

**УТВЕРЖДЕНА**

**Решением Совета директоров**

**ПАО «НК «Роснефть»**

**«31» марта 2020 г.**

**Протокол от «03» апреля 2020 г.**

**№ 19**

**Введена в действие «21» апреля 2020 г.**

**Приказом ПАО «НК «Роснефть»**

**от «21» апреля 2020 г. №233**

## **ПОЛИТИКА КОМПАНИИ**

---

### **В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**№ ПЗ-11.01 П-01**

**ВЕРСИЯ 2.00**

**МОСКВА  
2020**

# СОДЕРЖАНИЕ

1. ВВОДНЫЕ ПОЛОЖЕНИЯ.....	3
НАЗНАЧЕНИЕ .....	3
ОБЛАСТЬ ДЕЙСТВИЯ.....	3
ПЕРИОД ДЕЙСТВИЯ И ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ.....	3
2. ГЛОССАРИЙ .....	4
2.1. ТЕРМИНЫ И ОБОЗНАЧЕНИЯ КОРПОРАТИВНОГО ГЛОССАРИЯ .....	4
2.2. РОЛИ.....	6
3. ЗАЯВЛЕНИЕ О ПОЛИТИКЕ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ .....	7
3.1. ЦЕЛИ И ЗАДАЧИ КОМПАНИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ .....	8
3.2. ОБЪЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	8
3.3. ПРИНЦИПЫ УПРАВЛЕНИЯ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	9
4. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЯ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	12
5. ДОВЕДЕНИЕ И РАСПРОСТРАНЕНИЕ ПОЛИТИКИ .....	13
6. ССЫЛКИ .....	14
7. РЕГИСТРАЦИЯ ИЗМЕНЕНИЙ ЛОКАЛЬНОГО НОРМАТИВНОГО ДОКУМЕНТА .....	15

Права на настоящий ЛНД принадлежат ПАО «НК «Роснефть». ЛНД не может быть полностью или частично воспроизведён, тиражирован и распространён без разрешения ПАО «НК «Роснефть».

# 1. ВВОДНЫЕ ПОЛОЖЕНИЯ

## НАЗНАЧЕНИЕ

Настоящая Политика является основополагающим документом, предназначенным для выражения позиции Компании в области информационной безопасности, определяет систему взглядов, принципов и подходов в этой области для обеспечения защищенности бизнес-процессов Компании, создания условий безопасного цифрового развития Компании и обеспечения соответствия требованиям законодательства Российской Федерации в данной области, а также применимого законодательства любого иного государства, где Компания осуществляет деятельность.

Настоящая Политика разработана в соответствии с требованиями законодательства Российской Федерации в области информационной безопасности, с учетом применимых международных стандартов, передового опыта и лучших практик.

## ОБЛАСТЬ ДЕЙСТВИЯ

Настоящая Политика обязательна для исполнения работниками ПАО «НК «Роснефть» и подконтрольных ПАО «НК «Роснефть» Обществ Группы, в отношении которых уставами Обществ, акционерными и иными соглашениями с компаниями-партнерами не определен особый порядок реализации акционерами/участниками своих прав, в том числе по управлению Обществом.

Настоящая Политика не распространяется на организацию и порядок защиты информации, составляющей государственную тайну.

## ПЕРИОД ДЕЙСТВИЯ И ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ

Настоящая Политика является локальным нормативным документом постоянного действия.

Настоящая Политика утверждается, изменяется и признается утратившей силу в ПАО «НК «Роснефть» решением Совета директоров ПАО «НК «Роснефть» и вводится в действие в ПАО «НК «Роснефть» приказом ПАО «НК «Роснефть».

