КОНТРОЛЬНЫЙ ЭКЗЕМПЛЯР

Якутскэнерго

ПАО «Якутскэнерго»

СТАНДАРТ ОРГАНИЗАЦИИ

ИНТЕГРИРОВАННАЯ СИСТЕМА МЕНЕДЖМЕНТА

ИСМ СТО 00-022.01-22

Политика информационной безопасности ПАО «Якутскэнерго»

© Является интеллектуальной собственностью ПАО «Якутскэнерго»
При перепечатке ссылка обязательна

Предисловие

1. РАЗРАБОТАЛ:

Главный эксперт УБ		Е.М. Тимофеев
должность лица	личная подпись	расшифровка подписи

2. СОГЛАСОВАНО:

Начальник УИТС		О.А. Савин
должность лица	личная подпись	расшифровка подписи

3. СОГЛАСОВАНО:

Заместитель Генерального директора по управлению персоналом и корпоративно-правовому управлению– ПР ИСМ		Д.Ю. Латышев
должность лица	личная подпись	расшифровка подписи

4. СОГЛАСОВАНО:

Заместитель Генерального директора по безопасности		С.Н. Щеголеватый
должность лица	личная подпись	расшифровка подписи

5. СОГЛАСОВАНО:

Первый зам. Ген. директора – главный инженер		И.В. Шкурко
должность лица	личная подпись	расшифровка подписи

6. УТВЕРЖДАЮ:

Генеральный директор		А.А. Стручков
должность лица	личная подпись	расшифровка подписи

7. ВВЕДЕН В ДЕЙСТВИЕ

с « 23 » декабря 2022 г.

Взамен: СТО-00-047.02-21

Приказом ПАО «Якутскэнерго»

№ 2938 от 23.12.2022 г.

КОНТРОЛЬНЫЙ ЭКЗЕМПЛЯР
№ ИСМ СТО 00-022.01-22

Содержание

Принятые обозначения и сокращения 5
1. Вводная часть 6
1.1. Введение 6
1.2. Цели 6
1.3. Задачи 6
1.4. Область действия 6
1.5. Период действия и порядок внесения изменений 7
2. Комплексная система управления ИБ 8
2.1. Общее описание КСУИБ, включая ПОБИ ТС 8
2.1.1. Задачи СУИБ корпоративного сегмента: 8
2.1.2. Задачи ПОБИ ТС: 8
2.2. Взаимодействие с КЦОПЛ ПАО «РусГидро» 9
2.2.1. Задачи КЦОПЛ ПАО «РусГидро»: 9
2.2.2. Регламентация деятельности КЦОПЛ 10
2.3. Требования к применяемым техническим решениям 10
2.3.1. Требования к КСУИБ 10
2.3.2. Требования по взаимодействию с КЦОПЛ ПАО «РусГидро» 11
2.3.3. Требования по импортозамещению 11
3. Частные политики ИБ 13
3.1. Требования к организации управления и контроля доступа к информационным ресурсам 13
3.1.1. Порядок предоставления работникам Общества доступа к ИС 13
3.1.2. Парольная политика 14
3.1.3. Порядок отмены и изменения прав доступа пользователей к информационным ресурсам 18
3.1.4. Предоставление удаленного доступа 18
3.1.5. Требования по реализации контроля доступа 19
3.2. Обеспечение ИБ при использовании АРМ и информационных ресурсов 20
3.2.1. Требования по использованию АРМ 20
3.2.2. Требования по использованию ноутбуков 22
3.2.3. Требования по использованию мобильных устройств 22
3.2.4. Требования к использованию КЭП 23
3.2.5. Требования по использованию сети Интернет 25
3.2.6. Требования ИБ при замене АРМ или передаче в ремонт 28
3.2.7. Действия в нестандартных ситуациях 28
3.3. Требования к обеспечению антивирусной защиты 29
3.3.1. Требования к САЗ 29
3.3.2. Требования к конфигурации средств САЗ 29
3.3.3. Требования по контролю функционирования САЗ 30

3.4. Требования по защите сетевого периметра 30
3.4.1. Меры по обеспечению безопасности 31
3.4.2. Требования по построению эшелонированной защиты 31
3.4.3. Требования по сегментации и фильтрации 31
3.4.4. Требования к зонам безопасности 32
3.4.5. Требования по управлению доступом 32
3.4.6. Требования по контролю за сетевой безопасностью 33
3.5. Требования по контролю защищенности 33
3.5.1. Проведение инструментального контроля защищенности ИС 34
3.5.2. Проведение тестирования на проникновение 34
3.5.3. Требования по реализации контроля целостности 35
3.6. Требования ИБ при подключении дочерних организаций к информационным ресурсам Общества 35
3.6.1. Минимально необходимые требования ИБ 35
3.6.2. Контроль выполнения требований ИБ 36
4. Порядок сопровождения ИС, АСУ и ИТС 37
4.1. Обеспечение ИБ на стадиях жизненного цикла ИС, АСУ и ИТС 37
4.2. Профилактика нарушений Политики 38
4.3. Ликвидация последствий нарушения Политики 40
4.4. Ответственность за нарушение Политики 40
5. Внедрение 40
6. Внесение изменений 41
7. Отмена и изъятие 41
8. Рассылка и хранение 41
Лист регистрации изменений 42
Лист ознакомления 43

КОНТРОЛЬНЫЙ ЭКЗЕМПЛЯР
№ ИСМС-СТО-00-022.01-13

Принятые обозначения и сокращения

АРМ	Автоматизированное рабочее место
АСУ	Автоматизированная система управления
ГосСОПКА	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации
ИД	Исполнительная дирекция ПАО «Якутскэнерго»
ИБ	Информационная безопасность
ИС	Информационные системы Общества
ИТС	Информационно-телекоммуникационная сеть
Ключевые ИС	Ключевые информационные системы Общества
КТ	Коммерческая тайна
КСПД	Корпоративная сеть передачи данных
КСУИБ	Комплексная система управления информационной безопасностью
КЦОПЛ	Корпоративный центр обнаружения, предупреждения и ликвидации последствий компьютерных атак ПАО «РусГидро»
КЭП	Корпоративная электронная почта
ЛВС	Локальная вычислительная сеть
НКЦКИ	Национальный координационный центр по компьютерным инцидентам
НСД	Несанкционированный доступ
Общество	ПАО «Якутскэнерго»
ОС	Операционная система
ПК	Персональный компьютер
ПО	Программное обеспечение
ПОБИ ТС	Подсистема обеспечения безопасности информации технологических систем
САЗ	Система антивирусной защиты
СЗИ	Средства защиты информации
УБ	Управление безопасности
УИТС	Управление информационных технологий и связи
DLP	Предотвращение утечки данных (Data Leakage Prevention)
VPN	Виртуальная частная сеть (Virtual Private Network)

КОНТРОЛЬНЫЙ ЭКЗЕМПЛЯР
№ исм/СТО-00-022-01142

1. Вводная часть

1.1. Введение

Политика информационной безопасности ПАО «Якутскэнерго» (далее – Политика) описывает правила ИБ, обеспечения защиты информации, в том числе ограниченного распространения и доступа, и является основным документом, регламентирующим деятельность Общества в области безопасности информационных технологий.

1.2. Цели

Настоящая Политика разработана с целью информирования работников Общества об обязательных требованиях по защите информации и информационных ресурсов.

1.3. Задачи

Задачами настоящей Политики являются:

- Организация системы управления ИБ в Обществе.
- Определение частных политик ИБ, а именно:
  - политики реализации управления и контроля доступа к информационным ресурсам;
  - политики реализации антивирусной защиты;
  - политики организации защиты сетевого периметра;
  - политики организации контроля целостности;
  - политики организации защиты информации при подключении дочерних обществ к информационным ресурсам Общества.
- Определение порядка сопровождения ИС.

1.4. Область действия

Настоящая Политика распространяется на всех работников Общества.

Требования настоящей Политики распространяются также на иных лиц, имеющих доступ к информации, принадлежащей Обществу, на основании трудовых обязанностей или договорных отношений, включая:

- работников подрядчиков, поставщиков товаров, физических лиц, выполняющих работы / оказывающих услуги Обществу;
- партнеров, клиентов и других внешних пользователей.

Настоящая Политика рекомендована для применения путем включения ссылок на нее и (или) прямого использования устанавливаемых в ней положений и требований в локальных нормативных документах (актах) Общества, а также в договорах, заключаемых Обществом с контрагентами.

Использование и организация защиты сведений, составляющих государственную тайну, политика обеспечения безопасности критической информационной инфраструктуры Общества и требования к организации защиты технологических сегментов АСУ ТП регулируются отдельными локальными нормативными документами (актами) Общества.

1.5. Период действия и порядок внесения изменений

Введение в действие и внесение изменений в настоящую Политику осуществляются на основании локального нормативного документа (акта) Общества.

Инициаторами внесения изменений в Политику могут являться:

- ответственный за информационную безопасность Общества;
- УИТС;
- иные структурные подразделения Общества по согласованию с УИТС.

Плановая актуализация настоящей Политики производится 1 (один) раз в 3 (три) года.

Внеплановая актуализация настоящей Политики производится в обязательном порядке в следующих случаях:

- при внесении существенных изменений в типовые конфигурации программно-аппаратных средств ИС, зафиксированных в Технической политике ПАО «РусГидро» в области информационных технологий;
- при изменении политики Российской Федерации в области ИБ и / или издании новых нормативных правовых актов в сфере защиты информации;
- при изменении категорий обрабатываемой информации в ИС;
- при изменении локальных нормативных документов (актов) (инструкций, положений, руководств), касающихся ИБ Общества;
- при существенных изменениях условий эксплуатации КСПД Общества, влияющих на исполнение настоящей Политики;
- при происшествии и / или выявлении инцидента (инцидентов) по нарушению ИБ, влекущих материальный ущерб Общества.

Ответственным за актуализацию настоящей Политики (плановую и внеплановую) является начальник УИТС.

Контроль за исполнением требований настоящей Политики осуществляет заместитель Генерального директора – ответственный за информационную безопасность Общества.

