ЦЕНТРАЛЬНЫЙ БАНК
РОССИЙСКОЙ ФЕДЕРАЦИИ
(Банк России)

107016, Москва, ул. Неглинная, 12
www.cbr.ru
тел.: (495) 771-91-00

Публичным акционерным обществам

От 24.05.2019 № ИН-06-28/45

на от

Информационное письмо о рекомендациях по участию совета директоров (наблюдательного совета) в процессах развития и управления информационными технологиями и управления риском информационной безопасности в публичном акционерном обществе

В целях совершенствования корпоративного управления Банк России направляет для применения прилагаемые рекомендации по участию совета директоров (наблюдательного совета) в процессах развития и управления информационными технологиями и управления риском информационной безопасности в публичном акционерном обществе.

Настоящее информационное письмо подлежит опубликованию в «Вестнике Банка России» и размещению на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет».

Первый заместитель
Председателя Банка России С.А. Швецов

Приложение
к письму Банка России
от 24.05.2019 № ИН-06-28/45

Рекомендации по участию совета директоров (наблюдательного совета) в процессах развития и управления информационными технологиями и управления риском информационной безопасности в публичном акционерном обществе

В условиях стремительного развития информационных технологий цифровая трансформация бизнеса посредством внедрения современных информационных технологий в бизнес-процессы компании оказывает все возрастающее влияние на деятельность компании как в краткосрочной, так и в долгосрочной перспективе и становится ключевым фактором успешной реализации стратегии и достижения бизнес-целей компании, способствует развитию ее конкурентоспособности. С другой стороны, с развитием информационных технологий все более важное значение приобретают процессы управления риском информационной безопасности, пренебрежение которым представляет серьезную угрозу для стабильности деятельности компании и ее успешного развития в долгосрочной перспективе.

Вопросы развития и управления информационными технологиями, а также обеспечения информационной безопасности не ограничиваются исключительно решением технических и технологических задач, поскольку связаны непосредственно со стратегией развития компании. При этом процессы внедрения информационных технологий и обеспечения информационной безопасности взаимосвязаны и в условиях стремительного развития данной сферы требуют повышенного внимания компании, а проблемы, связанные с указанными процессами, — комплексного решения.

Системный подход к решению вопросов развития информационных технологий и информационной безопасности, в том числе путем грамотного инвестирования в указанные сферы и формирования компетентного кадрового ресурса для внедрения и эксплуатации информационных технологий, а также управления риском информационной безопасности, является важным фактором для достижения стратегических целей и эффективного развития компании.

В соответствии с Кодексом корпоративного управления[1], рекомендованным Банком России к применению акционерными обществами, ценные бумаги которых допущены к организованным торгам (далее — Кодекс корпоративного управления), вопросы стратегического управления компанией и определения принципов и подходов к организации системы управления рисками являются одними из ключевых функций совета директоров (наблюдательного совета) (далее — совет директоров). При реализации указанных функций на современном этапе возрастает роль совета директоров при формировании в компании запроса на цифровую трансформацию и принятии стратегических решений по вопросам внедрения и (или) развития информационных технологий с точки зрения оценки их роли и возможного влияния на деятельность и развитие бизнеса компании, а также по вопросам управления риском информационной безопасности.

Настоящий документ разработан в развитие рекомендаций Кодекса корпоративного управления[2] для использования в первую очередь публичными акционерными обществами, ценные бумаги которых допущены к организованным торгам, а также иными обществами, заинтересованными в эффективном управлении информационными технологиями и риском информационной безопасности (далее — общества). В качестве отправной точки, устанавливающей общие направления, общества могут использовать приведенные ниже рекомендации, адаптируя их под конкретные обстоятельства, отражающие специфику и особенности их деятельности.

1. При осуществлении стратегического управления обществом[3] совету директоров рекомендуется уделять внимание вопросам развития информационных технологий и управления риском информационной безопасности, связанным с реализацией информационных угроз, в том числе обусловленных недостатками (уязвимостью) применяемых информационных технологий.

В целях обеспечения эффективного развития информационных технологий и управления риском информационной безопасности в обществе совету директоров рекомендуется:

а) рассмотреть целесообразность разработки внутренних документов общества, определяющих вопросы внедрения новых информационных технологий с учетом целей и задач, стоящих перед обществом, а также характера и масштаба его деятельности и принимаемых рисков; определить

---

[1] Письмо Банка России от 10.04.2014 № 06-52/2463 “О Кодексе корпоративного управления”.

[2] Принципы 2.1.2, 2.1.3 Кодекса корпоративного управления.

[3] Принцип 2.1 Кодекса корпоративного управления.

основные направления информационной стратегии (ИТ-стратегия), политики в сфере информационных технологий (ИТ-политика), закрепляющие основные принципы развития и использования информационных технологий, а также ожидаемые результаты и эффекты от их внедрения;

б) рассмотреть целесообразность разработки внутренних документов общества, определяющих вопросы управления рисками информационной безопасности с учетом целей и задач, стоящих перед обществом, а также характера и масштаба его деятельности и принимаемых рисков; определить политику управления риском информационной безопасности, закрепляющую основные принципы организации системы управления риском информационной безопасности;

в) при определении принципов и подходов к организации системы управления рисками[4] принимать во внимание влияние новых информационных технологий, а также степень существенности влияния на общество рисков, связанных с реализацией информационных угроз, в том числе обусловленных недостатками (уязвимостью) применяемых информационных технологий, а также киберугроз, обусловленных возможностью реализации компьютерных атак;

г) на регулярной основе осуществлять контроль[5] за реализацией исполнительными органами ИТ-стратегии, управлением информационными технологиями, а также управлением риском информационной безопасности в обществе.