## 2. ГЛОССАРИЙ

### 2.1. ТЕРМИНЫ И ОБОЗНАЧЕНИЯ КОРПОРАТИВНОГО ГЛОССАРИЯ

<b>АВТОМАТИЗИРОВАННАЯ СИСТЕМА УПРАВЛЕНИЯ (АСУ)</b>	Комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления таким оборудованием и процессами.
<b>КОМПЬЮТЕРНАЯ АТАКА</b>	Действия, направленные на реализацию угроз несанкционированного доступа к ИТ-активу, воздействия на него или на ресурсы автоматизированной информационной системы с применением программных и (или) технических средств.
<b>ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ</b>	Состояние защищенности информационной среды, обеспечивающее ее формирование, использование и развитие в интересах Компании.
<b>ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА (ИТ-ИНФРАСТРУКТУРА)</b>	Совокупность компонентов информационных технологий, в том числе аппаратное (системы обработки и хранения данных, оборудование рабочего места, периферия и т.д.), системное программное и инженерное обеспечение, сети, специализированные помещения.
<b>ИНФОРМАЦИОННАЯ СИСТЕМА (ИС)</b>	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.
<b>ИНФОРМАЦИОННАЯ СРЕДА</b>	Совокупность разной информации вместе с ИТ-инфраструктурой, а также субъектами, которые занимаются сбором, использованием и распространением информации.
<b>ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННАЯ СЕТЬ</b>	Технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.
<b>ИНФОРМАЦИЯ</b>	Сведения (сообщения, данные) независимо от формы их представления.
<b>ИТ-АКТИВ</b>	Идентифицируемый предмет, вещь или объект в области информационных технологий, который имеет потенциальную или действительную ценность для Компании.
<b>ИТ-ПРОСТРАНСТВО</b>	Совокупность объектов (информационные ресурсы, средства информационного взаимодействия и информационная инфраструктура), вступающих друг с другом в информационное взаимодействие, а также сами информационные технологии, обеспечивающие данное взаимодействие.
<b>КОМПАНИЯ</b>	Группа юридических лиц различных организационно-правовых форм, включая ПАО «НК «Роснефть», в отношении которых последнее выступает в качестве основного или преобладающего (участвующего) общества.

<b>МОБИЛЬНОЕ ТЕХНИЧЕСКОЕ СРЕДСТВО</b>	Съемные машинные носители информации, портативные вычислительные устройства и устройства связи с возможностью обработки информации (переносные персональные компьютеры - ноутбуки, нетбуки, планшетные компьютеры, а также мобильные телефоны, смартфоны, умные часы/браслеты, цифровые камеры, звукозаписывающие устройства и иные средства).
<b>ОБЩЕСТВО ГРУППЫ (ОГ)</b>	Хозяйственное общество, прямая и (или) косвенная доля владения ПАО «НК «Роснефть» акциями или долями в уставном капитале которого составляет 20 процентов и более.
<b>ПОДКОНТРОЛЬНОЕ ПАО «НК «РОСНЕФТЬ» ОБЩЕСТВО ГРУППЫ</b>	Общество Группы, в котором ПАО «НК «Роснефть» имеет право прямо и/или косвенно (через подконтрольных ему лиц) распоряжаться в силу участия в таком Обществе Группы и (или) на основании договоров доверительного управления имуществом, и (или) простого товарищества, и (или) поручения, и (или) акционерного соглашения, и (или) иного соглашения, предметом которого является осуществление прав, удостоверенных акциями (долями) такого Общества Группы, более 50 процентами голосов в высшем органе управления, либо назначать (избирать) единоличный исполнительный орган и/или более 50 процентов состава коллегиального органа управления.
<b>ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ</b>	Совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ.
<b>ПРОИЗВОДСТВЕННАЯ СИСТЕМА</b>	Совокупность компонентов информационных технологий, обеспечивающих автоматизацию решения задач планирования и управления различными видами производственной деятельности и производственных процессов.
<b>РИСК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ИБ- РИСК)</b>	Сочетание вероятности реализации угрозы информационной безопасности и последствий её реализации, оказывающих негативное влияние на достижение целей Компании.
<b>СТРУКТУРНОЕ ПОДРАЗДЕЛЕНИЕ</b>	Структурное подразделение ПАО НК «Роснефть» или Общества Группы с самостоятельными функциями, задачами и ответственностью в рамках своих компетенций, определенных в Положении о структурном подразделении.
<b>УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (УГРОЗА)</b>	Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации или безопасности ИТ-актива.
<b>УЯЗВИМОСТЬ ИТ-АКТИВА</b>	Недостаток (слабость) ИТ-актива в целом, который(ая) может быть использован(а) для реализации угроз информационной безопасности.
<b>ЦИФРОВИЗАЦИЯ</b>	Применение прорывных технологий, трансформирующих операционные процессы за счет замещения или дополнения человека на базе использования качественно новой аналитики, искусственного интеллекта, мобильных и носимых устройств, роботизации, интеграционных технологических платформ.

## 2.2. РОЛИ

### РОЛИ КОРПОРАТИВНОГО ГЛОССАРИЯ

#### **ДЕЛОВОЙ ПАРТНЕР**

Текущие и потенциальные контрагенты ПАО «НК «Роснефть», а также Обществ Группы.