2. Комплексная система управления ИБ

2.1. Общее описание КСУИБ, включая ПОБИ ТС

Основной целью КСУИБ является обеспечение безопасности информационной инфраструктуры Общества и выполнение требований законодательства Российской Федерации в области защиты КТ и персональных данных, обеспечении безопасности объектов критической информационной инфраструктуры Общества.

2.1.1. Задачи СУИБ корпоративного сегмента:

- обеспечение конфиденциальности, целостности и доступности информационных ресурсов Общества;
- обеспечение защиты от утечек конфиденциальной информации;
- обеспечение защиты от НСД к АРМ и серверам, в том числе задействованным в хранении или обработке конфиденциальной информации;
- обеспечение защиты АРМ и серверов от вредоносного программного обеспечения;
- обеспечение криптографической защиты каналов связи между сегментами КСПД;
- обеспечение защиты виртуальной инфраструктуры Общества;
- обеспечение контроля действий привилегированных пользователей (администраторов) в сети и на серверах информационных систем;
- обеспечение контроля доступа на сетевом и транспортном уровнях к информационным ресурсам, содержащим или обрабатывающим информацию ограниченного распространения и доступа (служебной, коммерческой тайна, персональные данные);
- обеспечение контроля использования сменных носителей информации на рабочих станциях Общества;
- обеспечения контроля информации, выводимой на печать;
- обеспечение централизованного управления средствами защиты информации;
- предоставление администраторам ИБ средств анализа и управления рисками ИБ;
- предоставление администраторам ИБ средств для проведения расследований инцидентов ИБ.

2.1.2. Задачи ПОБИ ТС:

- обеспечение выполнения требований законодательства Российской Федерации о безопасности критической информационной инфраструктуры Российской Федерации;
- обеспечение защиты автоматизированных систем управления технологического сегмента, включая защиту объектов критической информационной инфраструктуры Общества;
- автоматизация процессов защиты автоматизированных систем управления;

- обеспечение требуемого уровня доступности и целостности технологической информации при обработке и передаче ее в технологических сегментах;
- обеспечение безопасности при информационном обмене АСУ ТП с внешними ИС;
- минимизация рисков технологического и экономического характера, возникающих при обработке и передаче информации в технологических сегментах;
- минимизация рисков вредоносного воздействия и НСД к информационным ресурсам технологических сегментов.

2.2. Взаимодействие с КЦОПЛ ПАО «РусГидро»

Основной целью КЦОПЛ ПАО «РусГидро» является обнаружение, предупреждение и ликвидация последствий компьютерных атак на информационные системы, автоматизированные системы управления и информационно-телекоммуникационные сети ПАО «РусГидро» и подконтрольных организаций, включая ПАО «Якутскэнерго»

Для достижения основной цели необходимо выполнение мероприятий:

- подключение к технической инфраструктуре КЦОПЛ ПАО «РусГидро» со стороны Общества;
- организация мониторинга состояния ИБ, включая мониторинг состояния ИБ объектов критической информационной инфраструктуры Группы РусГидро, включая ПАО «Якутскэнерго»;
- развитие сил и средств Общества в соответствии с нормативно-методическими документами в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;
- разработка Регламента взаимодействия Общества с КЦОПЛ с утверждением зон ответственности.

2.2.1. Задачи КЦОПЛ ПАО «РусГидро»:

- Обеспечение процессов обнаружения, предупреждения и ликвидации последствий компьютерных атак, направленных объекты критической информационной инфраструктуры Группы РусГидро.
- Реагирование на компьютерные инциденты.
- Сбор и анализ данных о состоянии информационной безопасности.
- Обеспечение контроля за событиями информационной безопасности, выявления, анализа и участия в устранении компьютерных инцидентов информационной безопасности и уязвимостей.
- Оценка степени защищенности информационных ресурсов Группы РусГидро.
- Круглосуточный мониторинг состояния информационной безопасности Группы РусГидро.
- Контроль за актуальностью сведений об информационных ресурсах Группы РусГидро.

2.2.2. Регламентация деятельности КЦОПЛ

Деятельность КЦОПЛ регламентируется документами, разработанными в соответствии с Методическими рекомендациями по созданию ведомственных и корпоративных центров ГосСОПКА (приказ ФСБ России от 27.12.2016 №149/2/7-200) и утверждаются отдельными локальными нормативными документами (актами) ПАО «РусГидро» и не являются частью настоящей Политики.

2.3. Требования к применяемым техническим решениям

2.3.1. Требования к КСУИБ

Организационные и технические меры защиты информации должны реализовываться в КСУИБ с учетом актуальных угроз безопасности информации, используемых информационных технологий, структурно-функциональных характеристик ИТ-инфраструктуры Общества и особенностей ее функционирования.

Совокупность реализуемых организационных и технических мер защиты информации должна обеспечивать выполнение требований законодательства Российской Федерации к защите персональных данных и обеспечении безопасности объектов критической информационной инфраструктуры Общества.

ИТ-инфраструктура Общества представлена следующими уровнями:

- Уровень ИС ИД Общества, который включает:
  - серверы приложений и баз данных основных критически важных ИС (включая серверы ИС персональных данных), размещенные на физических серверах и в виртуальной инфраструктуре;
  - централизованные публичные информационные ресурсы Общества;
  - централизованные сервисы мониторинга и управления ИТ-инфраструктурой и ИБ Общества;
  - АРМ пользователей.
- Уровень ИС филиала Общества, который включает локальные для филиала сервисы и службы базовой информационной инфраструктуры, локальные для филиала ИС, ИС персональных данных и АРМ пользователей.
- Уровень технологических систем филиала Общества, включающий сегменты технологических сетей передачи данных, автоматизированных систем, задействованных в мониторинге и управлении технологическими процессами, релейных защит и автоматики, противоаварийной автоматики.

Архитектура КСУИБ с учетом структурно-функциональных характеристик ИТ-инфраструктуры Общества и особенностей ее функционирования должна строиться по иерархическому принципу – уровень ИС ИД Общества должен обеспечивать сервисы управления и мониторинга ИБ для нижестоящих, для чего в состав КСУИБ необходимо включать специализированные компоненты подсистем и функциональных модулей КСУИБ, при этом необходимо выделять ряд централизованных для всей информационной инфраструктуры функциональных модулей, а также подсистемы и функциональные модули, реализуемые только на уровне ИС ИД Общества.

При создании/модернизации систем ИБ ИД Общества или его филиалов необходимо использовать технические решения, включенные в Реестр типовых технических решений ИБ ПАО «РусГидро» (далее – Реестр). В случае, если при проведении технорабочего проектирования в ИД Общества или его филиалах будут выявлены условия, при которых применение технического решения, зафиксированного в Реестре невозможно/нецелесообразно, допускается применение эквивалентов. Допустимо использование эквивалентов применяемым техническим решениям, зафиксированным в типовом техническом проекте (за исключением случаев, определенных в п. 6.4.4 (а) Единого положения о закупке продукции для нужд Группы РусГидро) при одновременном выполнении следующих условий:

- эквивалент дешевле при одинаковой функциональности;
- эквивалент бесшовно интегрируется в существующую КСУИБ, не требует дополнительных затрат на интеграцию и управляется из единой консоли управления, уже развернутой в Обществе;
- эквивалент полностью соответствует требованиям Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и иных нормативных правовых актов.

2.3.2. Требования по взаимодействию с КЦОПЛ ПАО «РусГидро»

Требования по взаимодействию с КЦОПЛ ПАО «РусГидро» утверждаются отдельными локальными нормативными документами (актами) ПАО «РусГидро» и не являются частью настоящей Политики.

Архитектура технических средств КЦОПЛ должна быть организована по иерархическому принципу, где каждый нижестоящий уровень должен передавать данные об обнаружении компьютерных атак на вышестоящий уровень, при этом каждый вышестоящий уровень должен передавать данные (команды) о предупреждении и ликвидации последствий компьютерных атак на нижестоящие уровни.

2.3.3. Требования по импортозамещению

Импортозамещение направлено на снижение степени влияния зарубежных технологий на деятельность производственных объектов Общества.

Увеличение доли продукции отечественных производителей при планировании и реализации производственных программ Общества достигается за счет:

- минимизации использования импортного оборудования, материалов и технологий при разработке технических заданий на выполнение проектных работ и при формировании проектных решений по созданию новых и модернизации существующих систем информационной безопасности с учетом законодательства Российской Федерации в части импортозамещения;
- приоритета закупки российской продукции (работ, услуг), эквивалентной по техническим характеристикам и потребительским свойствам иностранной продукции (работам, услугам), при формировании технических требований к закупаемой продукции.

Применение импортного оборудования, устройств, материалов и технологий на объектах Общества допускается исключительно в случае отсутствия отечественных аналогов, эквивалентных по техническим характеристикам и потребительским свойствам иностранной продукции, и / или необходимости обеспечения технической совместимости с существующим оборудованием с соответствующим согласованием с ПАО «РусГидро»

Отечественные аналоги импортной продукции до включения в проектную документацию по созданию новых и модернизации существующих систем информационной безопасности должны пройти необходимые качественные, ресурсные или иные испытания, а также сертификацию в соответствии с нормативной и технической документацией, распространяющей свои требования к данному виду (типу) продукции на территории Российской Федерации.

В Обществе обеспечивается переход на преимущественное использование отечественного программного и аппаратного обеспечения и исполнение следующих требований законодательства Российской Федерации:

1. Средства защиты информации, используемые в Обществе, только отечественного производства[1].
2. Реализация в Обществе комплекса мероприятий, направленных на обеспечение преимущественного применения Обществом критической информационной инфраструктуры отечественных радиоэлектронной продукции и телекоммуникационного оборудования на принадлежащих Обществу значимых объектах критической информационной инфраструктуры[2].

[1] Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

[2] Указ Президента Российской Федерации от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»

3. Частные политики ИБ

3.1. Требования к организации управления и контроля доступа к информационным ресурсам

Настоящий раздел Политики определяет требования по обеспечению защиты ИС и ресурсов Общества от НСД, парольную политику и устанавливает единый порядок предоставления, изменения, ограничения и контроля доступа к информационным ресурсам в Обществе.

