В данном разделе будут представлены варианты противодействия рискам и угрозам, которые были выявлены на предприятии в предыдущих разделах работы.

Для экономической безопасности:

- Увеличение долговой нагрузки:
  - Разработать стратегию сокращения долговой нагрузки, уделяя первоочередное внимание краткосрочным обязательствам.
  - Привлечь инвестиции или субсидии для стабилизации финансового положения.
  - Оптимизировать производственные процессы для повышения эффективности.
- Риск ухудшения оборачиваемости активов:
  - Увеличить скорость реализации продукции путём выхода на новые рынки сбыта.
- Снижение поставок сырья:
  - Диверсификация поставщиков и заключение долгосрочных контрактов.
- Поломка оборудования:
  - Проведение регулярного технического осмотра и профилактического обслуживания оборудования.
  - Обновление устаревших элементов производственной линии.

Соблюдение вышеперечисленных вариантов действий может благоприятно сказаться на экономическом состоянии предприятия. Сократить долговую нагрузку, а также снизить эффекты колебания курсов валют и инфляции. Кроме того, диверсификация поставщиков может благоприятно сказаться в случае нестабильности геополитической обстановки, а привлечение новых инвестиций и субсидий может помочь предприятию уменьшить долговую нагрузку и высвободить средства на модернизацию.

Для информационной безопасности:

- Контроль за обновление ПО:
  - Внедрить систему автоматического обновления ПО.
  - Организация отдела для мониторинга состояния IT-инфраструктуры предприятия.
- Пересмотр прав доступа:
  - Разработать регламент регулярного пересмотра прав доступа.
  - Внедрить систему контроля ролей и разграничения доступа.

- Риск внешнего проникновения:
    - Использование современных DLP и SIEM систем для мониторинга и предотвращения утечек.
    - Повысить защиту сетевых сегментов.

В современном мире количество кибер преступлений растёт и соблюдение вышеперечисленных мер позволит предприятию противостоять им. Украденная информация может не только повлечь за собой репутационные и финансовые потери для предприятия, но и повлечь за собой ответственность, предусмотренную законодательством, именно поэтому соблюдение мер информационной безопасности критически важно для современного предприятия.

Для инженерно-технической безопасности:

- Уязвимость оконных и дверных проёмов:
    - Установка металлических решёток и укрепление дверных конструкций.
    - Ремонт и замена уязвимых элементов.
- Отсутствие аппаратных средств защиты:
    - Закупка и внедрение оборудования для поиска радиопередатчиков и закладок.
    - Установка генераторов шума в критически важных зонах.
- Низкая защищённость инженерных конструкций:
    - Укрепление конструкций, подвергающихся неблагоприятному воздействию.
    - Проведение инспекций для оценки состояния конструкций.

Внедрение мер для улучшение инженерной безопасности позволит предприятию вовремя реагировать на недостаточную прочность конструкций. Нивелировать угрозы связанные с проникновением на территорию предприятия посторонних людей или с использованием радиоуправляемых систем.

Для физической безопасности:

- Пересмотр списков допуска:
    - Создание отдела физической безопасности, ответственного за контроль доступа и пересмотр прав.
    - Использование автоматизированных систем учета.
- Строгие меры идентификации:

    - Внедрение биометрической системы для доступа к критическим зонам.
    - Организация проверок эффективности работы существующих мер.
- Незащищённость телекоммуникационных кабелей:
    - Использование экранированных кабелей для предотвращения перехвата информации.
    - Разработать планы для экстренного восстановления сетей при аварийных ситуациях.

Риски, связанные с доступом к критическим зонам, могут повлечь за собой остановку производства и утечку конфиденциальной информации. Для минимизации таких рисков следует ограничивать круг лиц с доступом к таким зонам, а так использовать для такого разграничения системы основанные на биометрических или прочих идентифицирующих личность сотрудника данных. Кроме того, уязвимость телекоммуникационных сетей может повлечь за собой как нарушение производственной деятельности предприятия, так и нарушить организационную и коммерческую деятельность.

Для кадровой безопасности:

- Текучесть кадров:
    - Внедрить программу повышения квалификации сотрудников и мотивационные программы.
    - Рассмотреть увеличение заработной платы или внедрение бонусной системы.
- Утечка коммерческой тайны:
    - Заключение соглашение о конфиденциальности с ключевыми сотрудниками.
    - Использовать систему разграничения доступа к коммерческой информации.
- Приём некомпетентных сотрудников:
    - Внедрить более строгий отбор с пользованием профессиональных тестов.
    - Проводить регулярное обучение и тренинги для повышения квалификации.

Для удержания сотрудников и создания благоприятных условий для притока новых кадров предприятию рекомендуется повысить величину заработной плата или внедрить бонусную программу. Кроме того, для уменьшения

вероятности приёма на работу некомпетентного сотрудника рекомендуется внедрить строгий отбор, основанный на тестировании кандидата. Для повышения профессиональных навыков сотрудников хорошей идеей будет внедрение обучения и внедрения тренингов повышения квалификации, что в свою очередь может положительность сказаться на объёме выпускаемой продукции, а также снизить количество инцидентов на производстве связанных с ошибками сотрудников.

Для пожарной безопасности:

- Горючая среда:
  - Установить дополнительные системы вентиляции и очистки воздуха.
  - Усилить контроль за герметичностью оборудования.
- Источники зажигания:
  - Внедрить датчики перегрева на производственном оборудовании.
  - Обеспечить регулярные проверки состояния электропроводки.
- Модернизация систем:
  - Обновить системы пожаротушения и дымоудаления на критически важных участках.
  - Проводить обучение персонала действиям в чрезвычайных ситуациях.

Так как основная деятельность предприятия подразумевает высокий риск пожароопасности, то соблюдение норма пожарной безопасности является критически важным для существования и функционирования предприятия. Для минимизации рисков возникновения пожаров предприятию рекомендуется внедрить датчики перегрева, обеспечить регулярные проверки состояния электропроводки, кроме того, для минимизации ущерба при возникновении пожара, а также для остановки его распространения на всё предприятие предприятию необходимо следить и своевременно обновлять, модернизировать и обслуживать системы пожаротушения и дымоудаления, а также проводить обучения персонала на случай возникновения пожара.

В данном разделе были рассмотрены основные предложения по повышению уровня безопасности НПАО «Светлогорский ЦБК». Для наглядности все меры предложенные в этом разделе представлены в виде таблицы в приложении Г.