

В программы проверок были включены в том числе следующие вопросы:

- > проверка осуществления закупочной деятельности и ведения договорной работы;
- > проверка соблюдения требований Антикоррупционной политики, осуществления мероприятий по выявлению конфликта интересов.

Представитель ПАО «МРСК Юга» принял активное участие в рабочей группе по совершенствованию методологического обеспечения в области противодействия коррупции¹. В течение 2018 года направлено четыре аналитические записки с предложениями для рассмотрения на заседаниях группы.

Информация о деятельности ПАО «МРСК Юга» в области противодействия и профилактики коррупции размещена в сети Интернет. На официальном сайте Компании разработан новый раздел «Противодействии коррупции»: <http://mrsk-yuga.ru/pages/show/protivodeystvie-korrupcii>.

Обеспечение безопасности экономической деятельности

В 2018 году с участием подразделения безопасности ПАО «МРСК Юга» подготовлено и направлено в правоохранительные и надзорные органы 194 материала (в 2017 год – 41), в том числе:

- > по фактам неучтенного потребления электроэнергии перед правоохранительными органами инициировано 172 проверочных мероприятия на предмет наличия в действиях нарушителей признаков преступления, предусмотренных ст. 165 Уголовного кодекса Российской Федерации;
- > по итогам проверок финансово-экономической и хозяйственной деятельности – 3 (2017 год – 2);
- > в рамках работы по возврату просроченной дебиторской задолженности за услуги по передаче электроэнергии – 6 (в 2017 году – 6) (ООО «Донреко», ПАО «Волгоградэнерго», ПАО «ТНС энерго Ростов-на-Дону»);
- > по другим основаниям – 13, в том числе в отношении сотрудников Компании – 3.

На основании материалов, подготовленных и направленных в правоохранительные, надзорные органы с участием ПБ и сопровождаемых ПБ, по результатам проведенных процессуальных проверок возбуждено девять уголовных дел (в 2017 году – 14, из них девять – по фактам разукрупнения электрооборудования и хищения ТМЦ):

- > 1 – ст. 165 Уголовного кодекса Российской Федерации «Причинение имущественного ущерба»;
- > 2 – ст. 204 Уголовного кодекса Российской Федерации «Коммерческий подкуп»;
- > 3 – ст. 158 Уголовного кодекса Российской Федерации «Кража»;
- > 2 – ст. 159 Уголовного кодекса Российской Федерации «Мошенничество»;
- > 1 – ст. 272 Уголовного кодекса Российской Федерации «Неправомерный доступ к компьютерной информации».

По результатам рассмотрения материалов уголовных дел судами вынесено пять решений о привлечении нарушителей к уголовной ответственности (в 2017 году – 8, из них пять – по фактам разукрупнения электрооборудования и хищения ТМЦ):

- > 1 – ст. 204 Уголовного кодекса Российской Федерации «Коммерческий подкуп»;
- > 1 – ст. 272 Уголовного кодекса Российской Федерации «Неправомерный доступ к компьютерной информации»;
- > 1 – ст. 158 Уголовного кодекса Российской Федерации «Кража»;
- > 1 – ст. 159 Уголовного кодекса Российской Федерации «Мошенничество» (в отношении С. А. Хурджи);
- > 1 – ст. 201 Уголовного кодекса Российской Федерации «Злоупотребление должностными полномочиями».

В рамках административного судопроизводства (Кодекс об административных правонарушениях Российской Федерации) направлен 4 081 заявительский материал:

- > по признакам административного правонарушения в соответствии со ст. 7.19 Кодекса об административных правонарушениях Российской Федерации – 4 054 (в 2017 году – 1 121), по результатам рассмотрения судами вынесено 1 286 положительных решений (в 2017 году – 392);
- > по признакам административного правонарушения в соответствии со ст. 9.22 Кодекса об административных правонарушениях Российской Федерации – 27, по результатам рассмотрения которых Нижне-Волжским управлением Ростехнадзора вынесено 27 положительных решений.

РАБОТА С ИНСАЙДЕРСКОЙ ИНФОРМАЦИЕЙ

В соответствии с требованиями законодательства Российской Федерации в области защиты информации² в Компании утвержден Перечень информации, содержащей сведения конфиденциального характера, в который включена инсайдерская информация.