Настоящий раздел Политики направлен на достижение следующих целей:

- определение порядка предоставления, прекращения и изменения доступа пользователей к ИС, включая сетевые сервисы, разделяемые сетевые файловые ресурсы;
- определение парольной политики Общества;
- определение порядка изменения прав доступа пользователей к ИС при переходе на другую должность, изменении трудовых обязанностей;
- определение порядка отмены доступа при увольнении работника Общества;
- определение требований, предъявляемых к работникам Общества, в случае предоставления им доступа к ИС;
- определение порядка контроля доступа к информационным ресурсам.

3.1.1. Порядок предоставления работникам Общества доступа к ИС

Доступ к ИС предоставляется:

- работникам Общества;
- лицам, работающим по договору гражданско-правового характера;
- лицам, работающим по договору аутсорсинга;
- сотрудникам иных юридических лиц, осуществляющих деятельность, согласно договору с Обществом, с предварительным согласованием с главным инженером/генеральным директором Общества.

Для предоставления работникам Общества доступа к ИС необходимо проведение процедуры их регистрации в качестве пользователей, в результате которой для каждого работника должна быть создана одна именная учетная запись, используемая для получения доступа к рабочему АРМ, сетевым сервисам и разделяемым сетевым файловым ресурсам. Исключение могут составлять работники, которым в силу специфики их трудовых обязанностей необходимо иметь более одной учетной записи.

Учетная запись пользователя должна включать данные, однозначно идентифицирующие данного пользователя, и служить для определения пользовательских полномочий по доступу к ИС, а также для осуществления контроля над действиями пользователей.

Работникам Общества запрещено:

- использование учетных записей других пользователей для осуществления доступа к ИС;
- работа из-под локальной учетной записи в КСПД.

Каждому пользователю присваивается уникальное имя и предоставляется возможность сформировать пароль. Для идентификации в системе пользователь обязан вводить только свои имя и пароль (учетную запись).

Права доступа к ИС предоставляются пользователю:

- на время и в объеме, необходимом для исполнения им трудовых обязанностей;
- только после ознакомления с документами, регламентирующими правила работы пользователей в ИС (при первом доступе к ИС).

Доступ к ИС предоставляется УИТС на основании заявки, подписанной руководителем структурного подразделения ИД или руководством (директором, заместителем директора, главным инженером, заместителем главного инженера) филиала Общества. Доступ предоставляется с соблюдением принципов разумной достаточности и минимальной необходимости после согласования с УБ.

Руководители структурных подразделений ИД, руководство (директор, заместитель директора, главный инженер, заместитель главного инженера) филиала Общества несут ответственность за предоставление их подчиненным работникам доступа к ИС в строгом соответствии с их трудовыми обязанностями.

Административный доступ к системам ИБ и Ключевым ИС необходимо осуществлять только при использовании систем класса PAM (контроль привилегированных пользователей).

3.1.2. Парольная политика

3.1.2.1. Общие требования к паролям и парольной защите

В целях контроля использования ИС и сервисов корпоративной сети Общества доступ разрешается только после прохождения пользователем процедур идентификации и аутентификации (легальный субъект).

Для каждого легального субъекта доступа к объектам ИС должен быть установлен пароль или, в случае необходимости, несколько паролей следующих типов:

- административный – пароль легального субъекта доступа с правами администратора. Предназначен для обеспечения доступа к объектам и их ресурсам с максимальными правами по изменению параметров (конфигурации) объекта, предоставления другим субъектам доступа конкретных прав;
- пользовательский – пароль легального субъекта доступа с правами пользователя, предназначенный для обеспечения доступа к ресурсам.

Учетные данные пользователя и его пароль являются строго индивидуальными, создание единых идентификаторов и паролей на несколько лиц («гостевые входы») и передача пароля другим лицам запрещается. Данное требование не относится к технологическим идентификаторам и паролям, предназначенным для управления отдельными процессами в ИС. Учетные данные администраторов не должны содержать

признаков, позволяющих идентифицировать их принадлежность к привилегированным пользователям (например, наличие слов adm, root и т.д.).

Процедура аутентификации должна предусматривать в составе реквизитов доступа пароль с возможностью его смены пользователем.

Для обеспечения исполнения настоящей Политики необходимо использовать встроенные механизмы эксплуатируемых ИС (сервисов).

К паролям доступа в Обществе предъявляются следующие требования:

- для администраторов ИС и сервисов корпоративной сети, администраторов безопасности, администраторов САЗ, доступа к административным учетным записям серверов и коммутационного оборудования:
  - длина пароля должна составлять не менее 15 (пятнадцати) символов;
  - генерацию новых паролей необходимо осуществлять на основе псевдослучайных функций;
  - изменение пароля администраторов ИС 1 (один) раз в 90 (девяносто) дней.
- для сервисных учетных записей:
  - длина пароля должна составлять не менее 32 символов;
  - пароль должен содержать печатные символы из 4 (четырех) категорий:
    - прописные буквы A…Z;
    - строчные буквы a…z;
    - цифры 0…9;
    - специальные символы @, #, $, &, *, % и т.п.;
  - смена паролей производится по усмотрению ответственного лица, при условии соответствия сложности пароля минимальным характеристикам безопасности;
  - при выборе нового пароля запрещается циклическое использование старых паролей: новый пароль не должен совпадать ни с одним из ранее использовавшихся паролей.
- для пользователей корпоративной сети:
  - длина пароля должна составлять не менее 10 (десяти) символов;
  - использовать только NTLM-хеши (в случае применения АРМ на платформе Windows);
- общие требования:
  - пароль должен содержать печатные символы из 4 (четырех) категорий:
    - прописные буквы A…Z;
    - строчные буквы a…z;
    - цифры 0…9;
    - специальные символы @, #, $, &, *, % и т.п.;
  - **пароль не должен:**
    - содержать имена, названия компаний, даты рождений и т.д.;
    - совпадать ни с одним из последних 10 (десяти) использованных ранее паролей;

- включать легко вычисляемые сочетания символов (например, последовательно расположенные на клавиатуре символы: «12345678», «QWERTY»), содержать названия ИС или общепринятые сокращения («ИС», «USER» и т.п.).

- для различных ИС, не включенных в единый контур аутентификации, должны устанавливаться собственные, отличающиеся пароли;
- начальный пароль, задаваемый администратором ИС для обеспечения первого входа пользователя в ИС с принудительным требованием смены начального пароля, может не соответствовать минимальным требованиям по сложности в случае, если активация учетной записи происходит непосредственно перед входом пользователя в ИС.

К настройкам парольной политики информационных ресурсов предъявляются следующие требования:

- блокировка учетной записи после 5 (пяти) неудачных попыток входа с периодом блокировки продолжительностью 180 (сто восемьдесят) минут (или до разблокировки учетной записи администратором);
- блокировка сеанса работы пользователя через 15 (пятнадцать) минут неактивности работы за компьютером с требованием ввода пароля для разблокировки;
- изменение пароля пользователя 1 (один) раз в 42 (сорок два) дня;
- установка уникального первоначального пароля для каждого пользователя и требование его немедленного изменения при первом входе пользователя в ИС;
- ведение учета всех попыток входа в ИС (успешных и неуспешных) с хранением данных (дата время, сетевой идентификатор устройства) сроком не менее 90 (девяноста) дней.

Исключения (по согласованию с УБ) при настройке парольной политики могут составлять:

- требования по периодической смене пароля сервисной учетной записи;
- отсутствие технической возможности реализации конкретного требования парольной политики;
- требования по блокировке рабочего стола в случае неактивности со стороны пользователя более 15 (пятнадцати) минут в целях производственной необходимости (например, для АРМов АСУ ТП, отображающих технологический процесс производства).

3.1.2.2. Требования по организации и ведению системы парольной защиты

Обязанности по ведению системы парольной защиты должны быть возложены на администраторов ИС, в рамках которых они организовывают формирование паролей всех типов и реализуют мероприятия по обеспечению их плановой и внеплановой смены.

Пользовательские пароли первоначально формируются администратором ИС (начальные пароли) при заведении учетной записи в службе каталогов Active Directory и должны быть переданы пользователю лично. Допускается, с согласия пользователя,

доведение до него начального значения пароля по его рабочему телефону. Начальный пароль должен быть изменен пользователем после первого входа в систему и отвечать требованиям п. 3.1.2.1 настоящей Политики. Периодическую смену пароля пользователи производят самостоятельно.

Формирование и смена административного пароля должны производиться администратором ИС. После смены административного пароля администратор должен обеспечить его конфиденциальность и сохранность. Администратор ИС несет ответственность за правильность формирования, выполнение правил хранения и обеспечение конфиденциальности административного пароля.

После смена административного пароля администратор ключевых ИС фиксирует пароль на бумажном носителе, помещает его в непрозрачный конверт и передает руководителю подразделения для последующего хранения в сейфе. Список ключевых ИС, пароли которых должны храниться в бумажном виде, определяются отдельным распорядительным документом по Обществу. Пароль является строго конфиденциальной информацией. Каждый работник Общества несет ответственность за правильность формирования и хранения своих паролей. Запрещается передавать, записывать и сообщать кому-либо, включая системных администраторов и администраторов ИС, свой пароль для доступа к ИС.

Конфиденциальность пароля однозначно идентифицирует и определяет личную ответственность пользователя за действия в ИС.

Ввод (установка, смена) пароля должен проводиться так, чтобы исключить его компрометацию (возможность знания его другим лицом или подозрение на это).

В случае компрометации либо подозрении на компрометацию служебной учетной записи необходимо проведение внеплановой смены паролей всех зависящих от нее учетных записей в течении одного рабочего дня с момента обнаружения факта компрометации с обязательным оповещением УБ и УИТС.

Также внеплановую полную смену паролей всех учетных записей необходимо производить в случае прекращения полномочий (увольнение, перевод на работу в другое подразделение и другие обстоятельства) администратора и других работников, которым по роду работы были предоставлены полномочия по управлению парольной защитой.

3.1.2.3. Требования по контролю соблюдения парольной политики

Для контроля выполнения требований парольной защиты в Обществе должны проводиться периодические выборочные проверки использования паролей пользователями.