*Примечание: Потенциальные контрагенты, у которых на данный момент нет договорных отношений с ПАО «НК «Роснефть» или Обществом Группы, также относятся к деловым партнерам. К деловым партнерам также относятся государственные органы (включая налоговые органы) и физические лица (бенефициары, учредители). К потенциальным деловым партнерам относятся деловые партнеры, с которыми ПАО «НК «Роснефть» или Общество Группы только планирует вступить в договорные отношения. Взаимодействие с потенциальными деловыми партнерами возможно в рамках процедур аккредитации, квалификационной оценки и мониторинга цен.*

#### **РУКОВОДИТЕЛИ И СПЕЦИАЛИСТЫ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПАНИИ**

Руководители и/или работники структурного подразделения ПАО «НК «Роснефть»/Общества Группы, ответственного за координацию, планирование и организацию функционирования процессов в области информационной безопасности и за операционное управление ими.

#### **ТРЕТЬИ ЛИЦА**

Хозяйственные общества, в которых ПАО «НК «Роснефть» не имеет прямой либо косвенной доли в уставных капиталах, некоммерческие организации, в состав органов управления которых не входят представители Компании, а также лица, не являющиеся работниками и не занимающие должности в органах управления ПАО «НК «Роснефть» и Обществ Группы.

### РОЛИ ДЛЯ ЦЕЛЕЙ НАСТОЯЩЕГО ДОКУМЕНТА

#### **РУКОВОДСТВО КОМПАНИИ**

Главный исполнительный директор ПАО «НК «Роснефть», топ-менеджеры ПАО «НК «Роснефть», единоличные исполнительные органы Обществ Группы.

### 3. ЗАЯВЛЕНИЕ О ПОЛИТИКЕ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Настоящая Политика выражает позицию Компании в области информационной безопасности. Принятием настоящей Политики Компания провозглашает и обязуется осуществлять все возможные меры для защиты работников, имущества, информации, деловой репутации и бизнес-процессов Компании от риска причинения вреда, убытков и ущерба, возникающих в результате реализации угроз информационной безопасности.

Руководство Компании осознает важность и необходимость продвижения и совершенствования мер и средств обеспечения информационной безопасности в контексте развития законодательства РФ и регулирования норм информационной безопасности, а также развития используемых информационных технологий при автоматизации и цифровизации бизнес-процессов и технологических процессов на производствах. Соблюдение принципов информационной безопасности дополнительно позволит упрочить конкурентные преимущества Компании, обеспечить соответствие правовым, регуляторным и договорным требованиям, снизить имиджевые риски.

Настоящая Политика разработана с целью установления принципов, определяющих общие организационные и управленческие подходы, необходимые для обеспечения и управления информационной безопасностью Компании и защиты интересов Компании от рисков и угроз информационной безопасности.

Руководство Компании придерживается взглядов, что соблюдение принципов, правил и требований информационной безопасности является, в том числе, элементом корпоративной культуры. Следование требованиям информационной безопасности является важным условием при осуществлении повседневной деятельности (в том числе при реализации ИТ-проектов, проработке цифровых инициатив и т.д.), включая совместную работу с Деловыми партнерами. Каждый работник Компании и её Деловых партнеров несёт ответственность за безопасную работу с вверенными ему корпоративными ИТ-активами, компьютерным оборудованием, мобильными техническими средствами, носителями информации, предоставленной и обрабатываемой информацией Компании.

Руководители и специалисты по информационной безопасности Компании должны ответственно выполнять свои обязанности, осознавая, что качество их работы непосредственно влияет на состояние защищённости информации, ИТ-активов, бизнес- и технологических процессов Компании.

Работники Компании должны руководствоваться настоящей Политикой в профессиональной деятельности, при внутрикорпоративном взаимодействии, личном развитии и повышении культуры информационной безопасности. Политика раскрывает и дополняет при необходимости правила, определенные в Кодексе деловой и корпоративной этики НК «Роснефть» № ПЗ-01.06 П-01, в части принципов обеспечения информационной безопасности.

### 3.1. ЦЕЛИ И ЗАДАЧИ КОМПАНИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Управление и обеспечение информационной безопасности Компании ориентированы на достижение следующих целей в области информационной безопасности:

- предоставление безопасной информационной среды для функционирования и развития бизнес-процессов Компании;
- снижение уровня ИБ-рисков и угроз информационной безопасности до приемлемого уровня, позволяющего осуществлять устойчивое цифровое развитие Компании.