В целях усиления информационной безопасности, снижения рисков информационных угроз и уменьшения последствий нарушения правил информационной безопасности в Компании утверждены и введены в действие ряд нормативных документов в области защиты информации, в том числе инсайдерской:

- > Положение по защите информации ПАО «МРСК Юга»;
- > Регламент работы с автоматизированной системой Service Desk;
- > Регламент использования корпоративной ИТ-инфраструктуры.

По состоянию на 27 декабря 2018 года Компанией утвержден и передан в установленном порядке ПАО Московская Биржа (далее – Московская биржа) список инсайдеров ПАО «МРСК Юга» в количестве 1 808 инсайдеров.

1. Создана распоряжением ПАО «Россети» от 20 июня 2016 года № 244р.

2. В том числе Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 29 июля 2004 года № 98-ФЗ «О коммерческой тайне», Федерального закона от 27 июля 2010 года № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации».

Категория инсайдера	На 31.12.2017		1-й квартал 2018 года		На 31.03.2018		2-й квартал 2018 года		На 30.06.2018		3-й квартал 2018 года		На 30.09.2018		4-й квартал 2018 года		На 31.12.2018	
	вкл.	искл.	вкл.	искл.	вкл.	искл.	вкл.	искл.	вкл.	искл.	вкл.	искл.	вкл.	искл.	вкл.	искл.	вкл.	искл.
1	31	-	-	31	5	-	36	4	4	36	1	8	29					
2	1 746	32	25	1 753	35	34	1 754	37	29	1 762	51	54	1 759					
3	-	-	-	-	-	-	-	-	-	-	-	-	-					
4	20	1	2	19	1	-	20	1	-	21	-	1	20					
Итого	1 797	33	27	1 803	41	34	1 810	42	33	1 819	52	63	1 808					

Ежеквартально проводится анализ поступившей информации от акционеров – инсайдеров Компании, осуществляется внутренний контроль использования инсайдерской информации, проводится мониторинг информации к раскрытию на предмет возможного использования при сделках с ценными бумагами.

СИСТЕМА УПРАВЛЕНИЯ РИСКАМИ

В Компании действует система управления рисками (далее – СУР), целью которой является обеспечение устойчивого непрерывного функционирования и развития Компании путем своевременной идентификации, оценки и эффективного управления рисками, представляющими угрозу эффективному осуществлению хозяйственной деятельности и репутации Компании, здоровью сотрудников, окружающей среде, а также имущественным интересам акционеров и инвесторов.

В целях развития СУР в Компании Советом директоров утверждена Политика управления рисками (утверждена в новой редакции решением Совета директоров Компании 1 апреля 2016 года, протокол от 1 апреля 2016 года № 182/2016).

Участники СУР

В качестве основных выступают следующие участники процесса управления рисками.

Наименование участника	Основные функции в области СУР
Совет директоров	Утверждает внутренние документы Компании, определяющие организацию и функционирование СУР Компании. Рассматривает отчеты исполнительных органов Компании об организации, функционировании и эффективности СУР, оценивает функционирование СУР и вырабатывает рекомендации по ее улучшению
Уполномоченный комитет при Совете директоров	Осуществляет контроль за эффективностью процедур управления рисками, а также оценку эффективности мероприятий по управлению рисками и совершенствованию СУР
Исполнительные органы (Правление)	Устанавливают требования к формату и полноте информации о рисках Компании. Формируют направления и планы развития и совершенствования СУР. Проводят анализ портфеля рисков и вырабатывают меры по стратегии реагирования и перераспределению ресурсов в отношении управления соответствующими рисками
Владельцы рисков	Отвечают за своевременное выявление и оценку рисков, выбор метода реагирования на риски, своевременную разработку и организацию выполнения мероприятий по управлению рисками, регулярный мониторинг рисков
Исполнители мероприятий по управлению рисками	Отвечают за своевременное выявление и/или минимизацию рисков, выполнение мероприятий, направленных на управление рисками, своевременно и в полном объеме
Подразделение по управлению рисками	Осуществляет функции по общей координации процессов управления рисками
Подразделение внутреннего аудита	Осуществляет внутреннюю независимую оценку эффективности системы управления рисками и выдачу рекомендаций по повышению эффективности и результативности СУР