Мероприятия по контролю организует УБ.

В ходе проверок необходимо проведение следующих действий:

- контроль настроек доменных политик в части парольной защиты;
- контроль настроек серверов и активного сетевого и телекоммуникационного оборудования в части парольной защиты;
- аудит журналов регистрации событий по операциям смены паролей;
- наблюдение за действиями работников Общества.

Проверки могут выполняться с консолей администрирования технических средств и с применением специальных технических средств.

3.1.3. Порядок отмены и изменения прав доступа пользователей к информационным ресурсам

При прекращении трудовых отношений с работниками Общества, а также с лицами, работающим по договору гражданско-правового характера или по договору аутсорсинга со стороны УИТС по согласованной заявке должна производиться блокировка всех пользовательских учетных записей пользователя.

В случае изменения трудовых обязанностей работника Общества, перевода на другую должность, в другое структурное подразделение и т.п. его прежний руководитель подает заявку на ограничение прав доступа пользователя к ИС. В заявке необходимо указать дату ограничения прав доступа, перечень ресурсов и полномочий, назначенных пользователю ранее.

Расширение прав доступа пользователей к ИС необходимо производить в соответствии с порядком предоставления доступа, указанным в пункте 3.1.1 настоящей Политики.

При наличии отметки об отмене ранее назначенных пользователю прав доступа к ИС в заявке, перед назначением пользователю новых прав доступа системный администратор обязан ликвидировать все права доступа, назначенные пользователю ранее и несовпадающие с правами, указанными в заявке.

3.1.4. Предоставление удаленного доступа

При необходимости осуществления своих трудовых обязанностей вне стационарных рабочих мест работникам Общества может быть предоставлен удаленный доступ к ИС в режиме терминального доступа.

Доступ пользователей вне периметра Общества допускается только в режиме шифрования данных (по каналам сети Интернет) с обязательным проведением процедур аутентификации работников. На компьютерах в обязательном порядке должно быть установлено антивирусное ПО с актуальными обновлениями на момент установки и дальнейшим периодическим автоматическим обновлением.

Публикация WEB-ресурсов, находящихся внутри корпоративной сети Общества, осуществляется только с помощью средств защиты информации типа Applications Firewall, с использованием TLS-технологий и должны быть подключены к системам мониторинга состояния информационной безопасности Общества. WEB-ресурсы, которые не нуждаются в интеграции с элементами инфраструктуры Общества и иными ИС должны быть вынесены за пределы КСПД и размещены во внешнем облаке провайдера.

В случае необходимости предоставления доступа работникам сторонней организации к ИС должен быть заключен договор или подписано соглашение о конфиденциальности.

Право доступа к информационным ресурсам Общества через сеть Интернет предоставляется в порядке, установленным Регламентом предоставления удаленного доступа

В рамках работ по заявке исполнитель должен предоставить доступ к ИС и в дальнейшем заблокировать его в следующих случаях:

- окончания заявленного срока предоставления доступа;
- длительного (более 2 (двух) месяцев) отсутствия подключений;
- нарушение работником или третьим лицом требований ИБ.

При удаленном доступе все действия пользователей должны протоколироваться на межсетевом экране, на серверах, в системах предоставления удаленного доступа и в системах контроля действий привилегированных пользователей.

Пользователи обязаны во время сеанса работы в удаленном режиме с ИС исключить возможность доступа к рабочей станции посторонних лиц. При отсутствии активности пользователя при удаленном подключении в течение установленного времени должна быть выполнена автоматическая блокировка сессии удаленного подключения.

Пользователи в обязательном порядке должны оповестить УБ и УИТС в случае появления подозрений на НСД с использованием их аутентификационных данных.

3.1.5. Требования по реализации контроля доступа

Контроль доступа к информационным ресурсам необходимо осуществлять путем регулярного проведения аудита системы управления доступом (предоставления, изменения, отмены и использования прав доступа) к корпоративной сети Общества, а также путем регистрации событий, связанных с получением доступа к сетевым ресурсам. Мероприятия по контролю организует УБ.

В Обществе должен осуществляться регулярный анализ журналов регистрации событий, происходящих в корпоративной сети, с целью выявления попыток обхода механизмов защиты информации и получения НСД к корпоративным информационным ресурсам Общества.

С целью своевременного выявления уязвимостей системы защиты ИС и предупреждения возможных нарушений требований ИБ должны проводиться проверки уровня защиты сетевых ресурсов с использованием средств и методов анализа защищенности, включающих имитацию действий потенциального злоумышленника по осуществлению НСД к информации.

В Обществе должны применяться средства контроля доступа и другие меры защиты для обеспечения конфиденциальности, целостности и доступности информации, обрабатываемой в ИС. С этой целью, в случае необходимости, ответственным работникам Общества могут быть предоставлены следующие права:

- ограничивать или отменять полномочия любого пользователя;
- проверять, копировать, удалять или иным способом изменять любые данные, программы и другие системные ресурсы, из-за которых перечисленные выше цели могут оказаться недостижимыми;
- предпринимать любые другие действия, необходимые для обеспечения информационной безопасности корпоративной сети Общества.

Все перечисленные действия могут осуществляться как с уведомлением пользователей, которых затрагивают эти изменения, так и без такового.

3.2. Обеспечение ИБ при использовании АРМ и информационных ресурсов

Настоящий раздел Политики регламентирует обеспечение ИБ рабочих станций и информационных ресурсов с целью применения методов, мер и средств, направленных на минимизацию риска НСД к АРМ, предотвращение несанкционированных действий пользователей с конфиденциальной информацией, а также определяет основные принципы безопасного использования пользователями ресурсов ИС.

Все пользователи при получении первичного доступа к ресурсам ИС обязаны ознакомиться с требованиями настоящей Политики.

Каждый пользователь несет ответственность за свои действия и обязан строго соблюдать установленные правила по работе с программными и техническими средствами ИС.

Информация, создаваемая, получаемая и хранимая в ИС, считается собственностью Общества, если иное не оговорено соответствующими соглашениями. Общество оставляет за собой право протоколировать и контролировать действия работников при обработке ими информации в ИС.

Все АРМ, на которых обрабатывается информация ограниченного доступа, должны быть оборудованы необходимыми средствами защиты информации в соответствии с требованиями регуляторов. Запрещено использование АРМ, которые невозможно оснастить средствами защиты информации, используемыми в Обществе. Обработка персональных данных в системах, отличных от информационных систем персональных данных, запрещена.

Пользователи ИС:

- не имеют права предпринимать попыток получить НСД к информационным ресурсам ИС (перебор паролей, использование уязвимостей и неправильных настроек ИС);
- обязаны не разглашать информацию о процедурах и технической реализации защиты информации, принятых в Обществе;
- должны информировать своего непосредственного руководителя, УБ и УИТС обо всех выявленных ими фактах нарушения настоящей Политики.

3.2.1. Требования по использованию АРМ

В соответствии с локальными нормативными документами (актами) Общества пользователю выделяется АРМ с предустановленным программным обеспечением в соответствии с Реестром разрешенного / запрещенного к использованию программного обеспечения. Для доступа к информационным ресурсам ИС АРМ подключается к КСПД Общества. АРМ предоставляется пользователям во временное пользование на период работы в Общества и должен использоваться ими для исполнения своих трудовых обязанностей.

Пользователям разрешен доступ только к рабочим станциям, находящимся на их рабочих местах или доступ к которым предусмотрен их трудовыми обязанностями, а также в случае временного замещения пользователя АРМ. Выполнение на рабочих станциях

других пользователей любых операций запрещено, если иное не определено их непосредственными трудовыми обязанностями.

Пользователям запрещено использование АРМ, подключенных к КСПД, но не подключенных к службе каталогов Общества.

Пользователи при уходе с рабочего места обязаны блокировать доступ к рабочей станции (в операционной системе Windows путем одновременного нажатия клавиш Ctrl, Alt, Delete, а затем – выбора в появившемся меню позиции «Блокировать компьютер» или путем нажатия Win+L), если блокировка не прервет технологический процесс и выполнение трудовых обязанностей. При отсутствии активности пользователя на рабочей станции в течение 15 (пятнадцати) минут должна выполняться автоматическая блокировка сессии учетной записи пользователя, если блокировка не прервет технологический процесс и выполнение трудовых обязанностей.

Пользователь обязан ежедневно выключать свою рабочую станцию, если выключение не прервет технологический процесс и выполнение трудовых обязанностей.

Пользователи не имеют прав локального администратора на АРМ и не допускаются к конфигурированию ПК, инсталляции и деинсталляции программного обеспечения, если иное не определено их непосредственными трудовыми обязанностями.

Пользователям АРМ запрещено:

- открывать корпус системного блока и производить любую модификацию компонентов системного блока – извлекать, добавлять, заменять компоненты, менять положение переключателей и т.п., а также производить настройку оборудования АРМ (включая настройки BIOS);
- самостоятельно устанавливать, настраивать любые ОС и/или ПО (в том числе персональные межсетевые экраны и антивирусные средства, ограничивающие возможности обслуживания и мониторинга рабочих станций), а также удалять и изменять предустановленные настройки ОС и ПО;
- самостоятельно изменять сетевые настройки рабочих станций;
- открывать общий сетевой доступ к директориям и файлам на своей рабочей станции, а также общий сетевой доступ к любым устройствам, подключенным к рабочей станции, для других пользователей сети Общества;
- осуществлять действия, направленные на преодоление систем безопасности, получение НСД к ресурсам ИС, ухудшение рабочих характеристик ИС, перехват информации, циркулирующей в ИС.
- хранить, распространять и использовать на АРМ:
  - информацию развлекательного характера (игры, музыку, видеоролики, фильмы и т.п.);
  - ПО, установленное при нарушении требований Общества, в том числе хранить дистрибутивы;
  - любую другую информацию, которая не используется при выполнении трудовых обязанностей.

Работники, осуществляющие обслуживание АРМ в соответствии с их трудовыми обязанностями и зоной ответственности, имеют права на установку ПО, конфигурирование BIOS и ОС. Для выполнения указанных операций допускается подключение к АРМ пользователей в режиме удаленного рабочего стола (после разрешения пользователя).