Для достижения данных целей необходимо решение следующих задач:

- **обеспечение информационной безопасности бизнес-процессов Компании в условиях возрастающего уровня угроз**, включая обеспечение оперативного мониторинга и оценку состояния защищенности в Компании; повышение эффективности защиты от спланированных целенаправленных компьютерных атак злоумышленниками; повышение информационной безопасности технологических и производственных систем;
- **применение новых современных методов для защищенной цифровизации Компании**, включая организацию проработки вопросов информационной безопасности при реализации цифровых решений; организацию апробации и применения новых методов защиты информации от современных угроз, в том числе за счет взаимодействия и партнерства с лидерами отрасли информационной безопасности; обеспечение применения безопасных цифровых технологий при внедрении отечественных разработок и развитии собственного конкурентоспособного корпоративного программного обеспечения Компании;
- **соответствие требованиям государства в области информационной безопасности** путем обеспечения заданного уровня информационной безопасности ИТ-активов в соответствии с требованиями действующего законодательства стран присутствия Компании.

### 3.2. ОБЪЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В рамках обеспечения информационной безопасности объектами защиты в Компании являются информация, обрабатываемая в Компании, вне зависимости от формы представления; ИТ-активы, включая, но не ограничиваясь следующим перечнем:

- автоматизированные рабочие места, средства обработки информации и мобильные технические средства;
- ИС, системы хранения данных, программное обеспечение и отдельные технические решения;
- АСУ, системы метрологии и промышленной автоматизации, в том числе измерительные системы и системы налива;
- ИТ-инфраструктура, информационно-телекоммуникационные сети и системы связи;
- ИТ-сервисы (ИТ-услуги), оказываемые Компании или в интересах Компании;
- решения по цифровизации бизнес- и технологических (производственных) процессов.

### 3.3. ПРИНЦИПЫ УПРАВЛЕНИЯ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Деятельность Компании в области информационной безопасности осуществляется с соблюдением следующих основных принципов<sup>1</sup>.

***Ориентация на стратегию Компании*** – стратегические инициативы по информационной безопасности разрабатываются и осуществляются в соответствии с общей стратегией и целями развития Компании, с учетом корпоративных стратегий в области информационных технологий и в области производственной автоматизации, метрологии и контроля качества.

***Централизация функций управления*** – принцип заключается в возможности принятия управленческих решений в области информационной безопасности на уровне Компании за счет оперативного мониторинга (ИТ-пространства Компании и внешней обстановки в информационной сфере) и оценки состояния информационной безопасности; осуществления централизованного управления стратегическими инициативами по информационной безопасности; контроля реализации мероприятий по развитию информационной безопасности; создания и развития централизованных решений в области информационной безопасности.

***Проактивный подход и управление рисками*** – базируется на мониторинге, анализе и оценке появляющихся, актуальных и будущих ИБ-рисков и угроз информационной безопасности (включая изучение технологий, используемых злоумышленниками) с целью своевременного и осознанного принятия превентивных мер для предупреждения компьютерных атак и недопущения ущерба Компании.

***Стандартизация и унификация*** – подразумевает разработку и тиражирование в ОГ стандартизованных требований и подходов, типовых технических решений и элементов архитектуры обеспечения информационной безопасности для унификации средств и методов решения однотипных задач; интерфейсов управления системами информационной безопасности.

***Импортозамещение*** – заключается в снижении рисков неблагоприятной внешней конъюнктуры за счёт ориентирования на отечественные решения, средства и сервисы при обеспечении информационной безопасности на территории Российской Федерации.

***Ресурсное обеспечение*** – означает необходимость выделения целевого финансирования на обеспечение и развитие информационной безопасности Компании, поддержание требуемой организационной структуры.

***Законность и соответствие*** – деятельность по обеспечению информационной безопасности Компании основывается на выполнении требований нормативных правовых актов Российской Федерации и национального законодательства стран, на территории которых осуществляют деятельность зарубежные ОГ.

***Повышение культуры информационной безопасности*** – декларирует необходимость не только информировать всех работников Компании, её Деловых партнёров и третьих лиц,

<sup>1</sup> Данные принципы разработаны с учетом международных стандартов и практик в области информационной безопасности, включая COBIT 5 for Information Security; ITIL: 2011 Service Design; ISO/IEC TS 19249:2017.

