

УТВЕРЖДЕН

Решением Правления

ПАО «НК «Роснефть»

«10» февраля 2017 г.

Протокол от «10» февраля 2017 г. № Пр-ИС-03п

Введен в действие

приказом ПАО «НК «Роснефть»

от «28» марта 2017 г. № 161

ВВЕДЕН В ДЕЙСТВИЕ

Приказом АО «Востсибнефтегаз»

от «10» апреля 2017 г. №335

Вступил в силу «10» апреля 2017 г.

СТАНДАРТ КОМПАНИИ

ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПАО «НК «РОСНЕФТЬ» И ОБЩЕСТВ ГРУППЫ

№ ПЗ-11.01 С-0054

ВЕРСИЯ 1.00

(с изменениями, утвержденными решением Правления ПАО «НК «Роснефть» (протокол заседания от 30.06.2017 №Пр-ИС-22п), введенными в действие приказом ПАО «НК «Роснефть» от 28.08.2017 № 489, введенными в АО «Востсибнефтегаз» приказом от 11.09.2017 №848)

СОДЕРЖАНИЕ

ВВОДНЫЕ ПОЛОЖЕНИЯ	4
НАЗНАЧЕНИЕ.....	4
ОБЛАСТЬ ДЕЙСТВИЯ	4
ПЕРИОД ДЕЙСТВИЯ И ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ	5
1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ	7
2. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ	15
3. ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	17
3.1. НАЗНАЧЕНИЕ ПОЛИТИК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	17
3.2. СООТВЕТСТВИЕ ПОЛИТИК ДЕЙСТВУЮЩЕМУ ЗАКОНОДАТЕЛЬСТВУ	17
3.3. РАСПРЕДЕЛЕНИЕ ОТВЕТСТВЕННОСТИ ЗА РЕАЛИЗАЦИЮ ПОЛИТИК	17
3.4. ОБЛАСТЬ РАСПРОСТРАНЕНИЯ ПОЛИТИК	18
3.4.1. КАТЕГОРИИ ИНФОРМАЦИИ	18
3.4.2. КАТЕГОРИИ ИНФОРМАЦИОННЫХ СИСТЕМ.....	18
3.5. ПОЛИТИКИ ИБ.....	19
3.5.1. ПОЛИТИКА ЭТИКИ ИБ	20
3.5.2. ПОЛИТИКА БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ АВТОМАТИЗИРОВАННЫХ РАБОЧИХ МЕСТ.....	21
3.5.3. ПОЛИТИКА БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ СЕРВЕРНОГО И СЕТЕВОГО ОБОРУДОВАНИЯ.....	23
3.5.4. ПОЛИТИКА БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ЭЛЕКТРОННОЙ ПОЧТЫ	24
3.5.5. ПОЛИТИКА БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ СЕТИ ИНТЕРНЕТ	26
3.5.6. ПОЛИТИКА БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ СЪЕМНЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ.....	27
3.5.7. ПОЛИТИКА БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ БЕСПРОВОДНЫХ СОЕДИНЕНИЙ.....	28
3.5.8. ПОЛИТИКА БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ МОБИЛЬНЫХ АРМ	29
3.5.9. ПОЛИТИКА БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ.....	30
3.5.10. ПОЛИТИКА БЕЗОПАСНОСТИ ПРИ ПРОВЕДЕНИИ ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ	31
3.5.11. ПОЛИТИКА УПРАВЛЕНИЯ РИСКАМИ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	32
3.5.12. ПОЛИТИКА ПРОВЕДЕНИЯ АУДИТОВ ИБ.....	34
3.5.13. ПОЛИТИКА МОНИТОРИНГА СОБЫТИЙ ИБ	36

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

3.5.14.	ПОЛИТИКА УПРАВЛЕНИЯ ИНЦИДЕНТАМИ ИБ.....	37
3.5.15.	ПОЛИТИКА ЗАЩИТЫ СРЕДЫ ВИРТУАЛИЗАЦИИ.....	39
3.5.16.	ПОЛИТИКА УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ	40
3.5.17.	ПОЛИТИКА ПРОТИВОДЕЙСТВИЯ НСД и УТЕЧКАМ ИНФОРМАЦИИ	41
3.5.18.	ПОЛИТИКА УПРАВЛЕНИЯ ДОСТУПОМ.....	42
3.5.19.	ПОЛИТИКА ИСПОЛЬЗОВАНИЯ ПАРОЛЕЙ.....	44
3.5.20.	ПОЛИТИКА ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ	46
3.5.21.	ПОЛИТИКА БЕЗОПАСНОСТИ СЕТЕВОГО ПЕРИМЕТРА	47
3.5.22.	ПОЛИТИКА УДАЛЕННОГО ДОСТУПА В КОРПОРАТИВНУЮ СЕТЬ	50
3.5.23.	ПОЛИТИКА ЗАЩИТЫ ОТ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	50
3.5.24.	ПОЛИТИКА ИСПОЛЬЗОВАНИЯ СЗИ.....	51
3.5.25.	ПОЛИТИКА ИСПОЛЬЗОВАНИЯ СКЗИ.....	52
3.5.26.	ПОЛИТИКА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ НА ЭТАПАХ ЖИЗНЕННОГО ЦИКЛА ИНФОРМАЦИОННЫХ СИСТЕМ.....	54
3.5.27.	ПОЛИТИКА РЕЗЕРВНОГО КОПИРОВАНИЯ ИНФОРМАЦИИ	56
3.5.28.	ПОЛИТИКА ОБУЧЕНИЯ И ПОВЫШЕНИЯ ОСВЕДОМЛЕННОСТИ РАБОТНИКОВ В ОБЛАСТИ ИБ.....	57
4.	ОТВЕТСТВЕННОСТЬ НАРУШИТЕЛЕЙ ПОЛИТИК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	59
5.	ССЫЛКИ.....	60

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

© ® ПАО «НК «Роснефть», 2017

ВВОДНЫЕ ПОЛОЖЕНИЯ

НАЗНАЧЕНИЕ

Настоящий Стандарт разработан с целью определения совокупности правил и требований в области информационной безопасности, которыми руководствуется Компания в своей деятельности, а также обязанности и ответственность за их соблюдение работников Компании и третьих лиц, использующих информационные активы, информационно-технологическую инфраструктуру и средства защиты информации, принадлежащие Компании.

Общая политика информационной безопасности ПАО «НК «Роснефть» и Обществ Группы определяется всей совокупностью локальных нормативных документов, разработанных на основе настоящего Стандарта.

Задачами Стандарта являются:

- определение состава мер обеспечения информационной безопасности общего характера с учётом всех направлений деятельности Компании, существующих в Компании типов объектов защиты, категорий обрабатываемой информации и информационных систем, а также актуальных угроз информационной безопасности;
- определение состава мер обеспечения информационной безопасности общего характера, направленных на повышение эффективности процесса обеспечения информационной безопасности;
- обеспечение соответствия установленных мер обеспечения информационной безопасности общему характеру действующему законодательству.

Стандарт разработан в соответствии с:

- Политикой Компании «Концепция информационно-технической безопасности ПАО «НК «Роснефть» № ПЗ-11.1.
- Стандартом Компании «Охрана сведений конфиденциального характера» № ПЗ-11.03 С-0006.

ОБЛАСТЬ ДЕЙСТВИЯ

Настоящий Стандарт обязателен для исполнения работниками:

- всех структурных подразделений ПАО «НК «Роснефть»;
- дочерних обществ ПАО «НК «Роснефть», 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,

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

задействованными в использовании информационных активов, информационно-технологической инфраструктуры и средств защиты информации, принадлежащих Компании.

Настоящий Стандарт носит рекомендательный характер для исполнения работниками иных Обществ Группы, не являющихся дочерними обществами ПАО «НК «Роснефть».

Требования Стандарта становятся обязательными для исполнения в дочернем обществе ПАО «НК «Роснефть» и ином Обществе Группы, после его введения в действие в Обществе Группы в соответствии с Уставом Общества Группы с учетом специфики условий договоров или соглашений о совместной деятельности и в установленном в Обществе Группы порядке.

Распорядительные, локальные нормативные и иные внутренние документы не должны противоречить настоящему Стандарту.

Настоящий Стандарт не распространяется на область, связанную с использованием и организацией защиты сведений, составляющих государственную тайну.

Структурные подразделения ПАО «НК «Роснефть» и Общества Группы при оформлении договоров с подрядными (сервисными) организациями, осуществляющими деятельность по защите информации, обязаны включить в договоры соответствующие условия, требуемые для соблюдения указанными подрядными (сервисными) организациями, требований, установленных настоящим Стандартом.

ПЕРИОД ДЕЙСТВИЯ И ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ

Стандарт является локальным нормативным документом постоянного действия.

Настоящий Стандарт утверждается, признается утратившим силу в ПАО «НК «Роснефть» решением Правления ПАО «НК «Роснефть» и вводится в действие в ПАО «НК «Роснефть» приказом ПАО «НК «Роснефть».

Изменения в Стандарт вносятся на основании решения Правления ПАО «НК «Роснефть» и вводятся в действие в ПАО «НК «Роснефть» приказом ПАО «НК «Роснефть».

Необходимость актуализации Стандарта определяется не реже чем один раз в три года.

Изменения в Стандарт вносятся в случаях:

- изменений в Концепции информационно-технической безопасности Компании;
- изменений действующего законодательства в области информационной безопасности, способных оказать существенное влияние на состав применяемых защитных мер;
- изменений организационно-штатной структуры ПАО «НК «Роснефть» или структуры бизнеса Компании;
- изменений в составе направлений деятельности Компании;
- изменений в составе используемых информационных технологий;

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

- изменений распределения ответственности за реализацию Стандарта.

При внесении изменений Стандарта могут учитываться:

- результаты аудитов информационной безопасности Компании;
- актуальные угрозы информационной безопасности и уязвимости информационных систем и ресурсов, используемых информационных технологий, инфраструктуры и средств защиты информации Компании;
- отчёты об инцидентах в области информационной безопасности;
- рекомендации органов государственной власти;
- предложения работников.

Инициаторами внесения изменений в Стандарт являются: Служба безопасности ПАО «НК «Роснефть», а также иные структурные подразделения ПАО «НК «Роснефть» и Обществ Группы по согласованию со Службой безопасности ПАО «НК «Роснефть».

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

© ® ПАО «НК «Роснефть», 2017

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ КОРПОРАТИВНОГО ГЛОССАРИЯ

АВТОМАТИЗИРОВАННАЯ СИСТЕМА УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ – система контроля, управления и защиты технологического процесса, построенная на средствах измерения, вычислительной технике и исполнительных устройствах, и механизмах и предназначенная для обеспечения комплексной автоматизации технологических операций на производстве.

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – проверка и оценка соответствия информационной безопасности требованиям законодательства страны, локальных нормативных документов, а также международным стандартам в области обеспечения информационной безопасности.

АУТЕНТИФИКАЦИЯ – проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности).

ВЛАДЕЛЕЦ ИНФОРМАЦИОННОГО АКТИВА – работник Компании, в рамках своих должностных обязанностей и/или должностных полномочий и/или иным образом получивший право обладателя информации, обрабатываемой в информационной системе.

ВЛАДЕЛЕЦ РИСКА – должностное лицо (топ-менеджер ПАО «НК «Роснефть», руководитель Общества Группы или его заместитель, руководитель структурного подразделения ПАО «НК «Роснефть», Общества Группы), которое в соответствии со своими должностными обязанностями несет ответственность за управление данным риском с учетом существующего в Компании процесса принятия решений по управлению рисками.

ВНУТРЕННЯЯ СЕТЬ – внутренний участок корпоративной сети, отделенный от внешней сети (сети Интернет) и демилитаризованной зоны межсетевым экраном.

ГОСУДАРСТВЕННАЯ ТАЙНА - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации [Федеральный закон от 21.07.1993 № 5485-1 «О государственной тайне»].

ДЕМИЛИТАРИЗОВАННАЯ ЗОНА - участок корпоративной сети, расположенный между внешним межсетевым экраном и внешним маршрутизатором, используемым для подключения корпоративной сети к сети телекоммуникационных провайдеров (сети Интернет).

Примечание: в демилитаризованной зоне размещаются серверы, используемые для взаимодействия и предоставления сетевых сервисов внешним пользователям корпоративной сети, а также серверы, которые по соображениям информационной безопасности не целесообразно размещать во внутренней сети ПАО «НК «Роснефть».

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

ДОСТУП К ИНФОРМАЦИИ – возможность получения информации и ее использования, а также возможность пользователя работать с данными в структурированном хранилище данных.

ДОСТУПНОСТЬ ИНФОРМАЦИИ – состояние информации, характеризующееся способностью информационной системы обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

ЖИЗНЕННЫЙ ЦИКЛ ИНФОРМАЦИОННОЙ СИСТЕМЫ – непрерывный процесс, начинающийся с момента принятия решения о необходимости создания информационной системы и заканчивающийся в момент ее полного изъятия из эксплуатации.

ИДЕНТИФИКАЦИЯ – процедура, в результате которой для субъекта идентификации выявляется его идентификатор, однозначно определяющий этого субъекта в информационной системе.

Примечание: Для выполнения процедуры идентификации в информационной системе субъекту предварительно должен быть назначен соответствующий идентификатор (т.е. проведена регистрация субъекта в информационной системе).

ИНСАЙДЕРСКАЯ ИНФОРМАЦИЯ ПАО «НК «РОСНЕФТЬ» – точная и конкретная информация, которая не была распространена или предоставлена ПАО «НК «Роснефть» (в том числе сведения, составляющие коммерческую, служебную и иную охраняемую законом тайну), распространение или предоставление которой может оказать существенное влияние на цены финансовых инструментов ПАО «НК «Роснефть», и включенная в Перечень сведений, относящихся к инсайдерской информации ПАО «НК «Роснефть».

ИНФОРМАЦИЯ ДЛЯ ВНУТРЕННЕГО ПОЛЬЗОВАНИЯ – информация, не подпадающая под остальные категории, доступ к которой должен быть ограничен определенной категорией лиц.

Примечание: Решение об ограничении доступа на законных основаниях принимает владелец информационного актива.

ИНФОРМАЦИЯ «ДЛЯ СЛУЖЕБНОГО ПОЛЬЗОВАНИЯ» (СЛУЖЕБНАЯ ТАЙНА) – несекретная служебная информация ограниченного распространения с пометкой «Для служебного пользования», ограничения на распространение и передачу которой диктуются служебной необходимостью. Режим обращения и содержание информации «для служебного пользования» определяется в Компании с учетом положений Постановления Правительства Российской Федерации от 03.11.1994 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии».

