КИБЕРБЕЗОПАСНОСТЬ ДЛЯ НЕБОЛЬШИХ ОРГАНИЗАЦИЙ

КОНТРОЛЬНЫЙ СПИСОК СОВЕТА ДИРЕКТОРОВ: ЛИДЕРСТВО В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

ОСНОВЫ УПРАВЛЕНИЯ КИБЕРРИСКАМИ

☐ **Регулярно проверяйте в составе группы, может ли совет директоров утвердительно ответить на следующие вопросы:**

- Соответствует ли ваша организация применимым законодательным и нормативным требованиям, таким как Общий регламент по защите данных (GDPR)?
- Выполнила ли ваша организация количественную оценку киберрисков и проверку финансовой устойчивости?
- Имеет ли ваша организация действующий план по улучшению, гарантирующий, что воздействие находится в приемлемых пределах рисков?
- Регулярно ли совет директоров обсуждает лаконичную, четкую и действенную информацию касательно предоставляемой руководством устойчивости организации к угрозам кибербезопасности?
- Имеет ли ваша организация планы реагирования на недавно протестированные инциденты, в том числе на уровне совета директоров?
- Являются ли роли ключевых сотрудников, ответственных за управление киберрисками, четкими и согласованным с тремя линиями защиты?
- Получили ли вы независимую аттестацию и гарантию устойчивости вашей организации к киберрискам, например, в виде тестирования, сертификации или страховки?

☐ **Если вы не можете утвердительно ответить на один или более из вышеперечисленных вопросов, обратитесь к генеральному директору, директору по информационной безопасности, соответствующему персоналу организации и/или к внешним ресурсам, чтобы исправить проблему.**

НАДЗОР

☐ **Убедитесь, что совет директоров осведомлен о своей конечной ответственности за киберриски и устойчивость организации.**

☐ **При необходимости делегируйте надзор конкретному комитету совета директоров.**

☐ **Назначьте одного корпоративного директора, как правило, главного директора по информационной безопасности, ответственным за отчетность о способности организации управлять киберустойчивостью и развитием при достижении целей устойчивости к угрозам кибербезопасности.**

☐ **Убедитесь, что этот сотрудник имеет регулярный доступ к совету директоров, обладает достаточными полномочиями, имеет в распоряжении соответствующий коллектив, опыт и ресурсы для выполнения этих обязанностей.**

☐ **Ежегодно определяйте допустимость рисков организации; обеспечьте согласованность с корпоративной стратегией и приемлемыми пределами рисков.**

☐ **Обеспечьте проведение ежегодного официального независимого анализа киберустойчивости организации.**

☐ **Обеспечьте интеграцию процедур обеспечения киберустойчивости и оценки рисков в общую бизнес-стратегию организации, управление рисками, планирование бюджета и распределение ресурсов.**

☐ **Регулярно отслеживайте риски в отношении третьих лиц.**

- ☐ **Обеспечьте контроль над созданием, внедрением, тестированием и постоянным усовершенствованием планов по обеспечению киберустойчивости, обеспечением унификации во всей организации, а также регулярностью представления отчетов перед советом директоров со стороны главного директора по информационной безопасности или других ответственных должностных лиц.**

- ☐ **Периодически проверяйте собственную эффективность и рассмотрите возможность получения независимых рекомендаций по непрерывному усовершенствованию вашей системы.**

БУДЬТЕ В КУРСЕ

- ☐ **При принятии в совет нового члена убедитесь, что этот сотрудник обладает применимыми и актуальными навыками и знаниями, позволяющими понимать связанные с киберугрозами риски.**

- ☐ **Регулярно консультируйтесь с руководством по текущим и будущим рискам в организации, соответствующим нормативным требованиям, а также отраслевым и социальным ориентирам для снижения приемлемых пределов риска. Запланируйте:**
  - регулярные брифинги по обязанностям, соответствующим новым нормативным требованиям и законодательству;
  - совместное планирование советом директоров и исполнительным комитетом, а также визиты к коллегам и руководителям в области кибербезопасности;
  - брифинги по вопросам безопасности в среде кибербезопасности;
  - обмен информацией об управлении и отчетности на уровне совета.

- ☐ **Информируйте руководителей об их ответственности за предоставление количественно выраженной и доступно изложенной оценки киберрисков, угроз и событий в виде повестки дня во время заседаний совета директоров.**

- ☐ **Регулярно взаимодействуйте с руководителями и другими соответствующими сотрудниками и обсуждайте текущие системные проблемы, такие как уязвимость цепи поставок, общие зависимости, а также недостаток информации при обмене данными по вопросам управления киберрисками между советами директоров.**

СОЗДАНИЕ АТМОСФЕРЫ

- ☐ **Убедитесь, что сотрудники на всех уровнях осознают важность своих обязанностей в обеспечении киберустойчивости организации.**

- ☐ **Контролируйте роль руководства в формировании и поддержании в организации культуры рисков. Регулярно оценивайте эффективность культуры рисков организации, принимая во внимание ее влияние на безопасность и надежность, а также при необходимости вносите необходимые корректировки.**

- ☐ **Четко объясните, что вы ожидаете от всех сотрудников добросовестного отношения и незамедлительного информирования обо всех случаях несоблюдения нормативных требований в организации или за ее пределами.**

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

CarnegieEndowment.org