Приложение 1
к приказу АО «УК ГидроОГК»
от 30.08.2024 № 1п-65

Политика
информационной безопасности АО «УК ГидроОГК»

Содержание

Принятые обозначения и сокращения 3
1 Общие положения 4
1.1 Введение 4
1.2 Цели 4
1.3 Задачи 4
1.4 Область действия 4
1.5 Порядок утверждения и внесения изменений 4
2. Требования к организации управления и контроля доступа к информационным ресурсам 5
2.1. Порядок предоставления работникам Общества доступа к ИС 5
2.2. Парольная политика 6
2.2.1 Общие требования к паролям и парольной защите. 6
2.2.2. Требования по организации паролтной защиты 7
2.2.3 Порядок отмены и изменения прав доступа пользователей к информационным ресурсам 7
2.2.4 Предоставление удаленного доступа 8
2.3. Обеспечение ИБ при использовании АРМ и информационных ресурсов 9
2.3.1. Требования по использованию АРМ 10
2.3.2 Требования по использованию ноутбуков 11
2.3.3 Требования по использованию мобильных устройств 12
2.3.4 Требования к использованию КЭП 12
2.3.5 Требования по использованию сети Интернет 14
2.3.6 Требования ИБ при замене АРМ или передаче в ремонт 16
2.3.7 Действия в нестандартных ситуациях 17
2.4 Требования к обеспечению антивирусной защиты 17
2.4.1 Требования к САЗ 17
2.5.Контроль выполнения требований ИБ 18
2.6. Профилактика нарушений Политики 18
2.7. Ответственность за нарушение Политики 18

Принятые обозначения и сокращения

АРМ	Автоматизированное рабочее место
ДИТ	Департамент информационных технологий и цифрового развития
ИБ	Информационная безопасность
ИС	Информационные системы Общества
КТ	Коммерческая тайна
КСПД	Корпоративная сеть передачи данных
КЦОПЛ	Корпоративный центр обнаружения, предупреждения и ликвидации последствий компьютерных атак ПАО «РусГидро»
КЭП	Корпоративная электронная почта
ЛВС	Локальная вычислительная сеть
ЛНД(А)	Локальный нормативный документ (акт)
НСД	Несанкционированный доступ
Общество	АО «УК ГидроОГК»
ОС	Операционная система
ПК	Персональный компьютер
ПО	Программное обеспечение
САЗ	Система антивирусной защиты
СМНИ	Съемный машинный носитель информации
СПП	Служба технической поддержки пользователей
УКБ	Управление кибербезопасности ДИТ
DLP	Предотвращение утечки данных (Data Leakage Prevention)

1 Общие положения

1.1 Введение.

Политика информационной безопасности АО «УК ГидроОГК» (далее – Общество) (далее – Политика) описывает правила ИБ, обеспечения защиты информации, в том числе ограниченного распространения информации и доступа к информации, 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.

Задачей настоящей Политики является защита информации Общества.

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 контрагентов Общества;
- 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 ЛНД(А) Общества, а также в договорах, заключаемых Обществом с контрагентами.

Использование и организация защиты сведений, составляющих государственную тайну, регулируется отдельными ЛНД(А) Общества.

1.5 Порядок утверждения и внесения изменений.

Утверждение настоящей Политики и внесение в нее изменений осуществляются на основании ЛНД(А) Общества.

Ответственным за актуализацию настоящей Политики является Заместитель генерального директора Общества по безопасности.

2. 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 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.

2.1. Порядок предоставления работникам Общества доступа к ИС.

Доступ к ИС предоставляется:

- работникам Общества;
- контрагентам по договорам гражданско-правового характера (в том числе, по договору аутсорсинга).

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 начальный пароль, который должен быть изменен пользователем после первого

входа в систему и отвечать требованиям пункта 2.2. настоящей Политики. 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 СПП на основании заявки, подписанной руководителем структурного подразделения Общества. Доступ предоставляется с соблюдением принципов разумной достаточности и минимальной необходимости после согласования с УКБ ПАО «РусГидро».

Руководители структурных подразделений Общества несут ответственность за предоставление их подчиненным работникам доступа к ИС в строгом соответствии с их трудовыми обязанностями.

2.2. Парольная политика.

2.2.1. Общие требования к паролям и парольной защите.