Все действия по обслуживанию АРМ по запросу пользователей инициируются на основании заявок в УИТС.

Установка стороннего ПО на рабочие станции возможна только по согласованию с УИТС и УБ.

Инсталляция и эксплуатация ПО, правом использования которого Общество не обладает, запрещено.

3.2.2. Требования по использованию ноутбуков

Ноутбуки предназначены для работников Общества, выполнение трудовых обязанностей которых предполагает командировки и производственную необходимость вне стационарного рабочего места.

На ноутбук перед выдачей его работнику устанавливается специализированное ПО, выполняющее функции межсетевого экрана, настройки которого производятся централизованно, в том числе корпоративное антивирусное ПО с актуальными обновлениями на момент установки и дальнейшим периодическим автоматическим обновлением. Пользователь ноутбука не должен иметь возможности выключить или изменить настройки специализированного ПО.

Доступ в сеть Интернет и работа со съемными машинными носителями информации (далее – СМНИ) на ноутбуках вне информационной инфраструктуры Общества осуществляется с учетом ограничений, установленных пунктом 3.2.3 настоящей Политики и Инструкцией по регистрации съемных носителей информации.

3.2.3. Требования по использованию мобильных устройств

По умолчанию запрещено использование съемных носителей и устройств, подключение к АРМ и синхронизация телефонов и других мобильных устройств.

Подключение внешних устройств может быть разрешено только в случае служебной необходимости на основании согласованной с УБ заявкой, направленной руководителем структурного подразделения или руководством (директором, заместителем директора, главным инженером, заместителем главного инженера) филиала Общества, в которой обосновывается необходимость использования соответствующих устройств на конкретной рабочей станции определенным работником.

Допускается централизованное подключение заранее согласованных внешних устройств для определенной группы компьютеров с целью поддержки функционирования ИС или технологий.

Запись информации на внешние устройства в личных и иных непроизводственных целях запрещена.

3.2.4. Требования к использованию КЭП

При приеме на работу нового работника в рамках организации рабочего места пользователю предоставляется право пользования КЭП.

В рамках доступа к КЭП пользователям предоставляются следующие основные сервисы:

- создание почтового ящика пользователя и / или группы пользователей;
- почтовый обмен по почтовому адресу с другими пользователями КЭП и адресатами глобальной сети Интернет;
- возможность шифрованного обмена сообщениями внутри корпоративного сегмента КЭП;
- хранение входящей и исходящей корреспонденции в течение определенного срока со дня получения/формирования письма;
- доступ к адресной книге КЭП;
- проверка корреспонденции на наличие вредоносного ПО;
- защита почтового ящика от нежелательной корреспонденции (СПАМа).

Предоставление дополнительных сервисов и интеграция с другими корпоративными средствами электронных коммуникаций зависит от функционала, используемого для реализации КЭП ПО.

Право на использование КЭП прекращается по окончании действия трудового договора между работником и Обществом или в случае отсутствия служебной необходимости при изменении функционала работника.

Пользователь обязан использовать КЭП только для выполнения своих трудовых обязанностей. В связи с этим, информация в почтовом ящике является собственностью Общества и подлежит контролю.

Пользователю запрещается использовать сторонние сервисы электронной почты для исполнения трудовых обязанностей.

Запрещается использовать КЭП для пересылки и распространения:

- материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования;
- сведений для осуществления НСД к информационным ресурсам, для использования ПО с нарушением авторских прав и лицензионных соглашений, а также ссылок на вышеуказанную информацию;
- конфиденциальной информации[3];
- информации, содержание и направленность которой запрещены международным и российским законодательством, включая материалы,

[3] Информация ограниченного распространения и доступа, защита которой определена законодательством Российской Федерации, и / или локальными нормативными документами (актами) Общества.

носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.;

- информации, направленной на дискредитацию использования Вооруженных Сил Российской Федерации в целях защиты интересов Российской Федерации и ее граждан, поддержания международного мира и безопасности или исполнения государственными органами Российской Федерации своих полномочий в указанных целях.

Запрещается использовать электронный почтовый адрес КЭП для:

- ведения переписки в личных целях, не связанных с исполнением пользователем своих трудовых обязанностей;
- ведения экономической деятельности, кроме как в интересах Общества;
- пересылки любой информации на свой личный почтовый ящик;
- подписки на регулярное получение информационных материалов, не связанных с исполнением пользователем своих трудовых обязанностей;
- размещения его на общественных ресурсах глобальной сети Интернет, отличных от корпоративных, за исключением случаев регистрации на информационных ресурсах, связанных с профессиональной деятельностью;
- массовой рассылки информационных сообщений (свыше установленных ограничений);
- отправки сообщений, объем которых (включая вложения) превышает 20 Мб.

В целях минимизации потока нежелательной корреспонденции (СПАМа), а также корреспонденции, содержащей вирусы и другие вредоносные программы, ограничивается прием:

- писем, не прошедших антивирусную проверку;
- писем, не прошедших проверку системой антиспам;
- писем с отсутствующими или искаженными реквизитами отправителя;
- писем, объем которых (включая вложения) превышает 50 Мб для пересылки внутри Общества и 20 Мб для пересылки писем третьим лицам.

При выявлении попыток НСД к КЭП, необъяснимых сбоев в работе АРМ и в других случаях, указывающих на возможность умышленных действий извне, пользователь обязан незамедлительно сообщить непосредственному руководителю и УБ.

Пользователь несет ответственность за соблюдение установленных ограничений при использовании своего почтового ящика КЭП.

В случаях, когда нарушения порядка использования КЭП повлекли за собой НСД, несанкционированное копирование, передачу, модификацию, блокирование или уничтожение информации Общества, а также в случаях создания ситуаций, которые

потенциально могли бы привести к таким последствиям, проводится служебное расследование.

3.2.5. Требования по использованию сети Интернет

Ресурсы сети Интернет в Обществе должны использоваться для решения следующих задач:

- получения информации, необходимой для исполнения трудовых обязанностей, из размещенных в Интернете источников и ведения информационно-аналитической работы;
- предоставления уполномоченными работниками открытой информации о деятельности Общества;
- получения уполномоченными работниками и ИС Общества программных средств и обновлений к ним в рамках договоров по использованию и сопровождению программного обеспечения;
- осуществления обмена электронными почтовыми сообщениями, а также других видов электронной связи, основанных на технологиях сети Интернет, со сторонними организациями и физическими лицами в рамках исполнения трудовых обязанностей;
- организации каналов передачи данных для информационного обмена со сторонними организациями, филиалами Общества и удаленного доступа пользователей к информационным ресурсам корпоративной сети в рамках исполнения трудовых обязанностей и договорных обязательств Общества.

Доступ к информационным ресурсам сети Интернет, а также удаленный доступ к ИС и сервисам в рамках корпоративной сети должен предоставляться централизованно. Организация отдельного доступа к сети Интернет для дочерних организаций, рабочие места пользователей которых подключены к КСПД Общества, запрещена.

Все информационные потоки взаимодействия с сетью Интернет должны проходить через Интернет-шлюз, который организован как совокупность аппаратно-программных средств, включающая в себя:

- систему межсетевого экранирования;
- подсистему детектирования и противодействия сетевым атакам;
- подсистему организации виртуальных частных сетей (VPN);
- систему контентной фильтрации;
- прокси-сервер с функцией протоколирования запросов.

Архитектура системы межсетевого экранирования должна обеспечивать гарантированную доступность необходимых ресурсов сети Интернет и защиту от внешнего несанкционированного воздействия на инфраструктуру и информационные ресурсы корпоративной сети Общества.

Доступ в сеть Интернет предоставляется в минимально необходимом объеме только для выполнения работниками своих служебных обязанностей.

Все удаленные подключения к ресурсам корпоративной сети с использованием сети Интернет должны быть организованы путем создания защищенных каналов.

Организация внешних подключений к ресурсам корпоративной сети в обход Интернет-шлюза запрещена.

Система контентной фильтрации должна осуществлять ограничение доступа к потенциально опасным узлам сети Интернет и анализ входящих Интернет-потоков на наличие вредоносного программного кода.

Списки блокируемых узлов и сигнатур вредоносного ПО должны регулярно обновляться. Дополнительные правила блокирования узлов сети Интернет вводятся по запросу вышестоящих организаций и УБ

На всех клиентских компьютерах и серверах корпоративной сети Общества, имеющих доступ к ресурсам сети Интернет, должны быть установлены средства защиты от сетевых атак и вредоносного кода. Порядок реализации указанных средств регламентируется п. 3.3 настоящей Политики.

УБ должно выполнять постоянный контроль посещаемых веб-сайтов на основании записей, автоматически регистрируемых в журналах серверов и рабочих станций.

УБ и УИТС имеют право ограничивать доступ к определенным ресурсам Интернет путем формирования и дополнения списка сайтов, запрещенных для посещения работникам Общества.

Все обращения пользователей через сервера активного оборудования к ресурсам сети Интернет должны централизованно протоколироваться, в том числе посредством функции прокси-сервера в составе Интернет-шлюза.

На Интернет-шлюзе должны вестись журналы событий ИБ системы межсетевого экранирования, подсистем детектирования и противодействия сетевым атакам, системы контентной фильтрации и организации защищенных каналов доступа к корпоративной сети.

Протоколы Интернет-активности пользователей и журналы событий ИБ подлежат хранению не менее 1 (одного) года.

Указанные журналы должны использоваться УБ при расследовании инцидентов ИБ и анализе эффективности принимаемых мер защиты.