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ – состояние защищенности информационной среды, обеспечивающее ее формирование, использование и развитие в интересах Компании.

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

ИНФОРМАЦИЯ, СОСТАВЛЯЮЩАЯ КОММЕРЧЕСКУЮ ТАЙНУ (СЕКРЕТ ПРОИЗВОДСТВА) – сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

ИНФОРМАЦИОННЫЕ АКТИВЫ – информационные системы и информационные ресурсы, сформированные в их рамках.

Примечание: информационные активы могут входить в список конфигурационных единиц.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ – совокупность процессов, методов поиска, сбора, хранения, обработки, представления и распространения информации, а также способы осуществления таких процессов и методов на базе информационно-коммуникационных технологий и технических средств (включая средства производственной автоматизации, метрологии и контроля качества сырья и продукции) в целях обеспечения и поддержки деятельности Компании.

ИНФОРМАЦИОННЫЙ РЕСУРС – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий, используемая в бизнес-процессах Компании, формируемая в рамках существующих информационных систем.

ИНФОРМАЦИОННАЯ СИСТЕМА – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств [Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»].

ИНЦИДЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – появление одного или нескольких нежелательных или неожиданных событий информационной безопасности, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы нарушения информационной безопасности [ГОСТ Р ИСО/МЭК ТО 18044-2007].

ИНФОРМАЦИЯ – сведения (сообщения, данные) независимо от формы их представления [Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»].

КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ (СВЕДЕНИЯ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА) - сведения, содержащие информацию, составляющую коммерческую тайну Компании, информацию, являющуюся информацией «Для служебного пользования», инсайдерскую информацию, а также персональные данные.

КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим

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

лицам без согласия ее обладателя [Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»].

КУРАТОР РИСКА – должностное лицо (топ-менеджер ПАО «НК «Роснефть»)), которое в соответствии со своими должностными обязанностями осуществляет действия, направленные на эффективное управление межфункциональным риском. Объем действий, выполняемых Куратором риска, варьируется в зависимости от межфункционального риска, начиная с общей методологической поддержки Владельцев риска и заканчивая организацией и контролем исполнения всех работ по управлению межфункциональным риском.

ЛОКАЛЬНАЯ ВЫЧИСЛИТЕЛЬНАЯ СЕТЬ – группа электронно- вычислительных машин, а также периферийное оборудование, объединенные одним или несколькими автономными высокоскоростными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.

МЕЖСЕТЕВОЙ ЭКРАН – комплекс аппаратных и программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с текущей политикой.

МЕЖФУНКЦИОНАЛЬНЫЙ РИСК – риск, управление которым относится к ответственности двух и более Владельцев риска.

НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП – доступ к информации, нарушающий установленные правила разграничения доступа.

ОТКРЫТАЯ ИНФОРМАЦИЯ – информация, полученная от физических или юридических лиц, запрет на распространение и обработку которой был ими официально снят или не был установлен. Информация, сформированная в результате деятельности Компании, которую запрещено относить к коммерческой тайне на основании законодательства Российской Федерации. Информация, представляемая в публичный доступ и с которой сняты грифы конфиденциальности в соответствии с корпоративными требованиями, используемая в хозяйственной деятельности Компании или имеющая значение для имиджа Компании.

ПЕРСОНАЛЬНЫЕ ДАННЫЕ – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) [Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»].

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ – совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ. [ГОСТ 19781-90].

Примечание: Под программным обеспечением подразумевается:

- программное обеспечение, приобретенное или разработанное по заказу ПАО «НК «Роснефть» (информационные системы, подсистемы, информационные ресурсы), которые могут сопровождаться проектной доработкой или разработкой функций, дополняющих стандартные (базовые) возможности;

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

- *стандартное программное обеспечение, поставляемое на условиях «как есть», с одинаковыми для всех покупателей функциями.*

ПУБЛИЧНАЯ ИНФОРМАЦИЯ – открытая информация, находящаяся в публичном доступе.

РОЛЬ – совокупность полномочий, предоставляемых участнику процесса, необходимых для выполнения бизнес-задач в зоне его ответственности.

СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ – средства шифрования, средства имитозащиты, средства электронной подписи, средства изготовления ключевых документов (независимо от вида носителя ключевой информации), ключевые документы (независимо от вида носителя ключевой информации).

УЧЕТНАЯ ЗАПИСЬ ПОЛЬЗОВАТЕЛЯ - персонифицированная запись, характеризующаяся уникальным именем пользователя, присваиваемым пользователю при его регистрации в корпоративной информационной сети, и соответствующим ей паролем.

УЯЗВИМОСТЬ ИНФОРМАЦИОННОЙ СИСТЕМЫ – свойство информационной системы, обуславливающее возможность реализации угроз информационной безопасности, обрабатываемой в ней информации [Р 50.1.056-2005].

ЦЕЛОСТНОСТЬ ИНФОРМАЦИИ – состояние информации, при котором отсутствует любое её изменение, либо изменение осуществляется только преднамеренно субъектами, имеющими на него право [Р 50.1.056-2005].

ЭСКАЛАЦИЯ – деятельность, направленная на получение дополнительных ресурсов, когда это необходимо для достижения целевых показателей уровня ИТ услуги или ожиданий ИТ заказчиков.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ ДЛЯ ЦЕЛЕЙ НАСТОЯЩЕГО ДОКУМЕНТА

ДОВЕРЕННАЯ СЕТЬ – локальная вычислительная сеть, приведенная в соответствие требованиям Положения Компании «Требования к защите локальных вычислительных сетей Компании, подключаемых в единую корпоративную телекоммуникационную систему ПАО «НК «Роснефть» № ПЗ-11.01 Р-0123.

ЗАЩИТА ИНФОРМАЦИИ – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ – технологическая инфраструктура и сервисы, обеспечивающие безопасность информационных и коммуникационных систем на основе использования криптографических алгоритмов и сертификатов ключей подписей.

КОРПОРАТИВНАЯ СЕТЬ КОМПАНИИ – объединение информационных систем, компьютерного, телекоммуникационного и офисного оборудования всех структурных подразделений ПАО «НК «Роснефть» или Общества Группы, посредством их подключения к

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

единой компьютерной сети передачи данных с использованием различных физических и логических каналов связи.

КЛЮЧЕВАЯ (КРИТИЧЕСКИ ВАЖНАЯ) СИСТЕМА ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ – информационно-управляющая или информационно-телекоммуникационная система, которая осуществляет управление критически важным объектом (процессом), или информационное обеспечение управления таким объектом (процессом), или официальное информирование граждан и в результате деструктивных информационных воздействий на которую может сложиться чрезвычайная ситуация или будут нарушены выполняемые системой функции управления со значительными негативными последствиями.

КОНТРОЛИРУЕМАЯ ЗОНА – пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание работников и посетителей ПАО «НК «Роснефть» или Общества Группы, а также транспортных средств.

КРИТИЧЕСКИ ВАЖНЫЙ ОБЪЕКТ – объект, оказывающий существенное влияние на национальную безопасность Российской Федерации, прекращение или нарушение функционирования которого приводит к чрезвычайной ситуации или к значительным негативным последствиям для обороны, безопасности, международных отношений, экономики, другой сферы хозяйства или инфраструктуры страны, либо для жизнедеятельности населения, проживающего на соответствующей территории, на длительный период времени.

МОБИЛЬНОЕ АВТОМАТИЗИРОВАННОЕ РАБОЧЕЕ МЕСТО – переносные малогабаритные электронные средства или системы, имеющие возможность размещения и обработки на них с помощью программного обеспечения информации, а так же обмена этой информацией с другими электронными средствами или системами.

Примечание: В Компании в качестве мобильных рабочих мест рассматриваются портативные вычислительные устройства и устройства связи с возможностью хранения информации (ноутбуки, нетбуки, планшеты, смартфоны и иные устройства).

НЕОТКАЗУЕМОСТЬ — способность удостоверять имевшее место действие или событие так, чтобы эти события или действия не могли быть позже отвергнуты. Например, невозможность отправителя (автора) документа или сообщения отказаться от факта отправки (подписи) данного документа или сообщения.

ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ - информационно-технологическая концепция, подразумевающая обеспечение повсеместного и удобного сетевого доступа по требованию к общему пулу конфигурируемых вычислительных ресурсов, которые могут быть оперативно предоставлены и освобождены с минимальными эксплуатационными затратами или обращениями к провайдеру.

ОДНОРАНГОВАЯ (БЕСПРОВОДНАЯ) СЕТЬ – децентрализованная (беспроводная) вычислительная сеть, основанная на равноправии участников и не имеющая постоянной структуры. В одноранговой (беспроводной) вычислительной сети группа клиентских

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

вычислительных устройств объединяется друг с другом для возможности совместного использования ресурсов и данных пользователями.

ОПЕРАЦИОННАЯ СИСТЕМА – системная программа, осуществляющая взаимодействие пользователя и прикладных программ с аппаратной частью рабочих мест.

ПАРОЛЬ – секретное условное слово или секретный набор знаков, предназначенный для подтверждения личности или полномочий субъекта.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – совокупность документированных правил и требований, направленных на обеспечение безопасности информации и информационных процессов в Компании.

ПОЛЬЗОВАТЕЛЬ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ (ПОЛЬЗОВАТЕЛЬ) – работник Компании (штатный, временный, работающий по договору и т.п.), а также прочие лица (подрядчики, аудиторы и т.п.), легитимно зарегистрированный в корпоративной сети Компании и получивший права на доступ к ресурсам корпоративной сети в соответствии со своими функциональными обязанностями.

ПУБЛИЧНЫЕ ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ – вычислительная инфраструктура, доступ к которой неограничен и предназначенная для использования широким кругом лиц.

РАБОЧЕЕ МЕСТО – персональный компьютер, на котором пользователь сети выполняет свои служебные обязанности.

СЕКМЕНТ ДОСТУПА – сегмент вычислительной сети, из которого и/или в который осуществляется доступ. В качестве сегмента могут выступать как сами вычислительные сети целиком (локальная вычислительная сеть, Интернет), так и их отдельные части (сегмент локальной вычислительной сети, демилитаризованная зона, изолированный компьютер).

СЕРВЕР – совокупность средств вычислительной техники и программных средств, предназначенная для управления, хранения, представления информации в локальной вычислительной сети для рабочих мест и других сетевых устройств.

СОБЫТИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью.

СЪЕМНЫЕ НОСИТЕЛИ ИНФОРМАЦИИ – переносные малогабаритные технические и электронные средства, предназначенные или имеющие возможность для переноса информации с одного компьютера на другой без использования каналов связи, предоставляемых локальной вычислительной сетью, устройство для длительного хранения данных, конструктивно выполненное отдельно.

Примечание: В Компании в качестве съемных носителей информации рассматриваются как машинные носители информации (флэш-накопители, внешние

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

накопители на жестких дисках и иные устройства), так и медиа-носители (CD/DVD-диски, дискеты, ленты, кассеты и т. д.).

УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – угроза нарушения свойств информационной безопасности - доступности, целостности или конфиденциальности информационных активов.

ЧАСТНЫЕ ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ – вычислительная инфраструктура с ограниченным доступом в интересах ограниченного круга лиц.

ЭШЕЛОНИРОВАННАЯ ЗАЩИТА (ИНФОРМАЦИИ) – многоуровневая защита, состоящая из набора уровней (эшелонов), использующих различные контрмеры, что приводит к общему снижению вероятности реализации угроз информационной безопасности. В качестве уровней (эшелонов) могут выступать: уровень организационных мер, уровень физической защиты, уровень защиты периметра сети, уровень защиты внутренней сети, уровень защиты узлов сети, уровень защиты приложений, уровень защиты данных.

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

© ® ПАО «НК «Роснефть», 2017

2. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АРМ – автоматизированное рабочее место.

АСУ ТП - автоматизированная система управления технологическим процессом.

ДМЗ – демилитаризованная зона.

ИА – информационный актив.

ИБ – информационная безопасность.

РКИ – инфраструктура открытых ключей.

ИР – информационный ресурс

ИС – информационная система.

ИСПДн – информационная система персональных данных.

КОМПАНИЯ – группа юридических лиц различных организационно-правовых форм, включая ПАО «НК «Роснефть», в отношении которых последнее выступает в качестве основного или преобладающего (участвующего) общества.

КСИИ – ключевая (критически важная) система информационной инфраструктуры.

ЛВС – локальная вычислительная сеть.

ЛНД – локальный нормативный документ ПАО «НК «Роснефть»/Компании/Общества Группы.

МАРМ – мобильное автоматизированное рабочее место.

НСД – несанкционированный доступ.

ОБЩЕСТВО ГРУППЫ (ОГ) – хозяйственное общество, прямая и (или) косвенная доля владения ПАО «НК «Роснефть» акциями или долями в уставном капитале которого составляет 20 процентов и более.

ПО – программное обеспечение.

СБ – Служба безопасности ПАО «НК «Роснефть» или структурное подразделение Общества Группы, ответственное за контроль соблюдения требований защиты информации.

СЗИ – средство защиты информации.

СКЗИ – средство криптографической защиты информации.

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

СТРУКТУРНОЕ ПОДРАЗДЕЛЕНИЕ (СП) – структурное подразделение ПАО «НК «Роснефть» или Общества Группы с самостоятельными функциями, задачами и ответственностью в рамках своей компетенции, определенной Положением о структурном подразделении.

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

© ® ПАО «НК «Роснефть», 2017

3. ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. НАЗНАЧЕНИЕ ПОЛИТИК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Под ИБ Компании понимается состояние защищенности ее интересов в условиях угроз ИБ в информационной сфере, достигаемое путем обеспечения сохранения должного уровня конфиденциальности, целостности и доступности информационных активов, информационно-технологической инфраструктуры и СЗИ Компании.

Обеспечение ИБ должно достигаться за счет комплексного использования всей совокупности организационно-режимных, инженерно-технических, технических, программных методов и СЗИ, а также осуществления непрерывного, всестороннего контроля эффективности реализованных мер по обеспечению ИБ. Указанные меры должны обеспечивать эффективную защиту информации на протяжении всего ее жизненного цикла.

Политики ИБ относятся к организационным мерам защиты информации.

Политики определяют основные правила и требования по организации соответствующих направлений обеспечения ИБ и управления ИБ.

Выбор конкретных методов и СЗИ должен осуществляться на основе правил и требований Политик ИБ, с учетом действующего законодательства и экономической целесообразности.

