

ПАО РОСНЕФТЬ

Политика информационной безопасности
ПАО РОСНЕФТЬ

г. Москва
2023 г.

СОДЕРЖАНИЕ

1. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ.....	
2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ	
3. ОБЛАСТЬ ПРИМЕНЕНИЯ	
4. НОРМАТИВНЫЕ ССЫЛКИ.....	
5. ОБЩИЕ ПОЛОЖЕНИЯ.....	
6. ПОЛОЖЕНИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	
7. ЗАДАЧИ СИСТЕМЫ УПРАВЛЕНИЯ ИБ.....	
8. РЕАЛИЗАЦИЯ.....	
9. КОНТРОЛЬ	
10. СОВЕРШЕНСТВОВАНИЕ	

1. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящем документе использованы следующие сокращения:

ИБ	- Информационная безопасность
ИС	- Информационная система
СУИБ	- Система управления информационной безопасностью

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термины и определения, используемые в настоящей Политике и рекомендуемые к использованию в нормативных и организационно-распорядительных документах, созданных на ее основе, приведены в Приложении № 1 «Термины и определения».

3. ОБЛАСТЬ ПРИМЕНЕНИЯ

3.1. Настоящая Политика информационной безопасности (далее – «Политика») предназначена для выражения позиции компании ПАО «РОСНЕФТЬ» (далее – Роснефть) в области информационной безопасности, определяет систему взглядов, принципов и подходов в этой области для обеспечения защищенности бизнес-процессов компании Роснефть, создания условий безопасного цифрового развития компании Роснефть и обеспечения соответствия требованиям законодательства Российской Федерации в данной области, а также применимого законодательства любого иного государства, где компания Роснефть осуществляет деятельность.

3.2. Система обеспечения ИБ представляет собой совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется компания Роснефть в своей деятельности.

3.3. Система управления ИБ является составной частью общей системы управления компании, обеспечивает поддержку и управление процессами обеспечения ИБ на всех этапах деятельности корпоративной информационной системы.

3.4. Роснефть разрабатывает и внедряет систему управления ИБ, отвечающую требованиям и рекомендациям нормативных документов Российской Федерации.

3.5. Основные цели внедрения системы управления ИБ компании Роснефть:

- обеспечить защиту конфиденциальной информации, такой как финансовые данные, планы развития, технические решения и др. Это помогает предотвратить утечки информации, включая утечки от внутренних сотрудников и атаки со стороны злоумышленников.

- обеспечить целостность данные, т.е. гарантировать, что данные остаются целыми и не подвергаются воздействию несанкционированных изменений. Это важно для предотвращения внедрения вредоносного кода и модификации важной информации.

- обеспечить надежную доступность данных и предотвращать атаки, направленные на их недоступность, такие как DDoS-атаки.
- соблюдать законодательные и регуляторные требования, такие как ГОСТ Р ИСО/МЭК 27001, и гарантировать соответствие нормативным актам в сфере ИБ.
- обеспечить средствами для идентификации и управлением рисками, связанными с информационной безопасностью.
- обеспечить бесперебойной работы бизнес-процессов
- обеспечить быстрое обнаружение инцидентов и эффективное реагирование на них, чтобы минимизировать ущерб.

3.6. Положения настоящей Политики распространяются на все виды информации в компании Роснефть, хранящейся либо передающейся любыми способами, в том числе информацию, зафиксированную на материальных носителях.

3.7. Положения настоящей Политики также распространяются на средства приема, обработки, передачи, хранения и защиты информации компании.

3.8. Политика применяется ко всем сотрудникам нефтяной компании.

3.9. Область применения настоящей Политики распространяется на все подразделения Роснефти, в которых обрабатывается информация, не составляющая государственную тайну.

4. НОРМАТИВНЫЕ ССЫЛКИ

При разработке настоящей Политики учтены требования и рекомендации следующих документов:

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- перечень сведений конфиденциального характера, утвержденный Указом Президента РФ от 06 марта 1997 г. № 188;
- методический документ ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах»;
- Концепция информационной безопасности Профессионально-педагогического колледжа имени Гагарина Ю.А., утверждённая приказом от 22 марта 2022 г. № 179-П;
- ГОСТ Р ИСО/МЭК 27001-2021 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»;
- ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения;
- ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности».

