть пунктов можно подвергнуть критике за недостаточную конкретность:

1. упомянут “механизм оперативного реагирования”, однако нет никаких уточнений по поводу, собственно, оперативности этого реагирования. Может пройти час, неделя, месяц? А может в зависимости от важности и секретности информации прошедшее время может вариироваться?

2. “периодический контроль корректности действий ...”, опять же, не указан период, аналогично предыдущему пункту.

3. “контроль корректности ...”, “контроль целостности ...” - в данных пунктах никак не указан способ контроля. Автоматический (путем использования специализированного ПО)? Ручной? Смешанный?

Было бы уместным предположить, что данные пункты более подробно раскрываются в следующих разделах документа, однако это актуально лишь для пункта 3.

## 3 Глава “Реализация политики информационной безопасности”

По данной главе отсутствуют комментарии.

# 4 Глава “Методология и принципы построения политики безопасности”

В данном разделе описываются, в том числе, принципы построения политики безопасности. Набор принципов весьма всеобъемлющий и их описание исчерпывающе; впрочем, в модели безопасности использовался термин “уязвимость”, который, на мой взгляд, мог бы быть определен более полно. Помимо предложенных вариантов, это также состояние системы, которое позволяет, как минимум:

1. лишить доступа к информации иных пользователей
2. изменять настройки доступа к информации
3. использовать ресурсы предприятия для получения доступа к приватной информации, принадлежащей другим предприятиям

.

# 5 Глава “Угрозы информационной безопасности ЕСЭДО, методы и средства”

В данном разделе описана уже более прикладная информация. К сожалению, не обошлось без недоработок. В частности:

1. Страница 12, п. 4.2.2., “организация контроля за работой пользователей”. По тексту ранее упоминались системные администраторы, как отдельная группа лиц; системный администратор как один из источников внутренних угроз также должен быть проконтроллирован.
2. Страница 13, п. 4.2.3.1., “Монитор следует располагать таким образом, чтобы исключить возможность просмотра содержимого экрана посторонними лицами...”. Также была бы не лишней возможность оперативного отключения монитора.
3. Страница 14, п. 4.2.3.1., “Должен использоваться паролируемый хранитель экрана.”. В идеале, компьютер сам должен переводиться в режим хранителя экрана спустя небольшое время (скажем, не более 2 минут).
4. Страница 15, п. 4.2.3.5., “Должны быть рассмотрены следующие рекомендации по защите носителей информации, транспортируемых между территориями...”. Нет пункта, рекомендующего производить верификацию информации, находящейся на носителе, по прибытии в пункт назначения. Например, это может быть механизм ЭЦП.
5. Страница 16, п. 4.2.3.6., “защиту системы от наличия и появления нежелательной информации”. Каков механизм реагирования, если нежелательная информация все же появилась?
6. Страница 17, п. 4.2.3.9., “Средства управления для борьбы со злонамеренными программными кодами”. Не хватает пункта, к примеру, об отключении от сети заражённого компьютера для предотвращения распространения вируса.

# 6 Заключение

Большая часть документа содержит в себе скорее общие рекомендации, по причине чего иногда не хватает технических подробностей, как в уже приведенных примерах.