В зарубежных Обществах Группы и совместных предприятиях процесс обеспечения ИБ регламентируется Положением Компании «Обеспечение информационной безопасности зарубежных Обществ Группы и совместных предприятий» № ПЗ-11.01 Р-0088.

3.2. СООТВЕТСТВИЕ ПОЛИТИК ДЕЙСТВУЮЩЕМУ ЗАКОНОДАТЕЛЬСТВУ

Правовую основу Политик составляют Конституция Российской Федерации, законы Российской Федерации и другие законодательные акты, определяющие права и ответственность граждан, организаций и государства в сфере безопасности, а также руководящие, нормативные, отраслевые (ведомственные) документы по вопросам безопасности информации, утвержденные органами государственного управления различного уровня в пределах их компетенции. Деятельность по обеспечению ИБ Компании строится в строгом соответствии с указанной правовой основой.

3.3. РАСПРЕДЕЛЕНИЕ ОТВЕТСТВЕННОСТИ ЗА РЕАЛИЗАЦИЮ ПОЛИТИК

Распределение ответственности между должностными лицами, СП и сторонними организациями за реализацию Политик приведено в Стандарте ПАО «НК «Роснефть» «Разграничение полномочий и ответственности при организации обеспечения информационной безопасности ПАО «НК «Роснефть» № ПЗ-11.1 СЦ-001.01 ЮЛ-001.

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

3.4. ОБЛАСТЬ РАСПРОСТРАНЕНИЯ ПОЛИТИК

Правила и требования Политик распространяются на:

- информационные ресурсы и информацию, обрабатываемую в Компании, независимо от формы ее представления (передаваемую по каналам связи, зафиксированную на материальном носителе, представленную в аудио-визуальном виде и т.д.);
- ИС, находящиеся в собственности или распоряжении Компании (в отношении которых Компания может устанавливать требования по защите);
- ключевые системы информационной инфраструктуры, включая автоматизированные системы управления технологическими процессами, расположенные на промышленных объектах Компании;
- информационно-технологическую инфраструктуру, включая инфраструктурные сервисы, телекоммуникационное оборудование и каналы связи, обеспечивающие передачу информации между ИС и информационное взаимодействие участников информационного обмена;
- персонал Компании, вовлеченный в процессы сбора, накопления, систематизации, обработки, передачи и хранения информации, обрабатываемой в Компании СЗИ, ИС и подсистемы защиты, обеспечивающие реализацию и контроль мер по защите информации.

Приоритетность задач по обеспечению ИБ перечисленных объектов защиты определяется категориями защищаемой информации и ИС.

3.4.1. КАТЕГОРИИ ИНФОРМАЦИИ

В Компании устанавливаются следующие категории информации, подлежащей защите:

- ОТКРЫТАЯ
- ПУБЛИЧНАЯ
- СВЕДЕНИЯ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА
- ГОСУДАРСТВЕННАЯ ТАЙНА
- ИНФОРМАЦИЯ ДЛЯ ВНУТРЕННЕГО ПОЛЬЗОВАНИЯ.

3.4.2. КАТЕГОРИИ ИНФОРМАЦИОННЫХ СИСТЕМ

В Компании определены следующие категории ИС, подлежащих защите:

- ПУБЛИЧНЫЕ ИС – ИС, предназначенные для обработки информации категории «ПУБЛИЧНАЯ»;
- ОТКРЫТЫЕ ИС – ИС, предназначенные для обработки информации категории «ОТКРЫТАЯ»;
- ИС, ОБРАБАТЫВАЮЩИЕ СВЕДЕНИЯ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА – ИС, предназначенные для обработки информации подкатегорий «коммерческая тайна»,

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

«служебная тайна» и «инсайдерская информация» категории «СВЕДЕНИЯ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА»;

- ИСПДн – ИС, предназначенные для обработки информации «персональные данные»;
- АСУ ТП;
- КСII;
- ВНУТРЕННИЕ ИС – ИС, предназначенные для обработки информации категории «ИНФОРМАЦИЯ ДЛЯ ВНУТРЕННЕГО ПОЛЬЗОВАНИЯ».

3.5. ПОЛИТИКИ ИБ

Политики ИБ подразделяются на следующие группы:

- организационные политики;
- политики, ориентированные на задачи и системы.

К организационным политикам относятся:

- политика этики ИБ;
- политика безопасности при использовании АРМ;
- политика безопасности при использовании серверного и сетевого оборудования;
- политика безопасности при использовании электронной почты;
- политика безопасности при использовании сети Интернет;
- политика безопасности при использовании съемных носителей информации;
- политика безопасности при использовании беспроводных соединений;
- политика безопасности при использовании МАРМ;
- политика безопасности при использовании облачных вычислений;
- политика безопасности при проведении технического обслуживания.

К политикам, ориентированным на задачи и системы, относятся:

- политика управления рисками нарушения ИБ;
- политика проведения аудитов ИБ;
- политика мониторинга событий ИБ;
- политика управления инцидентами ИБ;
- политика обеспечения непрерывности деятельности;
- политика управления уязвимостями;
- политика противодействия утечкам информации;
- политика управления доступом;
- политика использования паролей;

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

- политика физической безопасности;
- политика безопасности сетевого периметра;
- политика удаленного доступа в корпоративную сеть;
- политика защиты от вредоносного программного обеспечения;
- политика использования СЗИ;
- политика использования СКЗИ;
- политика обеспечения безопасности на этапах жизненного цикла ИС;
- политика резервного копирования информации;
- политика обучения и повышения осведомленности работников в области ИБ.

3.5.1. ПОЛИТИКА ЭТИКИ ИБ

3.5.1.1. НАЗНАЧЕНИЕ

Политика определяет основные этические принципы в области ИБ, которыми должны руководствоваться работники Компании в профессиональной деятельности, внутрикорпоративном взаимодействии, личном развитии и самореализации. 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 ИБ.

3.5.1.2. ПОЛОЖЕНИЯ ПОЛИТИКИ

Профессиональные этические принципы работников в ходе обеспечения ИБ Компании:

- соблюдение конфиденциальности: в части данного принципа следует руководствоваться пунктом 3.2. «Кодекса деловой и корпоративной этики НК «Роснефть» № ПЗ-01.06 П-01;
- честность и добросовестность: выполнение функциональных обязанностей осуществляется работником только в рамках действующих требований законодательства и ЛНД в области ИБ. Работники осознанно отвергают возможность вовлечения в противозаконную деятельность или деятельность, приводящую к нарушению ИБ Компании;
- объективность, взвешенность и корректность: оценки, выводы, заключения и мнения должны быть основаны на источниках информации только при полном отсутствии сомнений в их достоверности и объективности. Отсутствие полной уверенности в достоверности и объективности источников информации должно быть четко и акцентированно раскрыто;
- профессионализм и компетентность: работники могут участвовать только в тех процессах обеспечения ИБ, которые они могут реализовать с надлежащим качеством в силу имеющихся у них знаний, опыта и компетенций, и обязаны информировать

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

руководителя о возникновении ситуации, в которой данное правило может быть нарушено;

- сотрудничество, конструктивность и уважение: работники не могут являться инициаторами и не поддерживают отношения нездоровой конкуренции между СП и между другими работниками, которая, в том числе, может привести к нарушению ИБ Компании;
- приоритет корпоративных интересов: работники осознают приоритет корпоративных интересов перед личной заинтересованностью и не допускают того, чтобы их действия привели к нарушению ИБ Компании;
- достоверность: работники должны предоставлять без искажений актуальную и достоверную информацию о текущем состоянии ИБ Компании при формировании ответов на запросы уполномоченных работников Компании (например, при проведении аудитов ИБ или выявлении причин возникновения инцидентов ИБ);
- осведомленность: работники должны быть осведомлены о правилах обеспечения ИБ Компании, а также принимать участие в осведомлении других работников Компании.

3.5.2. ПОЛИТИКА БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ АВТОМАТИЗИРОВАННЫХ РАБОЧИХ МЕСТ

3.5.2.1. НАЗНАЧЕНИЕ

Политика определяет правила и требования обеспечения ИБ при использовании АРМ.

3.5.2.2. ПОЛОЖЕНИЯ ПОЛИТИКИ

Доступ к АРМ предоставляется пользователям после прохождения вводного инструктажа и обязательного внутреннего обучения по ИБ.

АРМ, на которых предполагается обрабатывать сведения конфиденциального характера, должны быть закреплены за соответствующими работниками Компании. Работники должны использовать только АРМ, закрепленные за ними¹. Допускается поочередное использование одного АРМ несколькими работниками одного подразделения в пределах одного рабочего дня/смены при выполнении следующих условий:

- необходимость указанного поочередного использования обусловлена особенностями реализации соответствующего бизнес-процесса;
- каждый работник при поочередном использовании одного АРМ должен работать в собственном пользовательском рабочем сеансе, исключаящем НСД к информации и доступам других пользователей данного АРМ.

¹ Допускается закрепление АРМ за несколькими работниками, в случае если данный подход обусловлен посменным графиком работы. При этом, за соблюдение требований по работе с АРМ ответственность несут, как сами работники, так и их непосредственный руководитель в пределах своих должностных обязанностей.

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

Обработка на АРМ сведений конфиденциального характера в присутствии лиц, не допущенных к данной информации, должна осуществляться с соблюдением мер предосторожности, исключающих возможность неправомерного ознакомления с обрабатываемой информацией.

Запрещается подключать к АРМ личные съемные носители информации и МАРМ, а также создавать папки общего доступа на базе АРМ.

На время своего отсутствия на рабочем месте, работник должен переводить АРМ в режим блокировки или осуществлять выключение установленным порядком.

Пользователям АРМ должно быть запрещено неавторизованное и необоснованное служебной необходимостью использование привилегированных прав доступа, в том числе позволяющих самостоятельно устанавливать новое ПО или изменять конфигурацию существующего ПО на АРМ.

На АРМ должно устанавливаться только разрешенное к установке ПО. Пользователям запрещается устанавливать неавторизованное ПО на АРМ. Должны приниматься меры, направленные на исключение возможности и выявление фактов установки и использования на АРМ не разрешенного к установке ПО.

Для типовой настройки АРМ необходимо использовать эталонные образы операционной системы, подготовленные в соответствии с требованиями Стандарта Компании «Информационные технологии. Требования к автоматизированным рабочим местам пользователей корпоративной сети Компании» № ПЗ-04 С-0014.

Системные блоки АРМ должны быть опломбированы. Должны осуществляться периодические проверки целостности пломб системных блоков АРМ.

Информация, хранящаяся на АРМ, должна своевременно уничтожаться гарантированным способом, исключающим или существенно затрудняющим ее восстановление перед передачей АРМ новому работнику Компании.

При выводе из эксплуатации машинных носителей информации в составе АРМ, на которых осуществлялись хранение и обработка сведений конфиденциального характера, если гарантированное уничтожение информации на АРМ невозможно, используемый носитель информации должен быть утилизирован с использованием средств, осуществляющих размагничивание носителя либо его физическое разрушение, не позволяющее впоследствии восстановить хранившуюся на нем информацию.

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

3.5.3. ПОЛИТИКА БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ СЕРВЕРНОГО И СЕТЕВОГО ОБОРУДОВАНИЯ

3.5.3.1. НАЗНАЧЕНИЕ

Политика определяет правила и требования обеспечения ИБ при использовании серверного и сетевого оборудования.

3.5.3.2. ПОЛОЖЕНИЯ ПОЛИТИКИ

На серверное и сетевое оборудование должно устанавливаться только разрешенное к установке ПО. Перечень разрешенного к установке ПО должен быть определен в эксплуатационной документации на систему, в состав которой входит данное оборудование. Необходимо периодически проводить проверки с целью выявления неразрешенного к установке ПО.

Параметры настроек безопасности серверного и сетевого оборудования должны соответствовать рекомендациям производителя и должны быть отражены в эксплуатационной документации.

Физический и сетевой доступ к серверному и сетевому оборудованию, а также к их диагностическим и конфигурационным портам, должен предоставляться только работникам ответственных за их эксплуатацию СП для исполнения своих должностных обязанностей.

Сетевой доступ к серверному и сетевому оборудованию должен предоставляться только после успешного прохождения процедур идентификации и аутентификации.

Запрещено обрабатывать информацию различных категорий конфиденциальности на одном физическом или виртуальном сервере. Обработка информации одной категории конфиденциальности на одном физическом или виртуальном сервере в рамках различных ИС допускается по согласованию с СБ.

Запрещается подключать к серверному и сетевому оборудованию личные съемные носители информации и МАРМ.

При выводе серверного и сетевого оборудования из эксплуатации информация, хранящаяся на них, должна уничтожаться гарантированным способом, исключающим или существенно затрудняющим их восстановление на носителе.

В случае если гарантированное уничтожение технологической информации на серверном и сетевом оборудовании невозможно, используемый носитель информации должен быть утилизирован с использованием средств, осуществляющих размагничивание носителя либо его физическое разрушение, не позволяющее впоследствии восстановить хранившуюся на нем информацию.

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

3.5.4. ПОЛИТИКА БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ЭЛЕКТРОННОЙ ПОЧТЫ

3.5.4.1. НАЗНАЧЕНИЕ

Политика определяет правила и требования обеспечения ИБ при использовании электронной почты Компании.

3.5.4.2. ПОЛОЖЕНИЯ ПОЛИТИКИ

Использование электронной почты должно быть санкционировано в соответствии с действующей процедурой предоставления доступа к информационным активам и производиться посредством электронных почтовых адресов в почтовом(ых) домене(ах) Компании.

Доступ к электронной почте Компании должен предоставляться работникам только в целях исполнения ими должностных обязанностей. Все сообщения, созданные, переданные или полученные с помощью системы электронной почты Компании, являются и остаются собственностью Компании. Они не могут быть личной собственностью ни одного из ее работников. Компания оставляет за собой право распоряжаться на свое усмотрение (контролировать, перехватывать, просматривать, изымать и т.д.) всеми сообщениями, созданными, полученными или переданными с помощью системы электронной почты Компании. Содержание любого сообщения электронной почты Компании может быть доведено до сведения должностных лиц в пределах Компании без разрешения работника.

Информация для внутреннего пользования, передаваемая с использованием электронной почты за пределы контролируемой зоны Компании, должна быть защищена от несанкционированного доступа.

Передача сведений конфиденциального характера средствами электронной почты без использования сертифицированных технических средств защиты информации запрещена.