использующих ИТ-активы Компании, о требованиях информационной безопасности, но развивать навыки приемлемого обращения с информацией и безопасной работы с ИТ-активами Компании.

**Развитие компетенций и профессионализма** – принцип означает необходимость постоянного развития компетенций и практических навыков специалистов по информационной безопасности в условиях непрекращающегося изменения ИБ-рисков, ландшафта используемых информационных технологий и техник потенциальных нарушителей. Обеспечение информационной безопасности при автоматизации технологических и производственных процессов требует компетенций и знаний в областях производственной автоматизации и метрологии.

**Накопление знаний и обмен опытом** – следует накапливать знания и обмениваться опытом в ходе осуществления практической деятельности по обеспечению информационной безопасности (при мониторинге и реагировании на компьютерные атаки, при внедрении и эксплуатации технических решений, при аудитах информационной безопасности и т.д.).

**Информационная безопасность как неотъемлемое свойство ИТ-актива** – принцип заключается в следующем:

- требования информационной безопасности учитываются на всех этапах жизненного цикла ИТ-актива, вне зависимости от уровня конфиденциальности информации, обрабатываемой в ИТ-активе;
- создание программных продуктов в интересах Компании осуществляется с применением методов безопасной разработки программного обеспечения;
- предпочтительными являются ИТ-активы с наибольшим покрытием требований информационной безопасности встроенными функциями (при прочих равных характеристиках);
- встроенные функции по информационной безопасности должны быть настроены и использоваться при эксплуатации ИТ-активов, включая программно-аппаратные средства, автоматизированные системы управления и т.д.;
- соответствие приобретаемого/внедряемого ИТ-актива требуемому уровню информационной безопасности подтверждается согласно существующими процедурами, с учетом требований применимого законодательства.

**Информационная безопасность как неотъемлемое свойство ИТ-сервиса (ИТ-услуги)** – означает, что предлагаемые и оказываемые Компанией или в интересах Компании ИТ-услуги и ИТ-сервисы должны разрабатываться и оказываться с учетом требований информационной безопасности.

**Совместимость** – подразумевает подбор компонентов для обеспечения информационной безопасности способом, гарантирующим их взаимную системную совместимость на информационном, программном, электромагнитном и эксплуатационном уровнях, а также совместимость с используемыми ИТ-решениями, информационными технологиями и с решениями по автоматизации технологических и производственных процессов Компании.

**Надежность** – использование компонентов и средств для обеспечения информационной безопасности, соответствующих требованиям по надежности, готовности и обслуживаемости.

**Адекватность и обоснованность решений** – принимаемые в Компании меры и применяемые средства информационной безопасности эффективны, результативны и соразмерны с величиной ИБ-рисков и угроз информационной безопасности, влияющих на цели Компании.

**Комплексность** – применение любых доступных законных методов, средств и мероприятий (включая законодательные и нормативно-правовые, организационно-административные, программно-технические, инженерно-технические, физические), направленных на снижение ИБ-рисков, пресечение угроз информационной безопасности и недопущение ущерба Компании, её Деловым партнёрам и работникам.

**Разделение и минимизация полномочий** – означает, что выполнение критичных (итоговых) операций проводится только посредством разделения действий (например, алгоритмического разделения, временного или ресурсного - в т.ч. двумя работниками). Исключение единоличного совершения критичной операции может быть организовано на уровне организационных мер и/или программно-технических средств за счет выделения полномочий или роли пользователя. Программно-технический способ разделения полномочий является предпочтительным относительно организационного. Должны осуществляться контроль реализации принципов разграничения критических полномочий в ИС и в АСУ, ограничение прав доступа, в зависимости от уровня согласованных полномочий. Полномочия должны быть минимально достаточными для выполнения лицом своих должностных обязанностей, либо выполнения контрактных обязательств. При необходимости должен осуществляться контроль конфликта полномочий – организационный, а также программно-аппаратный.

**Постоянство совершенствования информационной безопасности** – обеспечение постоянного улучшения существующей практики и совершенствования средств и методов управления и обеспечения информационной безопасности на основе результатов аудитов информационной безопасности, мониторинга функционирования систем информационной безопасности, анализа изменений в методах и средствах компьютерных атак, анализа нормативных требований и существующего передового отечественного и зарубежного опыта в этой области.