При работе с ресурсами сети Интернет из КСПД пользователям запрещено:

- использовать ресурсы сети Интернет, не имеющие отношения к выполнению трудовых обязанностей;
- подключаться к сети Интернет с помощью модемов, а также с помощью мобильных устройств (телефон, ноутбук и т.д.);
- модифицировать конфигурацию ПО, используемого для доступа к сети Интернет;
- регистрироваться на сайтах с идентификатором и паролем, используемыми при работе в ИС;
- сохранять пароли ИС в web-браузерах;

- пересылать информацию ограниченного распространения и доступа. Если пересылка необходима в рамках исполнения трудовых обязанностей, то пересылку необходимо осуществлять способом, обеспечивающим конфиденциальность передаваемой информации;
- несанкционированно загружать, устанавливать и запускать ПО и средства разработки из сети Интернет;
- использовать средства интерактивного общения (мгновенного обмена сообщениями). В случае производственной необходимости разрешение на их использование выдается УИТС;
- использовать публичные системы обмена файлами. В случае производственной необходимости разрешение на их использование выдается УБ. В данном случае владелец информации обязан письменно подтвердить, что утечка размещаемой информации не нанесет ущерба экономическим и репутационным интересам Общества. Использование как для передачи, так и для скачивания или хранения информации систем обмена файлами, расположенными за территорией Российской Федерации, категорически запрещено;
- несанкционированно использовать ресурсы сети Интернет, организовывать хакерские атаки, а также осуществлять другие действия, запрещенные действующим законодательством Российской Федерации.
- посещать ресурсы сети Интернет, содержащие материалы противозаконного, экстремистского или неэтичного характера, использовать доступ в сеть Интернет в развлекательных целях;
- использовать ресурсы сети Интернет для несанкционированной передачи (выгрузки) или получения (загрузки) материалов, защищенных авторским правом и конфиденциальной информации.

Руководитель структурного подразделения Общества несет ответственность за соответствие запрашиваемых подчиненными работниками средств и ресурсов сети Интернет их трудовым обязанностям, задачам структурного подразделения и интересам Общества.

Пользователь несет ответственность за корректное пользование ресурсами сети Интернет. В случае нарушения вышеуказанных правил доступ пользователя к ресурсам сети Интернет может быть заблокирован с обязательным уведомлением об этом непосредственного руководителя.

В тех случаях, когда нарушение порядка использования сети Интернет повлекло за собой НСД, несанкционированное копирование, модификацию, блокирование или уничтожение информации Общества, а также в случаях создания ситуаций, которые потенциально могли бы привести к таким последствиям, проводится служебное расследование.

В Обществе устанавливаются различные профили доступа пользователей к ресурсам сети Интернет, которыми определяется перечень разрешенных и заблокированных

ресурсов. Для отдельных профилей устанавливается режим уведомлений о рисках доступа к потенциально опасным сайтам, а также к сайтам определенных категорий.

Профили доступа:

- Минимальный профиль (Minimum) – только разрешенные сайты («белый список»). Запрещено скачивание файлов и использование клиентов мгновенных сообщений.
- Привилегированный профиль – типовой профиль без ограничения доступа к сети Интернет.
- Для технических специалистов (Technical) – привилегированный профиль с разрешением закачки файлов, доступом по FTP и т.п., предназначен для ИТ-администраторов.

3.2.6. Требования ИБ при замене АРМ или передаче в ремонт

Перед передачей АРМ в ремонт сторонней организации ответственные работники обязаны провести удаление информации на его дисках либо произвести демонтаж устройств хранения в периметре Общества.

При замене АРМ, на котором содержится конфиденциальная информация, его передаче на склад или в другое структурное подразделение пользователь, являющийся документально закрепленным за ПК, должен совместно с ответственным работником произвести гарантированное удаление конфиденциальной информации.

При передаче жесткого диска в стороннюю организацию для восстановления данных с этой организацией заключается соглашение о конфиденциальности (неразглашении).

3.2.7. Действия в нестандартных ситуациях

Пользователи ИС обязаны немедленно ставить в известность своего непосредственного руководителя, УБ и УИТС в случае возникновения или возможного возникновения следующих событий:

- разглашения учетных данных;
- потери, кражи средств аутентификации;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств рабочей станции;
- фактов совершения попыток НСД к ресурсам ИС;
- фактов потери, кражи компьютеров или носителей информации, особенно если они содержали информацию ограниченного доступа;
- заражение ПК пользователя вредоносным ПО;
- сбоев в работе средств защиты информации;
- в любых других случаях если, по мнению пользователя, возникают риски нарушения ИБ.

3.3. Требования к обеспечению антивирусной защиты

Данный раздел Политики направлен на обеспечение комплексной защищенности от вирусных угроз, предусматривающей применение как организационных, так и программно-технических методов защиты.

Целями реализации антивирусной защиты являются:

- обеспечение защиты информации и ИС от угроз вредоносного кода;
- утверждение требований к организации функционирования САЗ;
- определение объектов, подлежащих антивирусной защите.

Любые исключения, связанные с отменой положений настоящего раздела Политики, в ИС необходимо согласовать с УБ и УИТС.

3.3.1. Требования к САЗ

В качестве САЗ необходимо использовать только лицензионное ПО.

Установка и настройка антивирусного ПО должна быть произведена в процессе инсталляции ОС на АРМ Общества. В Обществе должны быть назначены ответственные работники за установку и контроль наличия корректно функционирующего антивирусного ПО в ходе настройки и дальнейшего сопровождения АРМ.

В Обществе должен быть реализован принцип эшелонированной защиты, когда на разных уровнях применяются средства антивирусной защиты различных производителей. Допустимо использование на одном из эшелонов защиты антивирусного ПО иностранных производителей.

Антивирусное ПО должно быть установлено на всех серверах с различными ролями, при этом специализация САЗ должна соответствовать назначению сервера.

Антивирусная защита всех почтовых серверов Общества, обрабатывающих почтовые сообщения, должна осуществляться специализированным антивирусным ПО для почтовых серверов. В рамках данной защиты должна проводиться проверка всех входящих и исходящих почтовых сообщений на наличие вирусов во вложениях (включая файлы архивов и исполняемые файлы).

Для поддержания и развития уровня защиты должно осуществляться планирование работ по масштабированию системы антивирусной защиты с заблаговременным доведением информации о данной необходимости до руководства Общества.

3.3.2. Требования к конфигурации средств САЗ

Централизованная САЗ должна предусматривать использование средств антивирусной защиты различных производителей на АРМ и серверах.

Полная антивирусная проверка всех рабочих станций и серверов должна выполняться с периодичностью раз в неделю, с учетом рабочих часов пользователей и времени нагрузки на АРМ и сервера.

Назначенные администраторы САЗ несут ответственность за обеспечение функционирования антивирусного ПО.

Локальная консоль управления антивирусного ПО на АРМ должна быть заблокирована паролем учетной записи администратора САЗ для предотвращения

изменения локальной политики антивирусной защиты. Пароль учетной записи администратора САЗ должен удовлетворять требованиям пункта 3.1.2.1 настоящей Политики.

Проверка наличия новых сигнатур баз данных вирусов должна осуществляться центральным сервером САЗ каждые 15 (пятнадцать) минут по сети Интернет с официального ресурса производителя средства антивирусной защиты.

В Обществе должна осуществляться проверка наличия новых версий антивирусного ПО на официальном ресурсе производителя средства антивирусной защиты не реже одного раза в месяц.

Обновление сигнатур баз данных вирусов антивирусного ПО должно выполняться в течение дня центральным сервером САЗ.

Обновление новых версий антивирусного ПО должно выполняться только после успешной проверки совместимости новых версий на тестовых АРМ и серверах.

Установка новых видов ПО, новых версий и обновлений уже установленного ПО на АРМ должно производиться только после выполнения предварительной проверки данного ПО на отсутствие встроенного вредоносного кода.

Сервер администрирования САЗ должен регистрировать все события, связанные с работой САЗ и действиями всех пользователей данной системы.

Журналы регистрации, содержащие все события, связанные с работой САЗ и действиями всех пользователей данной системы за последние 2 (два) месяца, должны быть доступны в режиме оперативного доступа.

3.3.3. Требования по контролю функционирования САЗ

В Обществе должны быть организованы:

- регулярный мониторинг уровня антивирусной защищенности компьютеров Общества;
- регулярный мониторинг актуальности состояния САЗ;
- проверки соответствия конфигурации САЗ требованиям настоящей Политики.

Для своевременного реагирования на инциденты ИБ сервер администрирования САЗ должен автоматически отправлять уведомления по КЭП администратору САЗ и ответственным за обеспечение ИБ в Обществе о критических событиях, определяемых в процессе поддержки и мониторинга САЗ.

При возникновении инцидентов, связанных с обеспечением антивирусной защищенности Обществе, должны быть организованы мероприятия согласно локальным нормативным документам (актам) Общества, регламентирующим порядок обнаружения и реагирования на инциденты ИБ.

3.4. Требования по защите сетевого периметра

Настоящий раздел Политики определяет верхнеуровневую модель сетевых зон безопасности и определяет принципы контроля доступа к сетевым зонам безопасности.

3.4.1. Меры по обеспечению безопасности

Меры по обеспечению ИБ сетевого периметра Общества должны предусматривать разделение ИС на однотипные ресурсы по категориям функциональных возможностей, для чего составляется перечень и проводится классификация входящих в ИС информационных ресурсов.

Результаты классификации входящих в ИС информационных ресурсов должны обеспечивать назначение ИС обобщенной категории по каждому из признаков классификации. В зависимости от уровня обобщенной категории ИС, их элементы распределяются по «зонам доверия», которые представляют собой сетевые зоны безопасности.

Сетевая инфраструктура Общества должна обеспечивать защищенный обмен данными между ИД Общества, его филиалами, подконтрольными и сторонними организациями, сетью Интернет и другими сегментами сети. Защита и контроль данных должны обеспечиваться посредством технических средств защиты на сетевом уровне (межсетевые экраны и иные системы) и на уровне приложений (сетевой экран приложений).

С целью защиты и контроля данных необходимо выделять в отдельный контур безопасности корпоративные информационные ресурсы, автоматизированные системы управления технологическими процессами, ИС персональных данных и другие ИС, обрабатывающие информацию, требования по защите которой определены законодательством Российской Федерации.

3.4.2. Требования по построению эшелонированной защиты

При построении сети необходимо соблюдать принцип эшелонированной защиты, который обеспечивает безопасность информационных ресурсов посредством внедрения многоуровневых защитных барьеров в каждом сегменте.

