

КОНТРОЛЬНЫЙ СПИСОК ГЕНЕРАЛЬНОГО ДИРЕКТОРА: ЛИДЕРСТВО В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

УПРАВЛЕНИЕ

- ☐ Назначьте сотрудника на должность директора отдела информационной безопасности (CISO).
- ☐ Разработайте ориентированную на существующие риски политику кибербезопасности организации на основании международных, национальных и отраслевых стандартов и указаний, а также обеспечьте ее соблюдение.
- ☐ Определите роли и обязанности всех задействованных в обеспечении кибербезопасности сотрудников. Совместно с директором по информационной безопасности определите надлежащие роли в обеспечении кибербезопасности и права доступа для сотрудников всех уровней.
- ☐ Разработайте или определите четкие каналы связи между отдельными подразделениями или сотрудниками, работающими с различными аспектами кибербезопасности.
- ☐ Убедитесь, что директор по информационной безопасности имеет четкую прямую линию коммуникации для своевременного уведомления вас и совета директоров об угрозах.
- ☐ Регулярно приглашайте директора по информационной безопасности или другого технического специалиста для проведения брифинга перед высшим руководством.
- ☐ Убедитесь, что политики, стандарты и механизмы кибербезопасности унифицированы во всей организации.

ОЦЕНКА РИСКОВ И УПРАВЛЕНИЕ ИМИ

- ☐ Совместно с директором по информационной безопасности или техническими специалистами проведите оценку рисков, предусматривающую:
 - описание активов организации и различных уровней их зависимостей от технологических ресурсов;
 - оценку зрелости организации и неотъемлемых рисков, связанных с зависимостями ее активов от технологических ресурсов;
 - определение желаемого состояния зрелости организации;
 - анализ приоритетных областей для обеспечения кибербезопасности в организации;
 - выявление несоответствий между текущим состоянием и желаемым целевым состоянием кибербезопасности;
 - реализацию планов для достижения и поддержания зрелости;
- Оценка и выделение средств для инвестирования в безопасность и устранения существующих уязвимостей.
- постоянную переоценку зрелости кибербезопасности организации, рисков и целей;
- рассмотрение возможности принятия защитных мер, таких как приобретение киберстраховки.
- ☐ Обеспечьте проведение анализа и предоставление результатов ключевым заинтересованным сторонам и совету директоров.
- ☐ Запланируйте контроль всех мер, направленных на повышение осведомленности в сфере кибербезопасности, и отслеживание процесса их внедрения.

ОРГАНИЗАЦИОННАЯ КУЛЬТУРА

- ☐ Регулярно обсуждайте вопросы киберрисков и кибербезопасности на уровне руководства.
- ☐ Убедитесь, что обучение принципам кибербезопасности является частью процесса адаптации всех сотрудников, и все сотрудники подписывают документы, подтверждающие их согласие соблюдать политики кибербезопасности организации.
- ☐ Организуйте регулярные курсы обучения по вопросам кибербезопасности для всех сотрудников.
- ☐ Убедитесь, что вопросы кибербезопасности всегда учитываются при оценке организацией потенциальных поставщиков и передаче данных третьим сторонам.
- ☐ Интегрируйте оценку кибербезопасности организации при рассмотрении возможности слияний и поглощений.
- ☐ Ежегодно пересматривайте политики кибербезопасности организации.
- ☐ Поощряйте добровольный обмен информацией об угрозах кибербезопасности и инцидентах между техническими специалистами.