## 4. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЯ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Работники Компании должны выполнять требования и правила информационной безопасности при работе с информацией и ИТ-активами Компании и её Деловых партнёров.

Высокие корпоративные стандарты и правила обеспечения информационной безопасности обязательны для всех без исключения работников Компании и должны учитываться во взаимоотношениях с Деловыми партнерами.

Руководство Компании возлагает ответственность на руководителей структурных подразделений, представительств и филиалов ПАО «НК «Роснефть» / ОГ за организацию повседневной деятельности и выделение необходимых ресурсов для обеспечения информационной безопасности как неотъемлемой составляющей бизнес- и производственных процессов; за своевременную идентификацию значимых ИТ-активов, назначение ответственных за ИТ-активы и управление доступа к ним; за предъявление установленных требований информационной безопасности к работникам Компании и Деловым партнерам, использующим ИТ-активы Компании, и контроль за их выполнением.

При использовании сети Интернет, при общении в социальных сетях и мессенджерах, использовании электронной почты, других средств телекоммуникаций и мобильных технических средств работникам Компании рекомендуется проявлять осмотрительность и сдержанность, чтобы не допускать рисков личной безопасности, а также избегать непреднамеренной утечки рабочей информации. Правила внешних коммуникаций устанавливаются Кодексом деловой и корпоративной этики НК «Роснефть» № ПЗ-01.06 П-01 и Информационной Политикой ПАО «НК «Роснефть» № ПЗ-01.04 П-01 ЮЛ-001 / внутренними документами ОГ в области информационной политики.

Каждый работник Компании за несоблюдение требований информационной безопасности несет дисциплинарную, гражданско-правовую, административную и уголовную ответственность в соответствии с законодательством Российской Федерации.

Работники зарубежных ОГ несут ответственность в соответствии с действующим законодательством страны, на территории которой осуществляется его деятельность.

Работники Деловых партнёров, использующие корпоративные ИТ-активы, а также предоставленную Компанией информацию, несут ответственность в соответствии с договорными отношениями с ПАО «НК «Роснефть» или Обществом Группы, а также применимым законодательством.

## 5. ДОВЕДЕНИЕ И РАСПРОСТРАНЕНИЕ ПОЛИТИКИ

Настоящая Политика является публичной.

ПАО «НК «Роснефть» и Общества Группы доводят также настоящую Политику до своих Деловых партнеров, подрядных организаций и взаимодействуют с ними с учетом положений настоящей Политики.

## 6. ССЫЛКИ

1. COBIT 5 for Information Security.
2. ITIL 2011: Service Design. ISBN 9780113313051.
3. ISO/IEC TS 19249:2017 Information technology. Security techniques. Catalogue of architectural and design principles for secure products, systems and applications = Информационная технология. Методы и средства обеспечения безопасности. Каталог принципов архитектуры и проектирования защищенных продуктов, систем и приложений.
4. Кодекс деловой и корпоративной этики НК «Роснефть» № ПЗ-01.06 П-01 версия 1.00, утвержденный решением Совета директоров ОАО «НК «Роснефть» 05.06.2015 (протокол от 05.06.2015 № 35), введенный в действие приказом ОАО «НК «Роснефть» от 28.09.2015 № 428.
5. Информационная Политика ПАО «НК «Роснефть» № ПЗ-01.04 П-01 ЮЛ-001 версия 3.00, утвержденная решением Совета директоров ПАО «НК «Роснефть» 15.11.2017 (протокол от 17.11.2017 № 6), введенная в действие приказом ПАО «НК «Роснефть» от 30.01.2018 № 53.

## 7. РЕГИСТРАЦИЯ ИЗМЕНЕНИЙ ЛОКАЛЬНОГО НОРМАТИВНОГО ДОКУМЕНТА

Таблица 1  
Перечень изменений Политики Компании

ВЕРСИЯ	ВИД И НАИМЕНОВАНИЕ ДОКУМЕНТА	НОМЕР ДОКУМЕНТА	ДАТА УТВЕРЖДЕНИЯ	ДАТА ВВЕДЕНИЯ В ДЕЙСТВИЕ	РЕКВИЗИТЫ РД
1	2	3	4	5	6
1.00	Политика Компании «Концепция информационно-технической безопасности ПАО «НК «Роснефть»	ПЗ-11.1	14.03.2008	14.03.2008	Приказ ОАО «НК «Роснефть» от 14.03.2008 № 124