В целях контроля использования ИС и сервисов корпоративной сети Общества доступ разрешается только после прохождения пользователем процедуры идентификации.

Для каждого легального субъекта доступа к объектам ИС должен быть установлен 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.

К паролям доступа в Обществе предъявляются следующие требования:

- длина пароля должна составлять не менее 12 (двенадцати) 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.;
- **пароль не должен:**
  - содержать информацию личностного характера (имя, фамилия, дата рождения, логин, название организации в любых словоформах), а также основываться на словах естественного языка;

- совпадать ни с одним из последних 10 (десяти) использованных ранее паролей;
- содержать более 2 (двух) следующих друг за другом одинаковых символов;
- включать легко вычисляемые сочетания символов (например, последовательно расположенные на клавиатуре символы: «12345678», «QWERTY»), содержать названия ИС или общепринятые сокращения («ИС», «USER» и т.п.);
- совпадать со стандартными паролями «по умолчанию» производителей ПО и технических средств;
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 (шести) позициях.

2.2.2. Требования по организации парольной защиты.

Пароль является строго конфиденциальной информацией[1]. 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 течение 1 (одного) рабочего дня с момента обнаружения факта компрометации с обязательным оповещением УКБ и КЦОПЛ.

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

2.2.3.1. При прекращении трудовых отношений с работниками Общества, непосредственным руководителем должна подаваться заявка в СПП о блокировке всех пользовательских учетных записей пользователя, с указанием даты и номера приказа Общества об увольнении.

2.2.3.2. В случае изменения трудовых обязанностей работника Общества, перевода на другую должность, в другое структурное подразделение его прежний руководитель подает заявку в СПП на ограничение прав доступа пользователя

[1] Информация ограниченного распространения и доступа, защита которой определена законодательством Российской Федерации, и / или ЛНД(А) Общества.

к ИС. В заявке необходимо указать дату ограничения прав доступа, перечень ресурсов и полномочий, назначенных пользователю ранее.

2.2.4. Предоставление удаленного доступа.

При необходимости осуществления своих трудовых обязанностей вне стационарных рабочих мест работникам Общества может быть предоставлен удаленный доступ по заявке в СПП.

Обязательным условием удаленного доступа к ИС для работников Общества является установка на корпоративном АРМ агента DLP-системы, принадлежащего ПАО «РусГидро».

В исключительных случаях по согласованию с УКБ удаленный доступ может осуществляться с личных АРМ при условии выполнения описанных требований и реализации одной из двух дополнительных мер:

- применение сертифицированного средства обеспечения безопасной дистанционной работы (специализированное защищенное USB-устройство, обеспечивающее загрузку компьютера с внешнего USB-носителя, на котором находится сертифицированная операционная система с набором предустановленного программного обеспечения);
- на личном АРМ должно быть установлено корпоративное антивирусное ПО с актуальными обновлениями на момент установки и дальнейшим периодическим автоматическим обновлением, а также агент DLP-системы, принадлежащей ПАО «РусГидро».

В случае необходимости предоставления доступа работникам сторонних организаций к ИС должен быть заключен договор и подписано соглашение о конфиденциальности.

Право доступа к информационным ресурсам Общества через сеть Интернет предоставляется пользователям только после обязательного согласования с УКБ заявки, направленной руководителем структурного подразделения Общества, в которой обосновывается необходимость предоставления доступа.

При формировании заявки на предоставление удаленного доступа инициатор заявки в обязательном порядке должен указать цель и срок предоставления доступа, название ИС, сетевые сегменты ЛВС Общества, из (в) которых(е) необходим доступ.

Заявка будет отклонена в следующих случаях:

- нарушения правил оформления заявки (в том числе некорректное обоснование необходимости предоставления доступа);
- несоответствия требованиям ИБ;
- наличия факторов, обуславливающих повышение рисков ИБ в результате выполнения заявки.

Согласованная заявка направляется на исполнение в СПП.

В рамках работ по заявке исполнитель предоставляет доступ к ИС и в дальнейшем может 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 контролируются на межсетевом экране, на серверах, в системах предоставления удаленного доступа.

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 УКБ и КЦОПЛ в случае появления подозрений на НСД с использованием их аутентификационных данных.

2.3. 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.