5. ОБЩИЕ ПОЛОЖЕНИЯ

5.1 Любое лицо, работающее в нефтяной компании Роснефть, обязано поддерживать конфиденциальность и целостность деловой информации нефтяной компании Роснефть и защищать эту информацию от несанкционированного, незаконного или случайного раскрытия, искажения или уничтожения.

5.2 Защита информационных ресурсов компании Роснефть является обязанностью всех работников компании, а также лиц, работающих по договору гражданско-правового характера, и (или) любой третьей стороны, имеющей доступ к этим ресурсам. Лица, работающие в компании, несут персональную ответственность за выполнение внутренних требований и правил ИБ.

5.3 Знание и соблюдение требований настоящей Политики обязательно для всех работников компании и третьих лиц, использующих информационные ресурсы компании Роснефть.

6. ПОЛОЖЕНИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. Положения по информационной безопасности ПАО Роснефть (далее – «Положения») разрабатываются на основании Политики информационной безопасности компании Роснефть в целях создания, развития и совершенствования общей системы защиты информации нефтяной компании.

6.2. Положения по ИБ являются приложениями к настоящей Политике.

6.3. Правила доступа к информационным ресурсам Банка определены в «Положении о доступе к информационным ресурсам».

6.4. Правила использования паролей определены в «Положении об использовании паролей».

6.5. Программное обеспечение в нефтяной компании используется в соответствии с «Положением об использовании программного обеспечения».

6.6. Правила пользования ресурсами сети в нефтяной компании в Институте указаны в «Положении об использовании сети интернет».

6.7. Правила пользования электронной почтой компании Роснефть указаны в «Положении об использовании электронной почты».

6.8. Правила защиты от вредоносных программ определены в «Положении о защите от вредоносного программного обеспечения».

6.9. Правила использования средств беспроводного доступа приведены в «Положении об использовании средств беспроводного доступа».

6.10. Правила и порядок организации рабочих мест определены в «Положении об организации рабочих мест».

6.11. Общие правила технического обслуживания элементов информационных систем указаны в «Положении о техническом обслуживании».

6.12. Правила классификации информационных ресурсов Банка в целях обеспечения соответствующего уровня их защиты определены в «Положении о классификации информации».

6.13. Инвентаризация информационных систем компании Роснефть проводится в соответствии с «Положением об инвентаризации информационных ресурсов и систем».

6.15. Перечень ролей информационной безопасности и правила управления ролями ИБ приведены в «Положении об управлении ролями информационной безопасности».

6.16. Мониторинг информационной безопасности в компании Роснефть выполняется в соответствии с «Положением о мониторинге событий информационной безопасности».

7. ЗАДАЧИ СИСТЕМЫ УПРАВЛЕНИЯ ИБ

7.1. Основной целью управления ИБ является обеспечение защиты конфиденциальности, целостности и доступности информации и информационных ресурсов компании..

7.2. Основными задачами управления ИБ являются:

- определение идентификации и классификации информации;
- разработка политик и стандартов ИБ;
- осуществление контроля и управления доступом сотрудников и других пользователей к информационным ресурсам;
- осуществление мониторинга и обнаружение инцидентов;
- проведение анализа рисков и разработка стратегий по их снижению;
- разработка процедур реагирования на ИБ-инциденты;
- проведение обучения сотрудников по вопросам ИБ.

7.3. ПАО Роснефть осуществляет деятельность по управлению рисками, повышению осведомленности сотрудников и реагированию на инциденты в области ИБ. Регулярно, не реже одного раза в два года, производится анализ состояния рисков, связанных с ИБ. Защитные меры должны основываться на всесторонней оценке этих рисков и должны быть им соразмерны.

7.4. Всю ответственность за защиту своей информации и информационных ресурсов компании Роснефть возлагается на руководители структурных подразделений нефтяной компании. Сотрудники компании Роснефть обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информацией нефтяной компании, соблюдать требования настоящей Политики ИБ и других документов СОИБ.