Факты отправки и приема сообщений электронной почты должны централизованно фиксироваться, а сообщения – централизованно сохраняться. Должно осуществляться централизованное резервное копирование всех ящиков электронной почты Компании в рамках установленных лимитов объемов хранения данных в ящиках электронной почты.

Перед отправкой сообщений электронной почты необходимо проверять правильность указания адресов получателей. Пользователи должны тщательно продумывать содержание сообщений электронной почты и прикладываемых электронных документов, как если бы это было рукописное послание.

Ко всем исходящим сообщениям электронной почты, направляемым внешним адресатам, должно централизованно добавляться следующее предупреждение, ограничивающее неправомерное распространение и использование содержащейся в сообщении информации, а также снимающее ответственность с Компании за возможно причиненный в связи с этим

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

вред: «Настоящее сообщение (включая любые приложения к нему) предназначено только для указанного в нем адресата. Если данное сообщение попало к Вам по ошибке, пожалуйста, незамедлительно проинформируйте об этом его отправителя, а само сообщение уничтожьте. Настоящим Вам также сообщается, что любое несанкционированное раскрытие, копирование или распространение данного сообщения или совершение каких-либо действий, основанных на информации, содержащейся в нем, строго запрещено. Содержащиеся в сообщении утверждения не являются официальной позицией ПАО «НК «Роснефть», если иное прямо не указано отправителем».

Должны приниматься меры, направленные на предотвращение доставки анонимных не запрошенных сообщений, в том числе рекламного характера (спама).

Пользователям электронной почты строго запрещается:

- использовать для работы с электронной почтой любые внешние сервисы электронной почты (mail.ru, yandex.ru, gmail.com и др.), если это не связано с исполнением должностных обязанностей. В этом случае возможность использования необходимо согласовать со линейным руководителем и СБ;
- рассылать сообщения, нарушающие требования действующего законодательства Российской Федерации, нормы корпоративной этики и культуры, а также авторские и смежные права других лиц или представляющие собой любую форму преследования личности, сообщения, передаваемые «по цепочке» («письма счастья» и т. д.), сообщения рекламного или агитационного характера (спам);
- осуществлять массовые рассылки работникам Компании, не связанные с рабочими целями;
- настраивать автоматическую переадресацию, направляющую входящие сообщения с корпоративного почтового адреса на внешние электронные почтовые адреса;
- переходить по ссылкам и открывать вложенные файлы в сообщениях, полученных от неизвестных адресатов;
- публиковать свой корпоративный электронный адрес либо корпоративные электронные адреса других работников Компании на ресурсах сети Интернет (форумы, конференции и т. п.). Исключение – выполнение должностных обязанностей отдельными категориями работников, которым делегировано право представлять интересы Компании;
- использовать почтовые учетные записи других работников для пересылки сообщений от чужого имени, если это не входит в должностные обязанности и не санкционировано в соответствии с действующей процедурой предоставления доступа к информационным активам;
- предоставлять работникам Компании и третьим лицам доступ к своему электронному почтовому ящику, если иное не санкционировано в соответствии с действующей процедурой предоставления доступа к информационным активам.

Компания оставляет за собой право не производить доставку сообщения электронной почты в случае его несоответствия требованиям Политики.

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

3.5.5. ПОЛИТИКА БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ СЕТИ ИНТЕРНЕТ

3.5.5.1. НАЗНАЧЕНИЕ

Политика определяет правила и требования обеспечения ИБ при использовании сети Интернет.

3.5.5.2. ПОЛОЖЕНИЯ ПОЛИТИКИ

В Компании разрешен только контролируемый доступ к сети Интернет. Доступ к сети Интернет должен предоставляться работникам только в целях исполнения функциональных обязанностей. Самостоятельная установка программно-аппаратных средств доступа и работы с ресурсами сети Интернет запрещена.

Сведения конфиденциального характера, передаваемые посредством сети Интернет, должны быть защищены от НСД.

Пользователям сети Интернет строго запрещается:

- использовать сеть Интернет в целях, способных нанести вред репутации Компании;
- использовать сеть Интернет в целях, противоречащих законодательству Российской Федерации;
- использовать корпоративные реквизиты доступа (имя пользователя в ИС Компании, пароль, адрес электронной почты) при регистрации на ресурсах сети Интернет (сайтах социальных сетей, Интернет-магазинах и пр.), а также публиковать их в сети Интернет;
- посещать ресурсы сети Интернет, не имеющие отношения к выполнению должностных обязанностей (сайты знакомств, социальные сети и др.);
- использовать файлообменные сети для хранения, передачи/получения информации, принадлежащей Компании, ее партнерам, клиентам или контрагентам;
- использовать анонимные прокси-серверы;
- загружать из сети Интернет любое программное обеспечение, музыкальные и видеофайлы (за исключением случаев исполнения должностных обязанностей);
- осуществлять публикацию информации от имени Компании без соответствующего разрешения руководства.

Содержание и объем информации, передаваемой и (или) принимаемой с использованием сети Интернет, могут ограничиваться без уведомления работника.

Компания вправе контролировать и ограничивать использование сети Интернет с целью соблюдения требований Политики.

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

3.5.6. ПОЛИТИКА БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ СЪЕМНЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

3.5.6.1. НАЗНАЧЕНИЕ

Политика определяет правила и требования обеспечения ИБ при использовании съемных носителей информации.

3.5.6.2. ПОЛОЖЕНИЯ ПОЛИТИКИ

В Компании должны использоваться только разрешенные съемные носители информации.

Предоставление съемных носителей должно осуществляться по заявкам установленной формы только в целях исполнения должностных обязанностей. Необходимо осуществлять учет используемых в Компании съемных носителей информации.

Использование личных съемных носителей информации запрещено.

Сведения конфиденциального характера, хранящиеся на съемном носителе информации, должны быть защищены от НСД, а сами съемные носители при этом должны иметь внешнюю маркировку, указывающую на принадлежность носителя Компании.

Работникам, использующим съемные носители информации, строго запрещено:

- передавать съемные носители информации посторонним лицам или оставлять их без присмотра вне мест постоянного хранения;
- использовать съемный носитель информации не по назначению (например, для хранения личной информации).

Работники, использующие съемные носители информации, должны соблюдать следующие правила:

- обеспечивать физическую безопасность съемных носителей информации;
- извещать СБ о фактах утраты (кражи) съемных носителей информации;
- не допускать к съемным носителям информации лиц, не имеющих соответствующим образом оформленного разрешения к работе с конкретным съемным носителем (родственников, друзей и других лиц);
- хранить съемные носители информации в сейфах рабочих помещений или в запираемых ящиках столов.

По достижении целей использования съемных носителей информации, а также в случае увольнения работника Компании предоставленные ему съемные носители информации возвращают лицу, ответственному за их выдачу и учет.

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

Информация, хранящаяся на съемных носителях информации, должна своевременно уничтожаться гарантированным способом, исключающим или существенно затрудняющим ее восстановление на носителе.

В случае если гарантированное уничтожение информации на съемном носителе информации невозможно, носитель должен быть утилизирован с использованием средств, осуществляющих размагничивание носителя либо его физическое разрушение, не позволяющее впоследствии восстановить хранившуюся на нем информацию.

Компания вправе контролировать и ограничивать использование работниками съемных носителей информации.

3.5.7. ПОЛИТИКА БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ БЕСПРОВОДНЫХ СОЕДИНЕНИЙ

3.5.7.1. НАЗНАЧЕНИЕ

Политика определяет правила и требования обеспечения ИБ при использовании беспроводных соединений².

3.5.7.2. ПОЛОЖЕНИЯ ПОЛИТИКИ

Зона покрытия беспроводной сети Компании не должна выходить за пределы контролируемой зоны Компании.

Использование одноранговых беспроводных корпоративных сетей в Компании запрещено.

Необходимо осуществлять контроль создания и функционирования несанкционированных точек беспроводного доступа в пределах контролируемой зоны Компании.

Пользователям беспроводной сети запрещено создание общих сетевых ресурсов.

Подключение беспроводных устройств в сегмент беспроводного доступа должно производиться с использованием протокола динамической настройки узла (Dynamic Host Configuration Protocol).

Действия пользователей беспроводной сети должны регистрироваться.

Беспроводная сеть Компании состоит из двух сегментов, предназначенных для гостевого и корпоративного использования.

² В Компании все беспроводные соединения устанавливаются с использованием технологии Wi-Fi. Использование других технологий должно быть согласовано с СБ

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

Гостевой сегмент беспроводной сети должен соответствовать следующим требованиям:

- он должен быть выделен в отдельную ДМЗ;
- авторизация доступа в гостевой сегмент должна осуществляться с использованием индивидуальных идентификатора (логина) и пароля доступа;
- из гостевого сегмента беспроводной сети разрешен доступ только в сеть Интернет с соблюдением корпоративных политик контроля и ограничения доступа в сеть Интернет.

Корпоративный сегмент беспроводной сети должен соответствовать следующим требованиям:

- должен быть выделен в отдельный сегмент ЛВС;
- допускается доступ из корпоративного сегмента беспроводной сети к ИС Компании, если указанный доступ предусмотрен в эксплуатационной документации на данные ИС;
- должна обеспечиваться аутентификация по протоколу 802.1x с использованием паролей либо сертификатов и следующих механизмов:
 - ♦ взаимная проверка подлинности пользователя сети и централизованного сервера аутентификации;
 - ♦ динамическое получение уникального ключа шифрования для сессии;
 - ♦ централизованная политика периодической смены ключей шифрования;
- на сетевых устройствах, терминирующих беспроводной доступ, не должны использоваться технологии автоматической либо полуавтоматической настройки механизмов безопасности, разрабатываемые для удобства широкого круга потребителей;
- из корпоративного сегмента беспроводной сети разрешен доступ в сеть Интернет с соблюдением корпоративных политик контроля и ограничения доступа в сеть Интернет;
- при подключении беспроводных устройств должна осуществляться проверка безопасности устройства, включающая в себя:
 - ♦ контроль наличия установленных обновлений операционной системы;
 - ♦ наличие, корректность и актуальность настройки антивирусных средств.

Компания вправе контролировать и ограничивать использование сети беспроводных соединений с целью соблюдения требований Политики.

3.5.8. ПОЛИТИКА БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ МОБИЛЬНЫХ АРМ

3.5.8.1. НАЗНАЧЕНИЕ

Политика определяет правила и требования обеспечения ИБ при использовании МАРМ.

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

3.5.8.2. ПОЛОЖЕНИЯ ПОЛИТИКИ

В Компании должны использоваться только разрешенные типы МАРМ.

Предоставление МАРМ должно осуществляться по заявкам установленной формы только в целях исполнения должностных обязанностей на постоянной основе или для решения временных задач для обеспечения удаленного доступа работника к ИА при вынужденном отсутствии на рабочем месте (например, при командировке работника).

Необходимо осуществлять учет используемых в Компании МАРМ.

Запрещено использование личных АРМ, в том числе мобильных, для доступа к ИА, к которым не предусмотрен публичный доступ.

Для МАРМ, вынос которых за пределы контролируемой зоны санкционирован, необходимо обеспечить шифрование всей файловой системы устройства, в случае отсутствия такой технической возможности - только конфиденциальной информации Компании.

Работникам, использующим МАРМ, строго запрещено:

- передавать МАРМ посторонним лицам или оставлять их без присмотра вне мест постоянного хранения;
- использовать МАРМ не по назначению (например, для хранения личной информации).

Работники, использующие МАРМ, должны соблюдать следующие правила:

- обеспечивать физическую безопасность МАРМ за пределами контролируемой зоны;
- извещать Службу безопасности о фактах утраты (кражи) МАРМ;
- не допускать к МАРМ посторонних лиц (родственников, друзей и других лиц);
- хранить МАРМ в специально отведенных и обеспечивающих защиту от доступа посторонних лиц местах (в сейфах рабочих помещений, в запираемых ящиках столов и т.п.).

По достижении целей использования МАРМ, а также в случае увольнения работника Компании, предоставленные ему МАРМ возвращают лицу, ответственному за их выдачу и учет.

Компания вправе контролировать и ограничивать использование работниками МАРМ.

3.5.9. ПОЛИТИКА БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

3.5.9.1. НАЗНАЧЕНИЕ

Политика определяет правила и требования обеспечения ИБ при использовании облачных вычислений.

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

3.5.9.2. ПОЛОЖЕНИЯ ПОЛИТИКИ

В Компании в качестве облачных вычислений рассматриваются публичные и частные модели их развертывания.

Запрещается использовать публичные сервисы облачных вычислений для хранения и обработки любых категорий информации, кроме публичной. Использование публичных облачных вычислений должно быть согласовано с СБ.

Договор приобретения сервиса частных облачных вычислений между Компанией и владельцем облачных вычислений должен содержать:

- требования ИБ для обеспечения уровня защищенности ИА, разворачиваемых на базе инфраструктуры облачных вычислений, в соответствии с положениями ЛНД Компании в области ИБ, в зависимости от категории обрабатываемой информации;
- распределение ответственности за обеспечение ИБ ИА, разворачиваемых на базе инфраструктуры облачных вычислений, между Компанией и владельцем облачных вычислений в зависимости от предоставляемой модели обслуживания (IaaS, PaaS, SaaS).

Решение об использовании сервиса частных облачных вычислений для развертывания ИА должно основываться на результатах оценки рисков. Для ИА должны быть определены бизнес-требования и требования законодательства, применимые к данному активу, и оценен возможный ущерб для Компании, возникающий вследствие нарушения конфиденциальности, целостности или доступности актива, а также несоблюдения требований законодательства и договорных обязательств при использовании арендованных частных облачных вычислений.

При взаимодействии с ИА, размещенными на базе инфраструктуры облачных вычислений, необходимо обеспечить защиту передаваемой информации от НСД.

3.5.10. ПОЛИТИКА БЕЗОПАСНОСТИ ПРИ ПРОВЕДЕНИИ ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ

3.5.10.1. НАЗНАЧЕНИЕ

Политика определяет правила и требования обеспечения ИБ при проведении технического обслуживания АРМ, серверного и сетевого оборудования, СЗИ.

3.5.10.2. ПОЛОЖЕНИЯ ПОЛИТИКИ

Техническое обслуживание должно осуществляться только на основании зарегистрированного обращения или согласно утвержденному графику (регламенту) проведения технического обслуживания.

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

Локальное техническое обслуживание должно осуществляться только в личном присутствии работника, либо с санкции владельца информации или уполномоченного владельцем лица.