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, УКБ и КЦОПЛ обо всех выявленных ими фактах нарушения настоящей Политики.

2.3.1. Требования по использованию АРМ.

В соответствии с ЛНД(А) 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.

Пользователи при уходе с рабочего места обязаны блокировать доступ к рабочей станции средствами ОС, если блокировка не прервет технологический процесс и выполнение трудовых обязанностей. При отсутствии активности пользователя на рабочей станции в течение 10 (десяти) 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.

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

Установка стороннего ПО на рабочие станции возможна только по согласованию с УКБ.

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

2.3.2. 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 СМНИ на ноутбуках вне информационной инфраструктуры Общества осуществляется с учетом

ограничений, установленных пунктом 2.3.3 настоящей Политики и Инструкцией по использованию СМНИ в Группе РусГидро[2].

2.3.3. 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 УКБ заявкой, направленной руководителем структурного подразделения, 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.

2.3.4. 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 (спам).

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

---

[2] Приказ Общества от 19.04.2022 № 1п-37 «О присоединении к Инструкции по использованию съемных машинных носителей информации в Группе РусГидро и назначении ответственного за обеспечение информационной безопасности в АО «УК ГидроОГК»

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, в случае производственной необходимости передачи данной информации (в том числе в рамках осуществления договорной деятельности, взаимодействия с нотариусами), передачу информации необходимо осуществлять способом, обеспечивающим конфиденциальность и с обязательным уведомлением КЦОПЛ для внесения адресата в перечень адресов, с которыми разрешен обмен конфиденциальной информации. Передача конфиденциальной информации на зарубежные почтовые сервисы категорически запрещена;
- информации, содержание и направленность которой запрещены международным и российским законодательством, включая материалы, 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 адрес личной электронной почты, а также на личные адреса коллег, партнеров, других лиц и организаций, если легитимность такой пересылки официально не подтверждена;
- 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 15 Мб.

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 УКБ.

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.

2.3.5. 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 сети Интернет 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.

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

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), за исключением корпоративных сервисов, размещенных в сетевом периметре Общества;

- загружать информацию в системы обмена файлами, размещенные вне сетевого периметра Общества (за исключением внешних сервисов обмена файлами, с которыми Обществом заключен договор на оказание услуг и подписано соглашение о конфиденциальности, а также приняты меры по предотвращению утечки информации);
- использовать сервисы для работы с документами (редактирование, конвертирование, распознавание текста и т.д.), размещенные вне сетевого периметра Общества;
- несанкционированно использовать ресурсы сети Интернет, организовывать хакерские атаки, а также осуществлять другие действия, запрещенные 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, а также иной критичной информации, связанной с деятельностью Общества.

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 указанных 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.

2.3.6. Требования ИБ при замене АРМ или передаче в ремонт.

Перед передачей АРМ в ремонт сторонней организации работники совместно с работниками ООО «РусГидро ИТ сервис»[3] обязаны провести удаление информации на его дисках либо произвести демонтаж устройств хранения в периметре Общества.

[3] В соответствии с действующим Договором.

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 работником ООО «РусГидро ИТ сервис» произвести гарантированное удаление конфиденциальной информации.

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

2.3.7. Действия в нестандартных ситуациях.

Пользователи ИС обязаны немедленно ставить в известность своего непосредственного руководителя, УКБ и КЦОПЛ 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.

2.4. 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 УКБ.

2.4.1. 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 за установку и контроль наличия корректно функционирующего антивирусного ПО в ходе настройки и дальнейшего сопровождения АРМ отвечают работники ООО «РусГидро ИТ сервис», в соответствии с действующим Договором.

2.5. Контроль выполнения требований ИБ.

Контроль за соблюдением минимально необходимых требований ИБ осуществляет КЦОПЛ. В этих целях Обществом обеспечено подключение к технической инфраструктуре КЦОПЛ и передача данных о состоянии средств защиты информации в КЦОПЛ.

2.6. Профилактика нарушений Политики.

Под профилактикой нарушений настоящей Политики в Обществе понимается проведение разъяснительной работы по ИБ среди пользователей ИС, профилактических мероприятий по результатам проведения предварительных проверочных мероприятий по инцидентам ИБ.

Дополнительная разъяснительная работа проводится при возникновении инцидента нарушения положений настоящей Политики.

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

2.7. 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.