Приложение № 1 к приказу
от 30.04.2025 № ОД-0200

УТВЕРЖДАЮ
Генеральный директор

_____ А.Ф. Ханжин

«_30_» _____04_____ 2025 г.

РЕГЛАМЕНТ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ РЕСУРСОВ АО «КАРАБАШМЕДЬ»

Карабаш
2025

Содержание

1. ОБЩИЕ ПОЛОЖЕНИЯ ПО УПРАВЛЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

1.1. Термины, определения и сокращения

Термин	Определение
Актив	Произвольный объект, предмет или сущность, которые имеют потенциальную или фактическую ценность для Общества
Информационный ресурс	Разновидность актива, представляющая собой информацию на материальном носителе
Администратор	Работник Общества, наделенный правами администрирования информационных активов, в обязанности которого входят поддержка необходимых защитных мер и обеспечение использования информационного ресурса в соответствии с требованиями владельцев этих ресурсов
Бизнес-процесс (БП)	Система последовательной, целенаправленной деятельности, необходимой для осуществления бизнес-потребностей Общества
Владелец информационного ресурса (актива)	Работник Общества, наделенный полномочиями и отвечающий за утверждение прав доступа к активу в соответствии с принципом производственной необходимости
Вредоносное ПО	Компьютерная программа либо иная компьютерная информация, заведомо предназначенные для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации
Демилитаризованная зона (ДМЗ)	Сегмент вычислительной сети, явно выделенный для размещения сервисов, отвечающих на запросы из сети Интернет, и ограниченный в доступе к основным сегментам сети с помощью межсетевого экрана
Доступность информации	Свойство информации, которое характеризуется обеспечением беспрепятственного и своевременного доступа к ней субъектов, имеющих на это полномочия.
Информационная безопасность (ИБ)	Состояние защищенности интересов (целей) Общества от угроз в информационной сфере, а также сохранение конфиденциальности, целостности и доступности информации
Информационные технологии (ИТ)	Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов
Инцидент информационной безопасности	Одно или несколько нежелательных событий информационной безопасности, с которыми связана вероятность нанесения ущерба доступности, целостности или конфиденциальности информации, хранимой и обрабатываемой в локальной вычислительной сети Общества
ИТ-инфраструктура	Совокупность информационных технологий и технических средств, обеспечивающих хранение, обработку и передачу информации
Коммерческая тайна	Режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду
Контрагент	Юридическое или физическое лицо, использующее ИТ-инфраструктуру АО «Карабашмедь» при исполнении гражданско-правового договора (подрядчик, поставщик, партнер, консультант, стажер, практикант и т. д.)

Конфиденциальность информации	Свойство информации, которое характеризуется сохранением ее в тайне от субъектов, не имеющих прав на доступ к ней
Локальная вычислительная сеть (ЛВС)	Часть ИТ-инфраструктуры Общества, используемая для передачи информации
Межсетевой экран, Firewall	Программный или программно-аппаратный элемент ЛВС, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами
Нарушитель	Субъект, реализующий угрозы информационной безопасности
НСД	Несанкционированный доступ
НЭП	Неквалифицированная электронная подпись
Общество	АО «Карабашмедь»
Операционная система (ОС)	Комплекс взаимосвязанных программ, предназначенных для управления ресурсами компьютера и организации взаимодействия с пользователем
Пароль	Средство проверки личности пользователя для доступа к ресурсам ЛВС, обеспечивающее идентификацию и аутентификацию на основе сведений, известных только пользователю
Программное обеспечение (ПО)	Программа или множество программ, используемых для управления ЭВМ
Политика	Политика информационной безопасности, утвержденная Руководителем АО «Карабашмедь»
Пользователь	Лицо, группа лиц или организация, использующие информационные активы Общества в целях решения задач, отнесённых к их компетенции
ПЭП	Простая электронная подпись
Регламент	Регламент использования информационных ресурсов АО «Карабашмедь» (данный документ)
Риск информационной безопасности	Событие информационной безопасности, имеющее две характеристики: вероятность наступления события и ущерб вследствие наступления этого события
СЗИ	Средства защиты информации
СКЗИ	Средства криптографической защиты информации
Угроза информационной безопасности	Фактор или совокупность факторов, создающих опасность нарушения целостности, доступности и (или) конфиденциальности информации
УИБ	Управление информационной безопасности компании-партнера, оказывающей Обществу на основании договора консультационные услуги в области информационной безопасности
УИТ	Соответствующие подразделения компании-партнера, оказывающей Обществу на основании договора услуги в области информационных технологий
Уязвимость	Слабое место в информационной системе, которое может привести к нарушению целостности, доступности или конфиденциальности информации
Целостность информации	Свойство информации, которое характеризуется обеспечением ее достоверности и полноты
Security information and event management (SIEM)	Класс программных продуктов, предназначенных для сбора и анализа информации о событиях безопасности

RAID	Избыточный массив независимых (самостоятельных) дисков – технология виртуализации данных для объединения нескольких физических дисковых устройств в логический модуль для повышения отказоустойчивости и/или производительности
RAT	Утилиты удаленного управления (администрирования)
VLAN (виртуальная локальная компьютерная сеть)	Технология, позволяющая произвести группировку нескольких систем в выделенную сеть без физического отделения этих систем от общей сети
VPN (виртуальная частная сеть)	Территориально распределенная корпоративная логическая сеть, создаваемая на базе уже существующих сетей (локальных корпоративных сетевых структур, сетей связи общего пользования, сети Интернет, сетей связи операторов связи), имеющая сходный с основной сетью набор услуг и отличающаяся высоким уровнем защиты данных

1.2. Назначение и область действия Регламента

1.2.1. Цель Регламента

Целью Регламента является исполнение положений Политики информационной безопасности в части регулирования использования ИТ-инфраструктуры Общества контрагентами.