Дистанционное техническое обслуживание должно осуществляться только со специально выделенных АРМ или с использованием специально выделенных средств автоматизации, конфигурация и состав которых должны быть стандартизованы, а процесс эксплуатации регламентирован и контролироваться.

При проведении технического обслуживания должен выполняться минимальный набор действий, необходимых для устранения проблемы, явившейся причиной обращения, и использоваться любые возможности, позволяющие впоследствии установить авторство внесенных изменений.

Копирование информации, содержащейся на носителях объектов технического обслуживания, или временное изъятие носителей информации (в том числе в составе объекта технического обслуживания) может осуществляться только с соблюдением следующих требований:

- любые действия с информацией, либо с носителями, содержащими такую информацию, могут производиться с санкции владельца информации или уполномоченного владельцем на принятие данных решений лица;
- процесс миграции/копирования информации или изъятия носителей должен осуществляться таким образом, чтобы исключить НСД к соответствующей информации;
- информация на задействованных на временной основе в процессе миграции/копирования носителях информации должна своевременно уничтожаться гарантированным способом, исключающим или существенно затрудняющим ее восстановление.

3.5.11. ПОЛИТИКА УПРАВЛЕНИЯ РИСКАМИ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.5.11.1. НАЗНАЧЕНИЕ

Политика определяет основные правила управления рисками нарушения ИБ.

3.5.11.2. ПОЛОЖЕНИЯ ПОЛИТИКИ

Компания осознает, что ее деятельность подвержена негативному влиянию рисков нарушения ИБ.

Компания осуществляет управление рисками нарушения ИБ в порядке, установленном законодательством и соответствующими локальными нормативными документами.

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

Деятельность по управлению рисками нарушения ИБ включает в себя планирование, идентификацию риска, оценку риска, выбор способа реагирования на риск и разработку, планирование и внедрение мероприятий по управлению рисками нарушения ИБ.

Топ-менеджеры ПАО «НК «Роснефть», руководители Обществ Группы и работники Компании несут ответственность за управление рисками нарушения ИБ, включая:

- своевременное выявление (идентификацию) и оценку рисков;
- планирование деятельности с учетом влияния рисков на достижение целей и плановых показателей;
- реализацию мероприятий, направленных на снижение вероятности наступления рисков и/или минимизацию неблагоприятных последствий от их наступления;
- своевременное информирование о реализации рисков и существенных изменениях в перечне и описании рисков всех заинтересованных сторон, включая топ-менеджера ПАО «НК «Роснефть», ответственного за ИБ.

Идентификация и оценка рисков должна проводиться на регулярной основе, а также в случаях возникновения существенных изменений, влияющих на ранее выполненную оценку рисков ИБ:

- в производственных процессах Компании;
- в составе ИА;
- в составе информационно-технологической инфраструктуры и ее компонентов;
- при изменении внешних факторов (экономических, социальных, политических, экологической обстановки и т.п.), способных привести к появлению новых рисков нарушения ИБ для Компании.

Оценка рисков может проводиться как для Компании в целом, так и для определенной области оценки (для определенных СП, производственных процессов, ИС и информационных ресурсов, компонентов информационно-технологической инфраструктуры и т.д.).

Оценка рисков проводится в отношении всех информационных активов, эксплуатируемых в рамках определенной области оценки. Для каждого идентифицированного актива должны быть определены бизнес-требования и требования законодательства, применимые к данному активу, и оценен возможный ущерб для Компании, возникающий вследствие нарушения конфиденциальности, целостности или доступности актива, а также несоблюдения требований законодательства и договорных обязательств.

Для каждого информационного актива должны производиться идентификация и анализ рисков, включая оценку вероятности наступления рисков и воздействия рисков.

Способы определения величины риска (вероятности и воздействия) должны определяться в соответствии с принятой в Компании методологией оценки рисков нарушения ИБ.

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

Среди всех выявленных рисков нарушения ИБ должны быть идентифицированы риски, превышающие уровень приемлемого риска, утвержденного ответственным топ-менеджером ПАО «НК «Роснефть»/руководителем ОГ, и, следовательно, требующие выбора способа реагирования и разработки плана мероприятий по их управлению.

По результатам оценки рисков должен осуществляться выбор способа реагирования на выявленные риски и разработка плана мероприятий по управлению выявленными рисками. К возможным способам реагирования на риск относятся: избегание риска, минимизация риска, передача риска, принятие риска.

При выборе способа реагирования на выявленные риски и разработке плана мероприятий по управлению выявленными рисками должны учитываться стоимость внедрения мероприятий по управлению рисками, а также соотношение сопряженных с этим расходов с величиной ожидаемых потерь. Выбор способа реагирования на риск должен подтверждаться руководителями заинтересованных СП и владельцами информационных активов. Для каждого риска должен быть определен остаточный риск.

Окончательное решение в отношении выявленных рисков ИБ должно приниматься куратором/владельцем риска.

Общий порядок управления рисками процесса обеспечения ИБ, а также ключевые риски указанного процесса приведены в Политике Компании «Концепция информационно-технической безопасности ПАО «НК «Роснефть» № ПЗ-11.1.

3.5.12. ПОЛИТИКА ПРОВЕДЕНИЯ АУДИТОВ ИБ

3.5.12.1. НАЗНАЧЕНИЕ

Политика определяет правила и требования к проведению аудитов ИБ Компании, осуществляемых с целью обеспечения соответствия реализованных мер требованиям законодательства Российской Федерации, российских и (или) международных стандартов и ЛНД Компании в области ИБ, а также с целью повышения уровня защищенности информационных активов Компании.

3.5.12.2. ПОЛОЖЕНИЯ ПОЛИТИКИ

Аудит ИБ является одним из основных средств контроля и оценки организационных и технических мер защиты информации, реализуемых в Компании.

Предусматриваются следующие разновидности аудитов ИБ:

- тестирование и оценка адекватности дизайна и эффективности реализованных мер обеспечения ИБ;
- оценка соответствия мер обеспечения ИБ требованиям законодательства Российской Федерации, российских и (или) международных стандартов в области ИБ, а также ЛНД по обеспечению ИБ Компании.

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

Тестирование и оценка эффективности реализованных мер обеспечения ИБ должны осуществляться, в том числе, с обязательным применением автоматизированных средств анализа защищенности и поиска уязвимостей. Тестирование должно осуществляться с учетом специализированных международных и национальных методологий и лучших практик.

Аудит ИБ может проводиться в форме как внутреннего, так и внешнего аудита.

Внутренний аудит ИБ должен проводиться силами специалистов Компании, имеющих соответствующие компетенции: работники СБ и привлекаемые ими в качестве экспертов по смежным прикладным областям работники других СП.

Внешний аудит ИБ проводится внешними по отношению к Компании независимыми проверяющими организациями на основании оформленных договоров. Договоры должны включать требования по неразглашению сведений конфиденциального характера (Стандарт Компании «Охрана сведений конфиденциального характера» № ПЗ-11.03 С-0006) ставших известными аудиторам в ходе проведения аудита. Решение о необходимости проведения внешнего аудита ИБ может приниматься по следующим причинам:

- с целью выполнения требований законодательства Российской Федерации, договорных обязательств Компании или ЛНД;
- в случае отсутствия необходимых компетенций внутри Компании;
- во избежание случаев возникновения конфликта интересов.

Организации, привлекаемые для проведения аудита ИБ, должны обладать необходимыми лицензиями для осуществления соответствующих видов деятельности. При выборе организации, также должен учитываться опыт проведения соответствующих аудитов ИБ и наличие в проверяющей организации необходимого количества аудиторов с требуемой квалификацией.

В Компании должен быть документально определен и утвержден руководителем СБ план проведения аудитов ИБ, содержащий информацию, необходимую для их планирования, организации, контроля проведения, а также обеспечения ресурсами, необходимыми для эффективного и результативного проведения указанных аудитов ИБ в заданные сроки.

Аудит ИБ должен проводиться на регулярной основе, а также по мере необходимости. Периодичность проведения аудитов ИБ должна быть документально определена в плане проведения аудитов ИБ в рамках трехлетнего горизонта планирования.

В случае наличия объективной необходимости и/или во исполнение указаний руководства Компании допускается проведение внеплановых аудитов ИБ.

Результаты проведения аудитов ИБ должны быть документированы, а полученные сведения использоваться с целью улучшения мер и средств обеспечения ИБ, а также устранения несоответствий и уязвимостей, выявленных в ходе аудитов ИБ.

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

Для полученных свидетельств аудитов ИБ и документированных результатов аудитов ИБ должны быть определены правила хранения и использования, а также сроки хранения.

В ходе проведения аудитов ИБ работники Компании должны оказывать содействие специалистам, осуществляющим аудит, и оперативно предоставлять необходимые сведения в рамках своих компетенций.

3.5.13. ПОЛИТИКА МОНИТОРИНГА СОБЫТИЙ ИБ

3.5.13.1. НАЗНАЧЕНИЕ

Политика определяет правила и требования к постоянному контролю, наблюдению, получению, хранению, распознаванию и анализу информации, связанной с событиями ИБ, а также выявлению фактов, признаков и причин нарушения установленных требований, объектов и работников, с которыми связаны эти нарушения.

3.5.13.2. ПОЛОЖЕНИЯ ПОЛИТИКИ

Мониторинг событий ИБ должен осуществляться централизованно, в автоматическом (без участия человека) и непрерывном режиме. В случаях отсутствия соответствующих средств автоматизации, либо невозможности их внедрения мониторинг событий ИБ должен осуществляться работниками соответствующих СП и/или подрядных организаций, осуществляющих сопровождение ИС.

Для мониторинга событий ИБ, осуществляющегося без использования автоматизированных средств мониторинга, должны быть определены периодичность его проведения и отчетная форма для документирования результатов мониторинга.

Мониторинг событий ИБ должен осуществляться в отношении всех типов объектов защиты, определенных в подразделе 3.4 настоящего Стандарта.

Источниками данных мониторинга должны являться журналы регистрации событий ИБ объектов защиты. Журналы могут вестись как в электронном виде, так и на бумажных носителях.

Для всех объектов защиты должны быть определены события ИБ, которые необходимо регистрировать, и параметры их регистрации. Средства регистрации событий ИБ объектов защиты должны быть настроены соответствующим образом.

Состав событий ИБ должен пересматриваться на основании анализа результатов выполнения следующих действий:

- расследование инцидентов ИБ;
- проведение аудитов ИБ;
- анализ и оценка рисков нарушения ИБ;

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

- управление уязвимостями;
- управление изменениями ИС и их конфигурациями;
- появление новых объектов защиты.

В соответствии с определенными событиями ИБ, которые необходимо регистрировать, в автоматизированных средствах мониторинга событий ИБ необходимо:

- настроить механизмы передачи информации о событиях ИБ из журналов регистраций событий ИБ объектов защиты;
- настроить механизмы нормализации, фильтрации, классификации, агрегации и корреляции событий ИБ;
- настроить механизмы оповещения о событиях ИБ;
- установить правила обработки событий ИБ.

Должно осуществляться обеспечение конфиденциальности, целостности и доступности журналов регистрации событий ИБ объектов защиты, хранилища событий ИБ автоматизированного средства мониторинга событий ИБ и журналов на бумажных носителях.

Должен быть определен минимальный срок хранения событий ИБ в хранилище автоматизированного средства мониторинга событий ИБ, журналов регистрации событий ИБ объектов защиты, которые не подлежат автоматическому мониторингу, а также журналов на бумажных носителях.

По истечении срока хранения события ИБ должны архивироваться и храниться вне хранилища автоматизированного средства мониторинга событий ИБ и объектов защиты.

Должны быть определены средства архивирования событий ИБ, а также место и срок хранения архивных копий.

3.5.14. ПОЛИТИКА УПРАВЛЕНИЯ ИНЦИДЕНТАМИ ИБ

3.5.14.1. НАЗНАЧЕНИЕ

Политика определяет правила и требования к обнаружению и эффективному реагированию на события ИБ, являющиеся инцидентами ИБ, минимизации прямого или косвенного негативного воздействия на Компанию, минимизации вероятности повторения инцидентов ИБ в будущем.

3.5.14.2. ПОЛОЖЕНИЯ ПОЛИТИКИ

Управление инцидентами должно осуществляться централизованно и в непрерывном режиме. Необходимо вести централизованный учет всех выявленных инцидентов ИБ и связанных с ними мероприятий.

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

Управление инцидентами ИБ должно включать в себя следующие этапы:

- обнаружение и идентификацию инцидентов ИБ;
- регистрацию и эскалацию инцидентов ИБ;
- разрешение (локализация, контроль, устранение и восстановление) инцидентов ИБ;
- анализ и отчет по результатам устранения инцидентов ИБ;
- устранение причин и минимизация вероятности повторного возникновения аналогичных инцидентов.

Должны быть определены формы отчетных документов по результатам обнаружения, расследования и устранения выявленных инцидентов ИБ. Работа по обнаружению инцидентов ИБ должна осуществляться на постоянной основе. Отчетные документы должны предоставляться руководителям ответственных СП на регулярной основе, вне зависимости от наличия выявленных инцидентов ИБ.

Инциденты ИБ должны выявляться:

- работниками Компании во время выполнения своих должностных обязанностей;
- работниками уполномоченных подразделений СБ посредством наблюдения за деятельностью работников Компании и третьих лиц;
- работниками СП и подрядных организаций, осуществляющих сопровождение ИС и ресурсов, посредством анализа их работоспособности;
- в результате мониторинга событий ИБ.

Должны быть определены каналы оповещения и порядок эскалации обнаруженных инцидентов ИБ.

Работники должны информировать своих линейных руководителей и СБ обо всех фактах нарушений ИБ, либо иных событиях, способных привести к нарушению режима ИБ Компании.

Необходимо определить перечень типовых инцидентов ИБ и периодически пересматривать его. Для каждого типового инцидента ИБ должны быть определены рекомендуемые мероприятия по его устранению.

На этапе обнаружения и идентификации инцидентов ИБ должна применяться методика категоризации инцидентов, позволяющая сопоставить уровень критичности выявленному инциденту ИБ в зависимости от величины потенциальных негативных последствий на информационные активы Компании. Для каждого уровня критичности необходимо определить порядок эскалации инцидента ИБ, а также плановые (рекомендуемые) сроки разрешения инцидента ИБ.

На этапе разрешения инцидентов ИБ, после осуществления процедур по локализации и устранению причин инцидента ИБ, должно приниматься решение о необходимости выполнения процедур восстановления затронутых инцидентом объектов защиты.