8. РЕАЛИЗАЦИЯ

Реализация системы управления ИБ осуществляется на основе четкого распределения ролей и ответственности в области информационной безопасности.

8.1. Структура и ответственность

8.1.1. Ответственное лицо, назначенное приказом Руководителем нефтяной компании Роснефть, руководит работами по внедрению и совершенствованию СУИБ, в том числе организует выполнение Положений по ИБ.

8.1.2. Руководство всеми видами деятельности по управлению ИБ в структурных подразделениях нефтяной компании осуществляют руководители этих подразделений. Они же несут ответственность за выполнение обязательств Положений по ИБ.

8.1.3. Функции администраторов по ИБ возлагаются на штатных работников подразделений компании Роснефть, которые осуществляет свою деятельность во взаимодействии с другими подразделениями компании Роснефть. Координацию их деятельности по защите информации осуществляет ответственное лицо, назначенное Руководителем нефтяной компании Роснефть,

8.1.4. Ответственность работников нефтяной компании Роснефть за надлежащее выполнение требований и правил ИБ определена в положениях, правилах, регламентах и другие внутренних нормативных и организационно распорядительных документах компании Роснефть.

8.1.5. Все работники компании Роснефть несут персональную (должностную, материальную, административную, уголовную) ответственность за свои действия или бездействие, которые повлекут за собой разглашение или утрату конфиденциальных (служебных, коммерческих, персональных) данных, а также нарушение нормального функционирования информационных систем, информационно-телекоммуникационной сети компании.

8.2. Осведомленность и информирование

8.2.1. Для обеспечения эффективного функционирования СУИБ первостепенное значение имеет осведомленность работников компании Роснефть по вопросам информационной безопасности.

8.2.2. Доведение правил ИБ до персонала всех уровней проводится: при приеме на работу; в ходе производственных совещаний, собраний, профессиональной подготовки персонала, тренингов по информационной безопасности.

8.3. Реагирование на инциденты безопасности

8.3.1. Для определения возможных сценариев восстановления информационной системы Организации в чрезвычайных ситуациях, конкретизации технических средств и действий работников и структурных подразделений по локализации инцидентов ИБ должны быть разработаны планы восстановительных работ для важных информационных ресурсов.

8.3.2. Реагирование на инциденты ИБ осуществляется в соответствии с «Положением о реагировании на инциденты информационной безопасности» (Приложение № 2).

9. КОНТРОЛЬ

9.1. Контроль соблюдения требований настоящей Политики возлагается на ответственное лицо, назначенное приказом президента нефтяной компании Роснефть.

9.2. Контроль за актуальностью Политики осуществляет ответственное лицо, назначенное приказом президента нефтяной компании Роснефть.

9.3. Контроль в области информационной безопасности является частью работ по обеспечению ИБ компании Роснефть. Целью контроля ИБ является выявление угроз, предотвращение их реализации, минимизация возможного ущерба.

10. СОВЕРШЕНСТВОВАНИЕ

10.1. На основании утверждённого протокола правлением нефтяной компании Роснефть отдел информационный технологий организует подготовку проектов нормативных и организационно-распорядительных документов (положений, инструкций, регламентов и других), направленных на совершенствование СУИБ.

10.2. Нормативные и организационно-распорядительные документы по ИБ разрабатываются в строгом соответствии с Концепцией и Политикой ИБ нефтяной компании Роснефть.

10.3. Нормативные и организационно-распорядительные документы по ИБ утверждаются приказами по компании Роснефть и рассылаются руководству компании и руководителям подразделений.

10.4. Роснефть будет применять следующий системный подход к обеспечению исполнения требований и правил по ИБ:

10.5. Настоящая Политика информационной безопасности компании Роснефть считается официально принятым документом после его утверждения приказом руководителя компании Роснефть.

10.6. Разработка и внедрение нормативных и организационно-распорядительных документов по ИБ проводится поэтапно.

10.7. Все нормативные и организационно-распорядительные документы по ИБ могут быть приняты, отменены и пересмотрены отдельными приказами и распоряжениями по нефтяной компании Роснефть.