Посредством эшелонированной защиты сетевой архитектуры достигаются цели:

- усиление безопасности доступа к объектам защиты информации посредством внедрения различных средств защиты на разных уровнях;
- предотвращение сбоев в периметре одного уровня или на одном техническом объекте, которые могут представлять угрозу для объекта ИБ.

3.4.3. Требования по сегментации и фильтрации

Архитектура сети Общества должна обеспечивать сегментацию – разделение компонентов сети по степени защиты и выделение компонентов, имеющих одинаковую степень защиты, в отдельные сетевые сегменты. При этом сегментация сети должна обеспечивать:

- предоставление доступа только разрешенным пользователям Общества;
- снижение рисков утечки информации;
- предотвращение незаконных проникновений из одной сетевой зоны безопасности в другую;

- уменьшение вероятности проникновения или распространения компьютерных вирусов и вредоносных программ;
- уменьшение вероятности НСД к критическим ИС или конфиденциальным данным;
- упрощение обнаружения несанкционированного воздействия на информацию (утечка информации и т. д.) за счет создания необходимых контрольных точек для систем обнаружения / предотвращения вторжений.

3.4.4. Требования к зонам безопасности

Должны быть определены соответствующие зоны безопасности, включая доверенные, условно-доверенные и недоверенные зоны. Между зонами должны быть настроены соответствующие правила фильтрации.

Связь зон безопасности должна обеспечиваться посредством межсетевых экранов, которые предусматривают возможность учета различных параметров фильтрации трафика: протоколы, IP адреса, разрешенные маршруты и сегменты, время доступа (если применимо) и т.д.

Взаимодействие зон должно быть основано на соблюдении следующих принципов:

- взаимодействие Недоверенной и Доверенной зон должно происходить через Условно-доверенную зону с контролем информационных потоков и доступа, при этом должен быть обеспечен запрет возможности прямой передачи каких-либо транзакций и иной информации из Недоверенной зоны в Доверенную;
- сетевые коммуникации между элементами ИС, принадлежащими двум отличным друг от друга зонам, должна фильтроваться по набору протоколов зоны, в которой размещена целевая ИС.

Все изменения настроек сетевого оборудования должны быть согласованы с УБ.

3.4.5. Требования по управлению доступом

Предоставление доступа к сетевым зонам безопасности Общества должно осуществляться при выполнении следующих требований:

- наличие обоснования на предоставляемые права доступа;
- наличие разрешения на предоставляемые права доступа;
- регулярный пересмотр и отзыв избыточных прав доступа в рамках периодической процедуры пересмотра предоставленных прав доступа;
- автоматизация предоставления доступов.

Соблюдение этих требований предполагает:

- управление логическим доступом к различным сетевым сегментам (включает идентификацию подключаемых устройств, проверку их подлинности, подтверждение и авторизацию);
- разбиение вычислительных сетей на сетевые зоны безопасности (каждая из которых находится в ведении определенных работников и имеет описание схем физических и логических взаимосвязей с указанием механизмов контроля потоков данных на границах таких зон).

3.4.6. Требования по контролю за сетевой безопасностью

Сетевая безопасность в Обществе должна обеспечиваться и контролироваться в соответствии с установленными в Обществе требованиями к уровням доступности и конфиденциальности потоков, систем и процессов, используемых в сети. Меры по обеспечению безопасности информации в сети должны соответствовать типу сети.

Для предотвращения инцидентов информационной безопасности и уменьшения их количества необходимо принятие исчерпывающего перечня мер, а именно:

- регулярный мониторинг и анализ сетевого трафика;
- регулярные проверки правил сетевых экранов и контроль их изменений;
- регулярная оценка уязвимостей сетевых экранов и приложений критичных систем посредством внутреннего и внешнего (в случае необходимости) аудита.

3.5. Требования по контролю защищенности

Настоящий раздел Политики определяет требования, порядок подготовки и проведения контроля защищенности ИС в Обществе.

На всех объектах ИС администраторы ИС должны контролировать установку обновлений на периодической основе.

Обновления безопасности предназначены для устранения уязвимостей на элементах ИС и ошибок в их работе, выявленных в процессе эксплуатации. Своевременная установка обновлений безопасности позволяет предотвратить снижение уровня защищенности ИС и обеспечить защиту от различных угроз информационной безопасности.

На все объекты ИС должны быть установлены последние обновления безопасности, выпущенные производителем[4].

Обновления должны устанавливаться в автоматическом режиме при условии наличия актуальных резервных копий объектов ИС, на которые в автоматическом режиме ставятся обновления, а также при условии отсутствия явных нареканий на устанавливаемые обновления, выявленных в результате анализа источников информации о выпущенных обновлениях и уязвимостях сопровождаемых систем (сайты и новостные рассылки производителей оборудования и разработчиков программного обеспечения, специализированные базы данных уязвимостей, Интернет-ресурсы по ИБ).

В Обществе должны быть разработаны документы, содержащие общепринятые настройки безопасности для существующих элементов ИТ-инфраструктуры (стандарты конфигурирования), которые должны применяться в обязательном порядке для всех вновь вводимых в эксплуатацию ИС. Стандарты конфигурирования должны включать правила обновлений ИС.

Выявление уязвимостей должно осуществляться посредством анализа информации о возможных уязвимостях и выпущенных обновлениях, а также путем проведения технических проверок (проведение контроля защищенности ИС и тестирование на проникновение).

[4] С учетом указаний ФСТЭК России от 10.05.2022 №240/84/1224

Основными источниками информации о возможных уязвимостях и имеющихся обновлениях являются:

- Национальный координационный центр по компьютерным инцидентам;
- Федеральная служба технического и экспортного контроля России;
- Ведомственный центр обнаружения, предупреждения и ликвидации последствий компьютерных атак Минэнерго России;
- КЦОПЛ;
- сайты и новостные рассылки производителей оборудования и разработчиков программного обеспечения Общества;
- специализированные базы данных уязвимостей;
- интернет-ресурсы по ИБ;
- специализированные электронные почтовые рассылки по ИБ;
- другие уведомления об уязвимостях, обновлениях или угрозах ИБ.

При организации контроля защищенности ИС применяется система сканирования уязвимостей и средства оценки защищенности.

Одним из элементов контроля защищенности ИС является система обеспечения контроля целостности компонентов ИС, указанная в пункте 3.5.3 настоящей Политики.

3.5.1. Проведение инструментального контроля защищенности ИС

Инструментальный анализ защищенности ИС проводится на регулярной основе в автоматическом режиме с помощью программно-аппаратных средств.

Анализ защищенности ИС может являться составной частью комплексной проверки состояния ИБ или представлять собой самостоятельную инструментальную проверку (тестирование) ИС.

По результатам инструментального анализа защищенности формируется отчет, содержащий информацию о времени начала и завершения тестирования, список IP-адресов протестированных компонентов ИС, информацию о выявленных уязвимостях и их критичности, а также иные консолидированные сведения.

Руководствуясь результатами инструментального анализа защищенности, проводится устранение выявленных недостатков и уязвимостей. При необходимости, установленным порядком проводится изменение настроек политики безопасности, обновление ПО, а также изменение соответствующих стандартов конфигурирования.

После устранения обнаруженных уязвимостей должен проводиться повторный инструментальный анализ защищенности для фиксирования положительного результата.

3.5.2. Проведение тестирования на проникновение

Тестирование на проникновение осуществляется не реже одного раза в год или после внесения существенных изменений в ИС.

Тестирование на проникновение проводится уполномоченными работниками Общества либо с привлечением квалифицированной третьей стороны в соответствии с методологией, указываемой в соответствующем договоре.

Тестирование на проникновение осуществляется как из внешней (сети Интернет), так и из внутренней сети Общества (пользовательского сегмента сети).

Проведение тестирования на проникновение может приводить к нарушению работы ИС, в связи с чем должно осуществляться под непосредственным наблюдением администраторов тестируемой ИС.

3.5.3. Требования по реализации контроля целостности

В рамках реализации подсистемы обеспечения целостности в Обществе должно быть обеспечено:

- целостность программных средств;
- неизменность программной среды;
- проведение периодического тестирования системы защиты информации;
- наличие средств восстановления программных средств и среды.

Проверка обеспечения целостности программных средств и проверка неизменности программной среды должна производиться при помощи специализированных средств.

Проверка проведения периодического тестирования СЗИ осуществляется путем:

- контроля наличия организационно-распорядительной документации, определяющей периодичность и порядок тестирования всех функций СЗИ;
- проверки возможности периодического тестирования СЗИ в ходе анализа применяемых разработчиком средств контроля целостности компонентов системного ПО, реализующих функций СЗИ, и наборов данных, используемых этими средствами.

Средствами восстановления программных средств в ИС являются дистрибутивы (инсталляционные файлы) с системным и прикладным ПО. Копии дистрибутивов должны хранится отдельно для обеспечения возможной полной замены (переустановки) ПО в случае отказов (сбоев) или нарушений в работе технических средств ИС. Автоматическое оперативное восстановление функций программных средств при сбоях проверяется путем моделирования сбойных ситуаций и последующей проверки (тестирования) функций программного средства.

3.6. Требования ИБ при подключении дочерних организаций к информационным ресурсам Общества

Подключение дочерних организаций к информационным ресурсам Общества осуществляется в соответствии с Технической политикой ПАО «РусГидро» в области информационных технологий и требованиями настоящей Политики.

3.6.1. Минимально необходимые требования ИБ

Для подключения пользователей дочерних организаций к информационным ресурсам Общества необходимо соблюдение следующих условий:

- в дочерней организации развернута централизованная система антивирусной защиты, удовлетворяющая требованиям пункта 3.3 настоящей Политики;

- в дочерней организации развернута система обнаружения / предотвращения вторжений корпоративного сегмента с регулярно актуализируемыми сигнатурами.

3.6.2. Контроль выполнения требований ИБ

Контроль за соблюдением минимально необходимых требований ИБ осуществляет УИТС и УБ.

Подключение дочерних организаций к технической инфраструктуре КЦОПЛ ПАО «РусГидро» и передача данных о состоянии средств защиты информации в КЦОПЛ регулируется требованиями КЦОПЛ ПАО «РусГидро».