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

После разрешения инцидента и возврата к штатному функционированию, руководителям ответственных за обработку инцидента СП должен предоставляться подробный отчет с описанием инцидента ИБ, а также принятых мер по его разрешению. Все разрешенные инциденты ИБ должны анализироваться с целью выявления причин их возникновения и проведения корректирующих действий, позволяющих минимизировать воздействие инцидентов ИБ и избежать их повторения в будущем. Кроме того, должны устанавливаться лица, в результате действий которых возникли инциденты ИБ.

3.5.15. ПОЛИТИКА ЗАЩИТЫ СРЕДЫ ВИРТУАЛИЗАЦИИ

3.5.15.1. НАЗНАЧЕНИЕ

Политика определяет правила и требования к защите информации при ее обработке с использованием технологий виртуализации вычислительных мощностей.

3.5.15.2. ПОЛОЖЕНИЯ ПОЛИТИКИ

Виртуальная инфраструктура включает среду виртуализации (программное обеспечение, служебные данные компонентов виртуальной инфраструктуры) и аппаратное обеспечение (аппаратные средства, необходимые для функционирования среды виртуализации, в том числе средства резервного копирования и защиты информации).

Для защиты виртуальной инфраструктуры в ней должны, как минимум, быть реализованы требования по защите информации, предъявляемые к ИС, которые развернуты на базе виртуальных машин данной среды виртуализации. Виртуальная инфраструктура должна обеспечивать уровень защищенности информации не ниже чем уровень защищенности ИС, функционирующих на ее базе.

В качестве объектов доступа в виртуальной инфраструктуре необходимо, как минимум, рассматривать программное обеспечение управления виртуальной инфраструктурой, гипервизор, хостовую операционную систему (если применимо), виртуальные машины, программную среду виртуальных машин (в том числе их операционные системы и программное обеспечение), виртуальные контейнеры (зоны), виртуализированное программное обеспечение (виртуальные машины с предустановленным программным обеспечением, предназначенная для выполнения определенных функций в виртуальной инфраструктуре), СЗИ, используемые в рамках виртуальных машин и виртуальной инфраструктуры в целом.

В виртуальной инфраструктуре должны обеспечиваться:

- контроль доступа субъектов доступа к средствам управления компонентами виртуальной инфраструктуры;
- контроль доступа субъектов доступа к файлам-образам виртуализированного программного обеспечения, виртуальных машин, файлам-образам, служебным данным,

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

используемым для обеспечения работы виртуальных файловых систем, и иным служебным данным средств виртуальной среды;

- управление доступом к виртуальному аппаратному обеспечению ИС, являющимся объектом доступа;
- контроль запуска виртуальных машин на основе заданных оператором правил (режима запуска, типа используемого носителя и иных правил).

Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать разграничение доступа:

- субъектов доступа, зарегистрированных на виртуальных машинах, к объектам доступа, расположенным внутри виртуальных машин, в соответствии с правилами разграничения доступа пользователей данных виртуальных машин (потребителей облачных услуг);
- субъектов доступа, зарегистрированных на виртуальных машинах, к ресурсам ИС, размещенным за пределами виртуальных машин, в соответствии с правилами разграничения доступа принятыми в ИС в целом.

3.5.16. ПОЛИТИКА УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ

3.5.16.1. НАЗНАЧЕНИЕ

Политика определяет правила и требования к выявлению и устранению уязвимостей, которые могут быть использованы для реализации угроз ИБ в отношении Компании.

3.5.16.2. ПОЛОЖЕНИЯ ПОЛИТИКИ

Управление уязвимостями должно осуществляться в отношении всех типов объектов защиты, определенных в подразделе 3.4 настоящего Стандарта.

Выявление уязвимостей должно осуществляться периодически как с использованием автоматизированных инструментальных средств анализа защищенности, так и с использованием общедоступных источников информации (сайты и новостные рассылки производителей программно-аппаратных компонентов объектов защиты, новостные сайты третьих сторон, специализированные базы данных уязвимостей и т. д.).

В рамках выявления уязвимостей с использованием автоматизированных инструментальных средств анализа защищенности должно осуществляться внутреннее и внешнее сканирование программно-аппаратных компонентов объектов защиты.

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

Дополнительные мероприятия по выявлению уязвимостей с использованием автоматизированных инструментальных средств анализа защищенности необходимо осуществлять в следующих случаях:

- перед вводом в опытно-промышленную эксплуатацию новых программно-аппаратных компонентов объектов защиты;
- при внесении изменений (в том числе при установке обновлений и новых настроек) в используемые программно-аппаратные компоненты объектов защиты.

Проведение процедуры сканирования должно осуществляться после согласования с владельцем объекта защиты, а также с подразделением, ответственным за его эксплуатацию.

Выявленные уязвимости необходимо проанализировать с целью установления необходимости их устранения.

При осуществлении анализа необходимо учитывать следующие характеристики для каждой выявленной уязвимости:

- возможные последствия при неустранении уязвимости;
- период времени, прошедший с момента огласки информации об уязвимости;
- наличие обновлений программно-аппаратных компонентов или других средств устранения уязвимости;
- наличие детального описания уязвимости;
- простота реализации угроз нарушения ИБ с использованием уязвимости;
- наличие и доступность вредоносных программ, способных использовать уязвимость;
- изменение функционирования объектов защиты, в которых выявлена уязвимость, в процессе устранения уязвимости;
- возможные сроки устранения уязвимости.

Выявленные уязвимости должны быть учтены при анализе и оценке рисков нарушения ИБ.

Должна быть определена отчетная форма для документирования результатов выявления уязвимостей.

Используемые инструментальные средства анализа защищенности должны иметь регулярно обновляемую базу тестов и уязвимостей.

3.5.17. ПОЛИТИКА ПРОТИВОДЕЙСТВИЯ НСД И УТЕЧКАМ ИНФОРМАЦИИ

3.5.17.1. НАЗНАЧЕНИЕ

Политика определяет правила и требования к обеспечению защиты сведений конфиденциального характера в Компании от утечки и НСД.

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

3.5.17.2. ПОЛОЖЕНИЯ ПОЛИТИКИ

Защита информации от утечек должна осуществляться посредством выполнения комплекса организационных и технических мероприятий и должна быть дифференцированной в зависимости от категории информации и технологии ее обработки.

Для нейтрализации актуальных угроз ИБ, обусловленных наличием возможных программных закладок, должны осуществляться следующие мероприятия:

- проверка ПО, включая программный код, на отсутствие недокументированных (недекларированных) возможностей с использованием автоматизированных средств и (или) без использования таковых;
- тестирование ИС на проникновения;
- использование в ИС системного и (или) прикладного ПО, разработанного с использованием методов защищенного программирования.

Построение системы защиты от НСД для ИС должно исходить из принципа: «Не существует СЗИ, которое нельзя было бы преодолеть». В соответствии с данным принципом, система защиты от НСД должна обеспечивать эшелонированную защиту ИС, за счет применения специализированных СЗИ на различных уровнях ИС, включая в себя совокупность организационных, технических и физических меры защиты информации.

Все случаи выявления потенциальных утечек и нарушения порядка доступа к информации должны протоколироваться и обрабатываться в рамках процесса управления инцидентами ИБ.

3.5.18. ПОЛИТИКА УПРАВЛЕНИЯ ДОСТУПОМ

3.5.18.1. НАЗНАЧЕНИЕ

Политика определяет правила и требования к обеспечению ИБ Компании от угроз безопасности, связанных с НСД к ИА Компании.

3.5.18.2. ПОЛОЖЕНИЯ ПОЛИТИКИ

Доступ работников Компании к ИА Компании должен предоставляться только для исполнения ими функциональных обязанностей, согласно принципу минимизации привилегий (должны быть запрещены все функции и возможности ИА, которые не разрешены явным образом).

Предоставление доступа работника к ИА должно осуществляться на основании соответствующей заявки. Заявка должна содержать описание необходимых прав доступа и

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

срок их действия, а также обоснование необходимости доступа и его длительности. Заявка должна быть согласована с уполномоченными работниками ПАО «НК «Роснефть»/ОГ³. Изменение и блокирование предоставленных прав доступа должно осуществляться аналогичным способом.

При назначении прав на доступ пользователей к ИА необходимо руководствоваться следующими основополагающими принципами:

- ♦ пользователю должен выдаваться минимальный набор прав на доступ к ИА, необходимый для выполнения должностных обязанностей;
- ♦ доступ к информации может быть предоставлен только в том случае, если пользователь для выполнения своих должностных обязанностей должен быть ознакомлен именно с этой информацией.

Допуск третьих лиц к работе с ИА осуществляется только после заключения соответствующего договора с Компанией, содержащего требования ИБ. Ответственность за организацию внесения требований ИБ несет руководитель СП, являющийся куратором работ, осуществляемых третьим лицом по договору.

Каждому пользователю, допущенному к работе с ИА, должно соответствовать персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в ИА.

В случае производственной необходимости некоторым пользователям могут соответствовать несколько уникальных имен.

Использование несколькими пользователями при работе в ИА одного и того же уникального имени запрещено (исключения составляют административные и технологические учетные записи ИА, у которых отсутствует возможность для их персонификации).

При создании новой учетной записи пользователя должен быть сгенерирован случайный пароль для первого входа пользователя в ИА.

Исполненные заявки должны храниться в архиве в течение 3 (трех) лет с момента окончания предоставления доступа к ИА.

В случае изменения должностных обязанностей работника его права доступа в ИА должны быть пересмотрены.

При наступлении даты прекращения срока действия полномочий пользователя (окончание договорных отношений, увольнение работника) либо временной приостановки учетная запись должна немедленно блокироваться.

³ Перечень уполномоченных работников ПАО «НК «Роснефть»/ОГ определяется на основе конкретного распорядительного документа, разрабатываемого для каждого ИА

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

Заблокированные учетные записи должны сохраняться в системе не менее 3 (трех) лет с даты прекращения срока действия полномочий пользователя. По окончании срока хранения учетные записи удаляются из ИА.

Необходимо осуществлять периодический пересмотр прав доступа к ИА с целью выявления избыточных и (или) устаревших прав доступа.

3.5.19. ПОЛИТИКА ИСПОЛЬЗОВАНИЯ ПАРОЛЕЙ

3.5.19.1. НАЗНАЧЕНИЕ

Политика определяет правила и требования к обеспечению ИБ Компании от угроз безопасности, связанных с использованием паролей.

3.5.19.2. ПОЛОЖЕНИЯ ПОЛИТИКИ

Аутентификация работников Компании при доступе к ИА, СЗИ и компонентам информационно-технологической инфраструктуры должна осуществляться с использованием паролей или иных согласованных в Компании методов аутентификации.

Пароли должны удовлетворять следующим требованиям:

- максимальный срок действия пароля составляет 60 (шестьдесят) дней⁴;
- минимальный срок действия пароля составляет 1 (один) день;
- пароль должен содержать символы, относящиеся к 3 (трем) из перечисленных категорий:
 - ♦ латинские заглавные буквы (A–Z);
 - ♦ латинские строчные буквы (a–z);
 - ♦ цифры (0–9);
 - ♦ отличные от букв и цифр символы (например, !, \$, #);
- пароли должны состоять:
 - ♦ пользовательские пароли – не менее чем из 8 (восьми) символов;
 - ♦ административные пароли – не менее чем из 15 (пятнадцати) символов;
 - ♦ пароли, не предполагающие свое изменение со временем, должны быть не менее 32 (тридцати двух) символов;
- пароль не должен совпадать с 24 (двадцатью четырьмя) последними паролями;

⁴ Кроме паролей, не предполагающих свое изменение со временем. Например, пароли системных и служебных учетных записей, для которых процедура регулярной смены не предусмотрена или нецелесообразна

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

- пароль не должен содержать имя учетной записи пользователя или фрагменты имени пользователя длиной больше 2 (двух) символов;
- пароль не должен являться словом, присутствующим в словарях, или профессиональным термином, в т. ч. набранным в другой раскладке клавиатуры;
- пароль не должен основываться на семейной, служебной и другой легкодоступной информации (фамилии, имена, даты рождения, клички животных, автомобильные и телефонные номера, названия организаций, адреса сайтов и т. п.);
- пароль не должен содержать легко угадываемые последовательности символов (123456, aaabbbb, qwerty, q1w2e3 и т. п.);
- в случае 10 (десяти) подряд неудачных попыток ввода пароля в течение 30 (тридцати) минут доступ должен быть заблокирован.

Первичный пароль, создаваемый при заведении учетной записи или смене забытого пароля, сообщается исключительно пользователю, являющемуся владельцем данной учетной записи. По согласованию с СБ и с учетом результатов предварительной оценки рисков в отдельных случаях допускается передача первичного пароля пользователю посредством его корпоративной электронной почты.

Срок действия первичного пароля не должен превышать 3 (трех) рабочих дней.

Пароль должен быть изменен в следующих случаях:

- при первичном обращении к объекту доступа;
- при истечении срока действия пароля;
- при подозрении в компрометации пароля;
- при изменении владельца учетной записи;
- при изменении состава группы, использующей общий пароль.

Пользователь должен извещаться об истечении срока действия его пароля и необходимости его смены за 14 (четырнадцать) календарных дней до окончания указанного срока.

Пароли, предустановленные производителями компонентов информационно-технологической инфраструктуры и СЗИ, должны сменяться до начала его эксплуатации.

Ввод пароля должен обязательно маскироваться специальным символом («звездочками»). Новый пароль должен вводиться дважды (*с подтверждением*).

В случае использования для аутентификации аппаратного токена с генератором одноразовых паролей перед генерацией пароля должен требоваться ввод PIN-кода (*двухфакторная аутентификация*). PIN-код должен состоять не менее чем из 4 (четырех) символов. PIN-код запрещается передавать кому бы то ни было и хранить в открытом виде.

При хранении пароли должны быть защищены от НСД.

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

Должны быть предусмотрены дополнительные меры по защите административных паролей в целях предотвращения их нецелевого использования, а также восстановления в случае утраты.

Владельцам паролей запрещается:

- сообщать свой персональный пароль другим лицам или записывать его на материальных носителях, доступных для других лиц (кроме предусмотренных случаев сохранения паролей ключевых учетных записей владельцем информационного актива);
- сохранять пароль в программно-технических средствах в открытом виде или использовать средства его автоматического ввода;
- использовать легко угадываемый алгоритм смены пароля (например, F%1hTR8 -* F%2hTR8 -> F%3hTR8, или F%1hTR8 -* F1%hTR8 -* F1h%TR8 и др.);
- использовать вне ПАО «НК «Роснефть» пароли, совпадающие с паролями доступа к его ИС, информационным ресурсам, СЗИ и компонентам информационно-технологической инфраструктуры;
- использовать в качестве паролей примеры, приведенные в Политике.