Осуществление указанного контроля также может быть реализовано в рамках системы управления рисками и направлено на обеспечение:

финансовой устойчивости и операционной надежности (непрерывности) бизнеса, а также осведомленности об уровне риска информационной безопасности, присущего деятельности общества;

эффективной и достаточной реализации мер, направленных на снижение риска информационной безопасности до допустимого уровня;

интеграции процессов управления рисками, связанными с применением информационных технологий, и риском информационной безопасности в общий процесс риск-менеджмента организации;

своевременного выявления и реагирования на инциденты информационной безопасности;

эффективного управления взаимоотношениями с внешними поставщиками услуг и связанными с ними рисками;

оценки влияния на деятельность общества инвестиций, направленных на развитие информационных технологий и обеспечение информационной безопасности, оценки ИТ-бюджета, включая оценку проектов на всем протяжении их жизненного цикла и значительных эксплуатационных расходов;

ответственного применения информационных технологий и соблюдения этических норм при их применении.

2. С учетом характера и масштабов деятельности общества, уровня и специфики принимаемых рисков совету директоров рекомендуется определять периодичность предоставления отчетов[6] единоличного исполнительного органа и коллегиального исполнительного органа по вопросам создания эффективной системы управления информационными технологиями, а также системы управления риском информационной безопасности, об инвестициях в информационные технологии и обеспечение информационной безопасности, достигнутых результатах, оценке влияния внедрения новых технологий на деятельность общества.

3. С учетом целей и задач, стоящих перед обществом, а также характера и масштабов деятельности общества, уровня и специфики принимаемых рисков совету директоров рекомендуется рассмотреть вопрос о целесообразности создания комитета по информационным технологиям и комитета по информационной безопасности[7].

4. В случае принятия советом директоров решения о создании комитета по информационным технологиям и комитета по информационной безопасности, председателями указанных комитетов рекомендуется назначать лиц из числа членов совета директоров, обладающих компетенциями и опытом в области информационных технологий и информационной безопасности соответственно. Функции председателя комитета по информационным технологиям и председателя комитета по информационной безопасности не рекомендуется возлагать на одного и того же члена совета директоров.

5. В случае принятия советом директоров решения о создании комитета по информационным технологиям к его задачам рекомендуется отнести[8]:

выработку рекомендаций совету директоров в части утверждения ИТ-стратегии и ИТ-политики;

контроль за организацией процессов управления информационными технологиями;

---

[4] Принцип 2.1.3 Кодекса корпоративного управления.

[5] Принцип 2.1.1, пункт 60 Кодекса корпоративного управления.

[6] Пункты 59, 60, 73 Кодекса корпоративного управления.

[7] Принцип 2.8.4 Кодекса корпоративного управления.

[8] Задачи комитета по информационным технологиям могут быть реализованы в рамках иного комитета, например комитета по стратегии.

контроль за организацией процессов мониторинга и надлежащего реагирования на изменения в развитии информационных технологий, включая учет потенциальных возможностей их применения обществом, а также оценку их возможного негативного воздействия на общество и его бизнес-модель;

рассмотрение вопросов, связанных с использованием информации и информационных технологий для сохранения и повышения интеллектуального капитала общества.

6. В случае принятия советом директоров решения о создании комитета по информационной безопасности к его задачам рекомендуется отнести[9]:

выработку рекомендаций совету директоров в части утверждения политики управления риском информационной безопасности;

контроль за организацией процессов управления риском информационной безопасности, в том числе связанным с аутсорсингом и применением сторонних информационных сервисов, включая облачные технологии;

контроль за организацией процессов обеспечения защиты информации, в том числе персональных данных.

7. При осуществлении в обществе внутреннего аудита в оценку эффективности системы внутреннего контроля и системы управления рисками[10] рекомендуется включать оценку полноты и качества реализуемых мер, направленных на снижение риска информационной безопасности.

8. Наряду со сведениями, предусмотренными законодательством Российской Федерации, в годовой отчет общества с учетом целей и задач, стоящих перед обществом, а также характера и масштаба его деятельности и принимаемых рисков рекомендуется включать сведения о развитии и управлении информационными технологиями[11] и управлении риском информационной безопасности[12], в том числе:

сведения об основных направлениях деятельности в области развития и управления информационными технологиями в отчетный период, включая цели, значимые изменения и сведения по реализации ИТ-политики и ИТ-стратегии (при их наличии);

информацию о функционировании систем управления информационными технологиями и риском информационной безопасности и критериях оценки их эффективности;

сведения о мерах, направленных на повышение уровня знаний и квалификации членов совета директоров и менеджмента в области информационных технологий;

планы общества в области повышения надежности применяемых информационных технологий и эффективности управления риском информационной безопасности.

---

[9] Задачи комитета по информационной безопасности могут быть реализованы в рамках иного комитета, например комитета по управлению рисками.

[10] Принцип 5.2.2 Кодекса корпоративного управления.

[11] В рамках подп. 7, 9, 14 пункта 293 Кодекса корпоративного управления.

[12] В рамках подп. 13 пункта 293 Кодекса корпоративного управления.