4. Порядок сопровождения ИС, АСУ и ИТС

4.1. Обеспечение ИБ на стадиях жизненного цикла ИС, АСУ и ИТС

ИБ ИС, АСУ и ИТС обеспечивается на всех стадиях жизненного цикла (ЖЦ) ИС, АСУ и ИТС с учетом всех сторон, вовлеченных в процессы ЖЦ (включая разработчиков, заказчиков, поставщиков товаров, работ, услуг).

Разработка технических заданий, проектирование, создание, тестирование и приемка ИС, АСУ, ИКС должны осуществляться по согласованию с УБ.

Порядок разработки и внедрения ИС, АСУ и ИТС должен быть регламентирован и контролироваться.

При разработке ИС, АСУ и ИТС необходимо использовать системное и прикладное ПО, входящее в единый реестр российских программ для электронных вычислительных машин и баз данных и / или Реестр разрешенного к использованию ПО Общества.

При разработке ИС, АСУ и ИТС необходимо придерживаться требований и методических указаний, определенных стандартами, входящими в группу ГОСТ 34.ххх Стандарты «Информационная технология».

При проектировании значимых объектов критической информационной инфраструктуры необходимо соблюдать требования и методические указания стандартов по безопасной разработке кода «ГОСТ Р 56939-2016. Национальный стандарт Российской Федерации. Защита информации. Разработка безопасного программного обеспечения. Общие требования».

ИС, АСУ и ИТС должны вводиться в эксплуатацию в соответствии с Положением о процессе приемки ИС в эксплуатацию. Ввод в действие, эксплуатация и снятие с эксплуатации ИС, АСУ и ИТС в части вопросов ИБ должны осуществляться при участии УИБ.

На стадиях, связанных с разработкой ИС, АСУ и ИТС (определение и анализ требований, архитектурное проектирование, реализация, интеграция и верификация, поставка, ввод в действие), разработчиком должна быть обеспечена защита от угроз:

- неверной формулировки требований к ИС, АСУ и ИТС;
- реализации неверных проектных решений;
- возникновения дефектов на уровне архитектурных решений, в том числе по вине разработчиков;
- внесения разработчиком недокументированных возможностей в ИС, АСУ и ИТС;
- неадекватной (неполной, противоречивой, некорректной и пр.) реализации требований к ИС, АСУ и ИТС;
- разработки некачественной документации в части обеспечения требований ИБ;
- сборки ИС, АСУ и ИТС разработчиком/производителем с нарушением требований, приводящей к появлению недокументированных возможностей в ИС либо к неадекватной реализации требований;
- неверного конфигурирования ИС, АСУ и ИТС;
- приемки ИС, АСУ и ИТС, не отвечающей требованиям ИБ;

- внесения недокументированных возможностей в ИС, АСУ и ИТС в процессе проведения приемочных испытаний (в целях фальсификации результатов функциональных тестов и тестов ИБ).

Привлекаемые для разработки и/или производства средств и систем защиты ИС, АСУ и ИТС на договорной основе специализированные организации должны иметь лицензии на данный вид деятельности в соответствии с законодательством Российской Федерации и соответствовать требованиям к поставщикам и производителям, зафиксированным в Технической политике в области информационных технологий ПАО «РусГидро».

При приобретении готовых ИС, АСУ и ИТС и их компонентов разработчиком должна быть предоставлена:

- документация, содержащая описание защитных мер, предпринятых разработчиком в отношении угроз ИБ;
- документация, содержащая описание защитных мер, предпринятых разработчиком ИС и их компонентов относительно безопасности разработки, безопасности поставки и эксплуатации, поддержки жизненного цикла, включая описание модели жизненного цикла, модели угроз и нарушителя, оценки уязвимости (данная документация может быть представлена в рамках декларации о соответствии или быть результатом оценки соответствия изделия, проведенной в рамках соответствующей системы оценки).

На стадии эксплуатации ИС должны быть минимизированы следующие риски:

- умышленное несанкционированное раскрытие, модификация или уничтожение информации;
- неумышленная модификация или уничтожение информации;
- недоставка или ошибочная доставка информации;
- отказ в обслуживании или ухудшение обслуживания.

На стадии сопровождения ИС, АСУ и ИТС должна быть обеспечена защита от угроз:

- внесения изменений в ИС, АСУ и ИТС, приводящих к нарушению ее функциональности либо к появлению недокументированных возможностей;
- невнесения разработчиком/поставщиком изменений, необходимых для поддержки правильного функционирования и правильного состояния ИС, АСУ и ИТС.

На стадии снятия с эксплуатации ИС, АСУ и ИТС должно быть обеспечено удаление информации, несанкционированное использование которой может нанести ущерб Обществу, и информации, используемой средствами обеспечения ИБ, из постоянной памяти ИС, АСУ и ИТС или с внешних носителей.

Требования ИБ должны включаться во все договоры на проведение работ или оказание услуг на всех стадиях жизненного цикла ИС, АСУ и ИТС.

4.2. Профилактика нарушений Политики

Под профилактикой нарушений настоящей Политики понимается проведение регламентных работ по защите информации, предупреждение возможных нарушений ИБ в ИС и проведение разъяснительной работы по ИБ среди пользователей ИС.

Проведение в ИС регламентных работ по защите информации предполагает выполнение процедур контрольного тестирования (проверки) функций СЗИ, что гарантирует ее работоспособность с точностью до периода тестирования. Контрольное тестирование функций СЗИ может быть частичным или полным и должно проводиться с установленной в ИС степенью периодичности.

Задача предупреждения в ИС возможных нарушений ИБ должна решаться по мере наступления следующих событий:

- включение в состав ИС новых программных и технических средств (новых рабочих станций, серверного или коммуникационного оборудования и др.) при условии появления уязвимых мест в СЗИ ИС;
- изменение конфигурации программных и технических средств ИС (изменение конфигурации программного обеспечения рабочих станций, серверного или коммуникационного оборудования и др.) при условии появления уязвимых мест в СЗИ ИС;
- при появлении сведений о выявленных уязвимостях в составе операционных систем и/или программного обеспечения технических средств, используемых в ИС.

УБ (при необходимости, при помощи сторонней организации, специализирующейся в области ИБ):

- собирает и анализирует информацию о выявленных уязвимых местах в составе операционных систем и/или программного обеспечения относительно ИС (источниками подобного рода сведений могут служить официальные издания и публикации различных компаний, общественных объединений и других организаций, специализирующихся в области защиты информации);
- организовывает периодическую проверку СЗИ ИС путем моделирования возможных попыток осуществления НСД к защищаемым информационным ресурсам (в случае необходимости УБ может выполнять эту работу совместно с УИТС).

Для решения задач контроля защищенности ИС используются инструментальные средства для тестирования реализованных в составе КСУИБ средств и функций защиты, указанных в предыдущих разделах настоящей Политики.

Плановая разъяснительная работа по правилам настоящей Политики, а также инструктаж работников Общества по соблюдению требований локальных нормативных документов (актов) по ИБ, принятых в Обществе, проводятся ежегодно работниками УИБ.

Внеплановая разъяснительная работа и инструктаж проводятся при пересмотре настоящей Политики, а также при возникновении инцидента нарушения правил настоящей Политики.

Прием на работу новых работников Общества должен сопровождаться ознакомлением их с правилами настоящей Политики.

4.3. Ликвидация последствий нарушения Политики

УБ, используя данные, полученные в результате применения инструментальных средств контроля (мониторинга) безопасности информации ИС, должно своевременно обнаруживать нарушения ИБ, факты осуществления НСД к защищаемым информационным ресурсам ИС и предпринимать меры по их локализации и устранению.

В случае обнаружения факта нарушения ИБ или осуществления НСД к защищаемым информационным ресурсам Общества заинтересованному пользователю или работнику, ответственному за эксплуатацию ИС, необходимо незамедлительно уведомить работников УБ и УИТС и далее следовать их указаниям.

После устранения инцидента необходимо составить акт о факте нарушения и принятых мерах по восстановлению работоспособности ИС.

4.4. Ответственность за нарушение Политики

Ответственность за выполнение правил Политики несет каждый работник Общества в рамках своих трудовых обязанностей и полномочий.

На основании статьи 192 Трудового кодекса Российской Федерации работники, нарушающие требования настоящей Политики, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы.

За прямой действительный ущерб, причиненный Обществу в результате нарушения ими правил настоящей Политики, работники Общества несут материальную ответственность в соответствии со статьей 238 Трудового кодекса Российской Федерации).

За умышленное причинение ущерба, а также за разглашение сведений, составляющих охраняемую законом тайну (коммерческую или иную), работники Общества несут материальную ответственность в соответствии со статьей 243 Трудового кодекса Российской Федерации.

За неправомерный доступ к компьютерной информации, создание, использование или распространение вредоносных программ, а также нарушение правил эксплуатации ИС, следствием которых явилось нарушение работы ИС, уничтожение, блокирование или модификация защищаемой Обществом информации, работники Общества несут ответственность в соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации.

За причинение или допущение вреда критической информационной инфраструктуре Общества, в том числе в связи с нарушением правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, работники Общества несут ответственность в соответствии со статьей 274.1 Уголовного кодекса Российской Федерации.

5. Внедрение

Настоящая Политика изучается руководителями и сотрудниками структурных подразделений ИД и филиалов самостоятельно

6. Внесение изменений

Внесение изменений в настоящую Политику осуществляется УИТС в соответствии с СТО «Управление внутренней документацией интегрированной системы менеджмента»

7. Отмена и изъятие

Отмену действия и изъятие из обращения настоящей Политики осуществляется УИТС в соответствии с СТО «Управление внутренней документацией интегрированной системы менеджмента»

8. Рассылка и хранение

Контрольный экземпляр настоящего Регламента хранится в УИТС. Электронная копия контрольного экземпляра размещается в единой электронной базе данных ВНД ИСМ на сервере Общества

Лист регистрации изменений

1	Изменение
	Основание
	Текст изменения
	Лицо внесшее изменение/дата
2	

Лист ознакомления

NN	Должность	ФИО	подпись	дата