Процессы создания, изменения, использования, блокирования, удаления учетных записей, а также смены паролей должны быть регламентированы, протоколироваться и контролироваться.

3.5.20. ПОЛИТИКА ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ

3.5.20.1. НАЗНАЧЕНИЕ

Политика определяет правила и требования к обеспечению ИБ Компании от угроз непосредственного НСД, реализуемых третьими лицами и связанных с порчей и утратой технических средств информационно-технологической инфраструктуры, ИА, СЗИ.

3.5.20.2. ПОЛОЖЕНИЯ ПОЛИТИКИ

На территории всех физических объектов Компании должны действовать правила пропускного и внутриобъектового режима, которые обязательны к соблюдению всеми лицами, находящимися на территории объектов. Проход на территорию физических объектов Компании осуществляется по пропускам.

Все технические средства (серверы, системы хранения данных, сетевое оборудование и др.) информационно-технологической инфраструктуры, ИА, СЗИ должны размещаться в закрываемых помещениях на охраняемой территории, оборудованных системами аварийного энергоснабжения, кондиционирования, пожаротушения (сигнализации) и контроля доступа.

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

Технические средства, находящиеся вне охраняемой территории при транспортировке либо при использовании работниками для автономного хранения информации и удаленного доступа к ИА, не допускается оставлять без присмотра.

Доступ в помещения с усиленным режимом охраны (в частности, серверные помещения) предоставляется только авторизованному персоналу, а доступ третьих лиц осуществляется только в сопровождении уполномоченных работников Компании. Сведения о местонахождении помещений с усиленным режимом охраны не должны публиковаться в общедоступной документации, а внешний вид помещений не должен раскрывать их назначение.

Порядок доступа и проведения работ в помещениях с усиленным режимом охраны должен быть регламентирован.

Запрещается открытая прокладка линий связи во избежание их механических повреждений и несанкционированных подключений к корпоративной сети Компании.

3.5.21. ПОЛИТИКА БЕЗОПАСНОСТИ СЕТЕВОГО ПЕРИМЕТРА

3.5.21.1. ПОЛИТИКА СЕГМЕНТИРОВАНИЯ СЕТИ

3.5.21.1.1. НАЗНАЧЕНИЕ

Политика определяет правила и требования к повышению ИБ Компании путем изолирования друг от друга объектов сети.

3.5.21.1.2. ПОЛОЖЕНИЯ ПОЛИТИКИ

Для защиты сетевого периметра должны быть выделены внешние и внутренние сегменты ДМЗ.

Внешние ДМЗ должны использоваться в качестве буферной зоны для предоставления доступа серверам и пользователям к внешним сетям, в том числе сети Интернет, а также служат для размещения ИА, к которым необходимо обеспечить доступ из сети Интернет. Внутренние ДМЗ служат для изоляции в них ИС, обрабатывающих информацию для внутреннего пользования или сведений конфиденциального характера.

Сегменты доступа пользователей должны быть отделены от серверных сегментов.

Серверные сегменты должны быть разделены по функциональному назначению и/или в зависимости от категорий ИС, размещенных в них. Различные категории ИС должны размещаться в различных сегментах сети.

Сегменты доступа пользователей должны быть разделены на основе функциональных обязанностей работников.

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

Гостевой доступ к ИС, обрабатывающим публичную информацию, должен осуществляться через выделенные сегменты, надежно отделенные от остальной корпоративной сети.

3.5.21.2. ПОЛИТИКА МЕЖСЕТЕВОГО ЭКРАНИРОВАНИЯ

3.5.21.2.1. НАЗНАЧЕНИЕ

Политика определяет правила и требования к обеспечению ИБ Компании от несанкционированного сетевого взаимодействия между внутренними сетевыми сегментами, а также между корпоративной сетью Компании и сторонними сетями.

3.5.21.2.2. ПОЛОЖЕНИЯ ПОЛИТИКИ

При построении системы межсетевого экранирования должен использоваться принцип эшелонированной защиты. В соответствии с данным принципом, для различных рубежей защиты должны использоваться различные средства межсетевого экранирования.

Доступ из сети Интернет в корпоративную сеть Компании в обход сегмента ДМЗ запрещен.

Доступ из корпоративной сети Компании в сеть Интернет в обход сегмента ДМЗ запрещен.

Средствами межсетевого экранирования обязательно должны контролироваться взаимодействия между:

- сегментами ДМЗ и сетью Интернет;
- сегментами ДМЗ и доверенными сегментами сети;
- пользовательскими и серверными сегментами;
- серверными сегментами различного функционального назначения и\или серверными сегментами, содержащими ИС различных категорий.

Также средствами межсетевого экранирования могут контролироваться взаимодействия между пользовательскими сегментами с различными функциональными обязанностями работников.

Средства межсетевого экранирования должны реализовывать следующие основные функции:

- осуществлять межсетевое экранирование с учетом состояния соединений;
- фильтрацию входящих и исходящих пакетов (данных) коммуникационных протоколов сетевого уровня на основе заданных правил фильтрации;
- регистрацию и учет фильтруемых входящих и исходящих пакетов (данных) коммуникационных протоколов сетевого уровня с указанием атрибутов фильтруемых пакетов, времени, результата фильтрации и др.;
- регистрацию и учет попыток нарушения правил фильтрации.

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

Средства межсетевого экранирования, установленные на границе с сетью Интернет, должны осуществлять предотвращение раскрытия частных IP-адресов и данных маршрутизации внутренней сети в сети Интернет.

Резервное копирование конфигураций средств межсетевого экранирования должно периодически осуществляться на специально выделенное защищенное файловое хранилище.

Необходимо определить перечень разрешенных межсетевых взаимодействий, позволяющий контролировать наличие излишних разрешений в правилах межсетевого экранирования.

Изменения конфигураций средств межсетевого экранирования должны осуществляться только на основании согласованных уполномоченными лицами заявок.

Необходимо периодически осуществлять пересмотр правил межсетевого экранирования для выявления неиспользуемых разрешающих правил.

3.5.21.3. ПОЛИТИКА ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ

3.5.21.3.1. НАЗНАЧЕНИЕ

Политика определяет правила и требования к обеспечению ИБ Компании от НСД.

3.5.21.3.2. ПОЛОЖЕНИЯ ПОЛИТИКИ

Обнаружение и предотвращение вторжений должно осуществляться:

- на границах подключений корпоративной сети Компании к сети Интернет;
- на границах сегментов ДМЗ;
- на границах внутренних сегментов корпоративной сети Компании;
- внутри сегментов корпоративной сети Компании в соответствии с актуальными результатами анализа и оценки рисков нарушения ИБ.

Обнаруженные и предотвращенные вторжения должны быть учтены при анализе и оценке рисков нарушения ИБ.

Должна быть определена отчетная форма для документирования результатов обнаружения и предотвращения вторжений.

Используемые средства обнаружения и предотвращения вторжений должны иметь регулярно обновляемую базу сигнатур.

Средства обнаружения и предотвращения вторжений должны быть настроены таким образом, чтобы обеспечивать оперативное оповещение уполномоченных лиц при выявлении фактов попыток вторжений.

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

3.5.22. ПОЛИТИКА УДАЛЕННОГО ДОСТУПА В КОРПОРАТИВНУЮ СЕТЬ

3.5.22.1. НАЗНАЧЕНИЕ

Политика определяет правила и требования к обеспечению ИБ Компании от угроз безопасности, связанных с использованием удаленного доступа в корпоративную сеть Компании.

3.5.22.2. ПОЛОЖЕНИЯ ПОЛИТИКИ

Удаленный доступ в корпоративную сеть Компании осуществляется работниками Компании и третьими лицами из сторонних сетей связи, в том числе сети Интернет, для работы с ИА Компании.

Необходимо определить ИА, взаимодействие с которыми разрешается с использованием удаленного доступа. Для каждого разрешенного к удаленному использованию ИА необходимо определить порядок предоставления удаленного доступа в рамках соответствующей рабочей и проектной документации на ИА.

При удаленном доступе необходимо:

- использовать двухфакторную аутентификацию удаленных пользователей;
- обеспечить безопасность передаваемой информации от НСД;
- регистрировать все подключения удаленных пользователей;
- проводить проверку безопасности подключающегося устройства, включающую в себя контроль наличия установленных обновлений операционной системы, а также наличия, корректности и актуальности настройки антивирусных средств;
- автоматически блокировать доступ в случае неактивности сеанса пользователя.

Сегмент сети, предназначенный для создания удаленного доступа, должен быть изолирован от остальной корпоративной сети Компании. Взаимодействие сегмента удаленного доступа с остальными сегментами сети необходимо контролировать средствами межсетевого экранирования.

3.5.23. ПОЛИТИКА ЗАЩИТЫ ОТ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

3.5.23.1. НАЗНАЧЕНИЕ

Политика определяет правила и требования к обеспечению ИБ Компании от вредоносного ПО.

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

3.5.23.2. ПОЛОЖЕНИЯ ПОЛИТИКИ

Для обеспечения безопасности от вредоносного ПО должны использоваться средства антивирусной защиты, обеспечивающие обнаружение и устранение вредоносного ПО и последствий от его функционирования.

При построении системы антивирусной защиты должен использоваться принцип эшелонированной защиты. В соответствии с данным принципом, для различных рубежей защиты должны использоваться различные средства антивирусной защиты для увеличения вероятности успешного обнаружения вредоносного ПО.

Вся информация, хранимая, обрабатываемая и передаваемая в корпоративной сети Компании, а также информация, попадаемая в корпоративную сеть извне (по электронной почте, из сторонних сетей связи, в том числе из сети Интернет, с использованием съемных носителей информации и МАРМ, из сторонних ИА), должна подвергаться контролю на отсутствие вредоносного ПО.

Средства антивирусной защиты необходимо устанавливать на сервера ИА, АРМ пользователей и администраторов, МАРМ, СЗИ и компоненты информационно-технологической инфраструктуры.

Периодическая автоматическая проверка наличия сигнатур вредоносного ПО, их загрузка с сайтов производителей и установка должны осуществляться модулем управления средствами антивирусной защиты.

Периодически должна проводиться полная проверка АРМ, МАРМ и серверов ИА на наличие вредоносного ПО.

Средства антивирусной защиты не должны препятствовать корректному функционированию объектов, на которые они установлены.

Пользователи АРМ и МАРМ не должны иметь возможность отключать средства антивирусной защиты и препятствовать их работе.

3.5.24. ПОЛИТИКА ИСПОЛЬЗОВАНИЯ СЗИ

3.5.24.1. НАЗНАЧЕНИЕ

Политика определяет правила и требования к обеспечению ИБ Компании с использованием СЗИ⁵.

⁵ За исключением СКЗИ

3.5.24.2. ПОЛОЖЕНИЯ ПОЛИТИКИ

Использование СЗИ осуществляется для обеспечения безопасности ИА и компонентов информационно-технологической инфраструктуры.

СЗИ должны реализовывать требования по обеспечению безопасности для соответствующего уровня защищенности ИС в зависимости от категории обрабатываемой в ней информации.

Использование СЗИ, прошедших процедуру оценки соответствия требованиям законодательства РФ в области обеспечения безопасности информации является обязательным в следующих случаях:

- когда применение таких СЗИ необходимо для нейтрализации актуальных угроз безопасности персональных данных;
- когда применение таких СЗИ необходимо для защиты ИС, обрабатывающих конфиденциальную информацию;
- когда применение таких СЗИ необходимо для защиты КСИИ.

Во всех остальных случаях решение о применении сертифицированных СЗИ принимает СБ с учетом следующих аспектов:

- актуальная модель угроз безопасности информации;
- экономическая целесообразность использования (не)сертифицированных СЗИ;
- СЗИ используются для централизованного управления КСЗИ;
- СЗИ обеспечивают безопасность компонентов информационно-технологической инфраструктуры, нарушение корректного функционирования которых может нанести Компании значительный ущерб.

3.5.25. ПОЛИТИКА ИСПОЛЬЗОВАНИЯ СКЗИ**3.5.25.1. НАЗНАЧЕНИЕ**

Политика определяет правила и требования к обеспечению ИБ Компании с использованием СКЗИ. Основные принципы применения и использования СКЗИ для обеспечения безопасности информации Компании определены в Методических указаниях «Об организации криптографической защиты информации в Компании» № ПЗ-11.01 М-0020, версия 1.00.

3.5.25.2. ПОЛОЖЕНИЯ ПОЛИТИКИ

В Компании использование СКЗИ осуществляется для защиты информации криптографическими методами при ее обработке на АРМ пользователей, МАРМ, съемных носителях информации и передачи в рамках сеанса работы удаленного пользователя с ИА

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

Компании, а также для защиты информации, передаваемой в рамках территориально распределенных ИА с целью:

- обеспечения конфиденциальности информации;
- обеспечения целостности информации;
- обеспечения неотказуемости и авторства информации;
- аутентификации пользователей при непосредственном доступе к АРМ, при удаленном доступе пользователей к ИА Компании, при доступе в личный кабинет, а также для аутентификации ИА при их интеграции между собой.

Должны быть организованы удостоверяющие центры для выпуска сертификатов ключей проверки электронных подписей. Должны быть определены типы и правила выбора удостоверяющих центров в зависимости от объектов защиты, в рамках которых должны применяться ключи электронной подписи и сертификаты ключей проверки электронной подписи.

Обязательным принимается использование сертифицированных⁶ СКЗИ в следующих случаях:

- когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных⁷;
- когда применение таких средств необходимо для формирования и проверки квалифицированной электронной подписи;
- когда применение таких средств необходимо для организации обмена информацией с органами государственной власти и местного самоуправления Российской Федерации;
- когда применение таких средств необходимо для подключения ИС, информационно-телекоммуникационных сетей и средств вычислительной техники, применяемых для хранения, обработки или передачи информации, обладателями которой являются государственные органы и которая содержит сведения, составляющие служебную тайну, к информационно-телекоммуникационным сетям общего пользования (Интернет);
- когда применение таких средств необходимо для защиты информации, отнесенной в Компании к сведениям конфиденциального характера.

Во всех остальных случаях решение о применении сертифицированных СКЗИ принимает СБ.

