Проанализировав политику безопасности предприятия ООО «Ромашка», можно выделить следующие положительные и негативные стороны принятой политики информационной безопасности.

Принятие решений о разделении обязанностей сотрудников по ролям и следовании принципа минимальных привилегий для каждой роли позволяет минимизировать возможный ущерб, что обеспечивает большую устойчивость системы к угрозам, появляющихся после компрометации средств получения доступа к защищаемой системе.

К недостаткам или недостаточной точности политики по обеспечению физической безопасности можно отнести отсутствие точного указания периодичности проверки систем, обеспечивающих физическую безопасность. Указывается только наличие обслуживающего персонала. Отсутствие данной информации может привести к деградации защитных качеств средств, обеспечивающих безопасность, и выводу её из строя.

Также возникают вопросы к требованиям носителей информации для транспортировки. Указывается пункт, что носитель должен быть устойчив к любым факторам окружающей среды, которые могут уменьшить эффективность восстановления данных. Таким образом указывается, что целостность информации может быть восстановлена. Данное замечание указывает на возможность появления ситуации, когда нарушители могут восстановить информацию из скомпрометированного носителя, что противоречит целям политики информационной безопасности. Должно использоваться средство, которое позволяет гарантировать сохранение целостности, доступности и конфиденциальности передаваемой информации во время транспортировки. При нарушении хотя бы 1 пункта вся информация на носителе должна быть утеряна без возможности восстановления.

Ещё хотелось бы отметить не совсем ясное требование к защите файлов, дисков и каталогов путем их вакцинирования. Мне не известны средства, которые могут реализовать данное требование. Могу предложить использование внедрения «канарейки» в файл с чувствительной информацией, создание и установку «HoneyPot» системы. Данные способы позволяют реагировать на компрометацию файла и узнавать о проведении атаки в кратчайшие сроки, что должно положительно повлиять на защиту информационной системы предприятия.

Не могу не упомянуть критерии классификации злонамеренного кода от мистификации. Использование журналов, «имеющих хорошую репутацию» и «надежных» сайтов сети Интернет в качестве квалифицированных источников считаю должно происходить с максимальной осторожностью, так как невозможно определить в полной мере достоверность предоставляемой информации, и не исключены ситуации, когда эти источники могут быть скомпрометированы и выступать в роли распространителей вредоносного программного обеспечения.

Мной были указаны все достоинства и недостатки выбранной политики информационной безопасности предприятия ООО «Ромашка», заслуживающие упоминания.