В случае принятия решения о применении сертифицированного СКЗИ класс СКЗИ определяется на основании разработанного для объекта защиты документа «Модель нарушителя».

⁶ В системе сертификации ФСБ России.

⁷ Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденные приказом ФСБ России от 10.07.2014 № 378.

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

Применяемые сертифицированные СКЗИ должны подлежать поэкземпляроному учету.

В случаях использования несертифицированных СКЗИ допускается применение зарубежных криптографических алгоритмов.

Должны быть определены порядки и инструкции, в частности:

- использования РКИ и электронной подписи;
- использования СКЗИ для защиты информации, обрабатываемой на АРМ пользователей, МАРМ, съемных носителях информации;
- использования СКЗИ для защиты информации, передаваемой в рамках сеанса работы удаленного пользователя с ИА Компании, а также информации, передаваемой в рамках территориально распределенных ИА;
- при использовании СКЗИ для аутентификации пользователей при непосредственном доступе к АРМ, при удаленном доступе пользователей к ИА Компании, при доступе в личный кабинет, а также для аутентификации ИА при их интеграции между собой;
- использования СКЗИ для защиты различных категорий информации;
- обращения с ключевой информацией;
- использования СКЗИ в зарубежных офисах и представительствах Компании.

Эксплуатация СКЗИ пользователем допускается после ознакомления с эксплуатационной документацией СКЗИ и проведения инструктажа уполномоченным работником Службы безопасности.

3.5.26. ПОЛИТИКА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ НА ЭТАПАХ ЖИЗНЕННОГО ЦИКЛА ИНФОРМАЦИОННЫХ СИСТЕМ

3.5.26.1. НАЗНАЧЕНИЕ

Политика определяет правила и требования к обеспечению ИБ на всех этапах жизненного цикла ИС.

3.5.26.2. ПОЛОЖЕНИЯ ПОЛИТИКИ

Необходимость разработки ИС определяется владельцем бизнес-процесса, который должен быть автоматизирован в разрабатываемой ИС.

Формирование требований к защите информации в разрабатываемой ИС должно включать:

- категорирование информации, обрабатываемой в ИС;
- классификацию ИС по требованиям защиты информации;

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

- определение угроз безопасности информации, реализация которых может привести к нарушению доступности, целостности или конфиденциальности информации и (или) безопасного функционирования ИС, и разработку на их основе модели угроз безопасности информации;
- определение требований к системе защиты ИС.

Требования по защите информации в ИС должны быть включены в Функциональные и технические требования либо Техническое задание на создание ИС и согласованы с СБ.

Технический проект на создание ИС должен содержать результаты классификации разрабатываемой ИС, а также описание защитных мер (технических и (или) организационных), обеспечивающие выполнение требований ФТТ или ТЗ в части защиты информации.

Для определения технической возможности и совместимости при использовании дополнительных СЗИ, т.е. не являющихся составной частью общесистемного или прикладного программного обеспечения, в ИС может быть проведено макетирование (стендовые испытания) СЗИ. Необходимость проведения макетирования СЗИ определяется СБ после выбора технических СЗИ.

При создании и тестировании ИС необходимо:

- обеспечить ИБ среды разработки и тестирования компонентов ИС;
- провести тестирование компонентов ИС;
- разработать эксплуатационную документацию. При проведении опытной эксплуатации должен использоваться ограниченный набор данных, определяемый по согласованию с СБ и руководителем СП, в интересах которого осуществляется внедрение ИС. В рамках проведения опытной эксплуатации рекомендуется проведение комплексной оценки защищенности, включающей проведение:
 - ◆ тестирования на проникновение⁸;
 - ◆ выявления известных уязвимостей компонентов ИС.

Перевод ИС в опытно-промышленную эксплуатацию должен осуществляться только по согласованию сроков со СП, в интересах которого осуществляется внедрение ИС, и с СБ при наличии полного комплекта утвержденной технико-проектной и эксплуатационной документации.

Должна проводиться оценка эффективности реализованных в рамках системы защиты информации мер по обеспечению безопасности информации, обрабатываемой в ИС. Оценка эффективности может проводиться в форме государственной аттестации или оценки соответствия требованиям ИБ. Определение потребности в проведении аттестации и оценки соответствия, порядок проведения аттестации и оценки соответствия определены в

⁸ Для информационных систем Компании, к которым предоставляется публичный доступ и/или которые осуществляют взаимодействие с внешними публичными информационными системами

Положении Компании «Порядок ввода информационных систем в промышленную эксплуатацию» № ПЗ-11.01 Р-0085.

Ввод ИС в промышленную эксплуатацию должен осуществляться в соответствии с Положением Компании «Порядок ввода информационных систем в промышленную эксплуатацию» № ПЗ-11.01 Р-0085.

Требования по обеспечению защиты информации на всех стадиях жизненного цикла ИС должны включаться во все договоры и контракты на проведение работ или оказание услуг по созданию ИС с подрядными (сервисными) организациями.

3.5.27. ПОЛИТИКА РЕЗЕРВНОГО КОПИРОВАНИЯ ИНФОРМАЦИИ

3.5.27.1. НАЗНАЧЕНИЕ

Политика определяет правила и требования к обеспечению ИБ Компании от нарушения целостности и доступности информации.

3.5.27.2. ПОЛОЖЕНИЯ ПОЛИТИКИ

Резервному копированию должны подвергаться информация, обрабатываемая в ИС и ИР, а также конфигурационная информация системного и прикладного программного обеспечения, серверного и сетевого оборудования, а также СЗИ.

Должен быть определен перечень объектов, подлежащих резервному копированию, а также параметры резервного копирования, а именно:

- тип;
- периодичность;
- время восстановления после отказа;
- время допустимой потери до момента отказа;
- время и место хранения резервной копии.

Тип и периодичность резервного копирования должны устанавливаться таким образом, чтобы обеспечить минимальные потери данных и время простоя ИС и ИР.

Резервное копирование должно производиться в автоматическом режиме. Хранение резервных копий рекомендуется осуществлять в специально оборудованных для этих целей помещениях, размещенных на удалении от источника резервного копирования, с целью минимизации рисков утраты резервных копий при аварийных ситуациях. События резервного копирования должны регистрироваться в журнале.

Резервные копии должны подвергаться регулярному тестированию (тестирование целостности самой резервной копии и тестирование восстановления из резервной копии).

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

В случае передачи резервных копий на хранение третьему лицу содержащаяся на них информация должна быть защищена от НСД.

Восстановление информации осуществляется в случае аварий и отказов ИС и ИР. Процедуры восстановления информации могут быть инициированы строго при наличии соответствующей заявки, согласованной владельцем восстанавливаемой ИС/ИР или техническое средство.

Работники обязаны сохранять копию всей значимой рабочей информации, необходимой для обеспечения непрерывности бизнес-процессов, в которых они задействованы, на соответствующих сетевых ресурсах. В случае только локального хранения информации (например, на рабочем столе, локальном диске и т.д.) работник несет персональную ответственность за ее сохранность и возможность восстановления в случае утраты.

Резервные копии, средства резервного копирования и аварийного восстановления должны располагаться на территориальном удалении от объекта проведения аварийного восстановления (на другой площадке).

3.5.28. ПОЛИТИКА ОБУЧЕНИЯ И ПОВЫШЕНИЯ ОСВЕДОМЛЕННОСТИ РАБОТНИКОВ В ОБЛАСТИ ИБ

3.5.28.1. НАЗНАЧЕНИЕ

Политика определяет правила и требования к обеспечению необходимого уровня компетентности работников в области ИБ, а также на предупреждение и снижение угроз нарушения ИБ, связанных с человеческим фактором.

3.5.28.2. ПОЛОЖЕНИЯ ПОЛИТИКИ

Обучение работников Компании осуществляется в соответствии с положениями Стандарта Компании «Организация обучения персонала» № П2-03 С-0005.

В рамках обучения и повышения осведомленности работников в области ИБ должны проводиться следующие мероприятия:

- вводный инструктаж по ИБ для всех принимаемых на работу лиц;
- обязательное обучение работников;
- профессионально-техническое обучение, в том числе повышение квалификации, для работников, решающих специфические задачи по ИБ;
- повышение осведомленности.

При проведении вводного инструктажа работник должен ознакомиться с необходимыми действующими документами, регулирующими вопросы обеспечения ИБ в Компании. Вводный инструктаж проводится до предоставления работнику доступов к информации, ИА.

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

О прохождении инструктажа работник обязан расписаться в соответствующем журнале учета.

Обязательное обучение должно быть направлено на получение знаний безопасной работы с информацией и ИА Компании, в том числе:

- с персональными данными;
- со сведениями конфиденциального характера;
- с электронной почтой Компании и сетью Интернет;
- со средствами вычислительной техники, включая АРМ, МАРМ, съемные носители информации;
- с СЗИ, применяемыми в Компании.

По результатам обучения должно проводиться тестирование для определения уровня освоения учебного материала. Работники, не набравшие необходимые для успешного прохождения тестирования баллы, должны пройти обучение и тестирование повторно. Работник не допускается к работе с информацией, ИА до момента успешного прохождения тестирования.

Профессионально-техническое обучение в области ИБ проводится для специалистов, в должностные обязанности которых входит администрирование СЗИ и управление ИБ в Компании.

Сведения о проведенных обучении и инструктажах работников подлежат учету и должны актуализироваться на регулярной основе.

Повышение осведомленности работников в области ИБ проводится на постоянной основе и включает в себя постоянное размещение информационных материалов по основным угрозам и проблемам безопасности (публикация новостей, размещение информационных щитов и плакатов, установка компьютерных заставок и т. д.) и оперативное доведение информации о появлении новых угроз, методиках реагирования на возможные инциденты, изменениях в нормативно-правовых актах и ЛНД.

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

4. ОТВЕТСТВЕННОСТЬ НАРУШИТЕЛЕЙ ПОЛИТИК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

За несоблюдение требований настоящего Стандарта работники могут быть привлечены к дисциплинарной, административной или уголовной ответственности, в соответствии с действующим законодательством Российской Федерации. В случае нарушения работниками требований настоящего Стандарта, Компания вправе требовать возмещения убытков, причиненных в связи с указанными нарушениями.

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

© ® ПАО «НК «Роснефть», 2017

5. ССЫЛКИ

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
3. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».
4. Федеральный закон от 27.07.2010 № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации».
5. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне».
6. Постановление Правительства РФ от 03.10.2002 № 731 «Об изменении и признании утратившими силу некоторых Постановлений Совета Министров РСФСР, Правительства РСФСР и Правительства Российской Федерации, касающихся государственной регистрации юридических лиц».
7. Постановление Правительства Российской Федерации от 03.11.1994 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии».
8. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденные приказом ФСБ России от 10.07.2014 № 378.
9. ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности.
10. ГОСТ 19781-90 Обеспечение систем обработки информации программное. Термины и определения.
11. Р 50.1.056-2005 Техническая защита информации. Основные термины и определения.
12. Кодекс деловой и корпоративной этики НК «Роснефть» № ПЗ-01.06 П-01 версия 1.00, введенный в действие приказом ОАО «НК «Роснефть» 28.09.2015 № 428
13. Политика Компании «Концепция информационно-технической безопасности ПАО «НК «Роснефть» № ПЗ-11.1 версия 1.00, утвержденная приказом ОАО «НК «Роснефть» от 14.03.2008 № 124.

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

14. Политика Компании «Система управления рисками и внутреннего контроля» № П4-01 П-01, версия 2.00, введенная в действие приказом ОАО «НК «Роснефть» от 16.11.2015 № 522.
15. Стандарт Компании «Охрана сведений конфиденциального характера» № ПЗ-11.03 С-0006 версия 4.00, утвержденный приказом ОАО «НК «Роснефть» от 29.12.2012 № 727.
16. Положение Компании «Требования к защите локальных вычислительных сетей Компании, подключаемых в единую корпоративную телекоммуникационную систему ПАО «НК «Роснефть» № ПЗ-11.01 Р-0123, версия 1.00, утвержденное приказом ПАО «НК «Роснефть» от 26.12.2016 № 804.
17. Стандарт Компании «Информационные технологии. Требования к автоматизированным рабочим местам пользователей корпоративной сети Компании» № ПЗ-04 С-0014 версия 2.00, утвержденный решением Правления ПАО «НК «Роснефть», протокол заседания от 26.09.2016 № Пр-ИС-30п.
18. Стандарт Компании «Политика Компании в области обеспечения инженерно-технической защиты и охраны объектов» № ПЗ-11.01 С-0001 версия 2.00, утвержденный приказом ОАО «НК «Роснефть» от 15.04.2014 № 201.
19. Стандарт Компании «Организация обучения персонала» № П2-03 С-0005 версия 2.00, утвержденный приказом ОАО «НК «Роснефть» от 28.12.2010 № 670.
20. Стандарт Компании «Система внутреннего контроля» № П4-01 С-0018, версия 1.00, введенный в действие приказом ОАО «НК «Роснефть» от 10.03.2015 № 100.
21. Стандарт Компании «Общекорпоративная система управления рисками» № П4-05 С-0012, версия 1.00, введенный в действие приказом ОАО «НК «Роснефть» от 23.03.2016 № 108.
22. Положение Компании «Порядок ввода информационных систем в промышленную эксплуатацию» № ПЗ-11.01 Р-0085 версия 1.00, утвержденное приказом ОАО «НК «Роснефть» от 31.03.2014 № 172.
23. Положение ПАО «НК «Роснефть» «Об инсайдерской информации» № ПЗ-01.04 Р-0014 юл-001 версия 1.00, утвержденное приказом ОАО «НК «Роснефть» от 24.07.2014 № 353.
24. Положение Компании «Обеспечение информационной безопасности зарубежных Обществ Группы и совместных предприятий» № ПЗ-11.01 Р-0088 версия 1.00, утвержденное приказом ОАО «НК «Роснефть» от 29.01.2016 № 43.
25. Стандарт ПАО «НК «Роснефть» «Разграничение полномочий и ответственности при организации обеспечения информационной безопасности ПАО «НК «Роснефть» № ПЗ-11.1 СЦ-001.01 ЮЛ-001 версия 1.00, утвержденный приказом ОАО «НК «Роснефть» от 28.02.2008 № 91.

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

26. Методические указания «Об организации криптографической защиты информации в Компании» № ПЗ-11.01 М-0020, версия 1.00, утвержденные приказом ПАО «НК «Роснефть» от 14.11.2016 №649.

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

© ® ПАО «НК «Роснефть», 2017