Регламент разработан с учетом требований законодательства, международных и национальных стандартов, а также лучших практик в области информационной безопасности.

Требования данного Регламента могут быть усилены или ослаблены в каждом конкретном случае на основе результатов оценки рисков ИБ работниками УИБ.

1.2.2. Область действия Регламента

Настоящий Регламент применяется на уровне Общества и при взаимодействии с контрагентами, использующими ИТ-инфраструктуру Общества.

Требования Регламента являются обязательными для исполнения контрагентами в период использования ИТ-инфраструктуры Общества. Соответствующие положения должны быть включены в обязательства контрагента по договору (приложение).

Требования данного Регламента применяются ко всем технологиям, компьютерной технике, сетям, приложениям, автоматизированным и операционным системам Общества, к процессам администрирования, сопровождения и использования информационных систем Общества.

Использование информационных активов Общества, вне зависимости от цели, автоматически накладывает ответственность по соблюдению требований, предусмотренных данным Регламентом.

1.3. Соответствие законодательству

1.3.1. Деятельность контрагента по обеспечению информационной безопасности должна соответствовать требованиям действующего законодательства.

1.3.2. Контрагент должен иметь соответствующие лицензии на виды деятельности по обработке и защите информации, определенные действующим законодательством как подлежащие лицензированию.

1.3.3. Использование контрагентом объектов авторского права и интеллектуальной собственности допускается только при наличии исключительных прав или на основании и в рамках лицензионных соглашений с их правообладателями.

1.3.4. Обработка персональных данных должна осуществляться контрагентом в соответствии с требованиями действующего законодательства и заключенного договора.

1.3.5. Информационные системы контрагента должны регулярно проверяться на предмет соответствия требованиям Общества в области информационной безопасности.

2. РОЛИ И ОТВЕТСТВЕННОСТЬ ЗА ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Представители контрагентов

Контрагенты в рамках исполнения требований Регламента несут ответственность за:

- ознакомление подчиненных работников, исполнителей с требованиями Регламента;
- выполнение требований Регламента;
- контроль выполнения подчиненными работниками, исполнителями требований Регламента;
- содействие представителям Общества в служебных расследованиях по фактам нарушения требований ИБ;
- своевременное предоставление требуемых документов и иной информации уполномоченным представителям Общества.

2.2. Управление информационной безопасности

Работники УИБ в рамках исполнения требований Регламента несут ответственность за:

- согласование доступа представителям контрагентов к ИТ-инфраструктуре Общества;
- разработку мер, нормативных документов и технических решений, направленных на минимизацию рисков ИБ;
- идентификацию и анализ угроз ИБ, источников угроз ИБ, уязвимостей информационных ресурсов, рисков реализации угроз ИБ;
- мониторинг журналов информационной безопасности (журналов сетевых событий, действий пользователей и администраторов информационных систем, журналов антивирусных приложений), SIEM-систем и т. п.;
- выявление, организацию расследования и ликвидацию инцидентов ИБ;
- контроль исполнения представителями контрагентов требований Регламента и иных нормативных документов Общества в области ИБ;
- согласование исключений из области действия Политики информационной безопасности;
- осуществление коммуникации с контрагентами по вопросам ИБ от имени Общества.

2.3. Управление информационных технологий

Работники УИТ в рамках исполнения требований Регламента несут ответственность за:

- предоставление контрагентам доступа к ИТ-инфраструктуре Общества после получения согласования УИБ;
- конфигурацию ИТ-активов Общества в соответствии с требованиями ИБ;
- реализацию требований информационной безопасности в ИТ-проектах по развитию информационной инфраструктуры, а также по разработке и внедрению информационных систем;
- реализацию корректирующих мероприятий по результатам аудита ИБ;
- предоставление требуемых документов и информации для проведения идентификации и оценки рисков ИБ;
- содействие в расследовании инцидентов информационной безопасности.

2.4. Подразделение-куратор Общества, ответственное за заключение договора

Руководитель подразделения-куратора и ответственные исполнители по договору в рамках исполнения требований Регламента несут ответственность за:

- включение положений о соблюдении требований Регламента и ответственности за их нарушение (в соответствии с приложением) во все договоры, дополнительные соглашения и иные документы, устанавливающие коммерческие отношения сторон, если взаимодействие сторон предполагает получение доступа к ИТ-инфраструктуре Общества в каком-либо виде (прибытие представителя контрагента на объект Общества для проведения работ, получение удаленного доступа и т. д.).

2.5. Ответственность за неисполнение Регламента

Нарушение контрагентом требований Регламента может быть выражено как в форме действия, так и бездействия.

Нарушение или невыполнение контрагентом требований Регламента является ненадлежащим исполнением договорных обязательств и влечет за собой последствия в виде применения к контрагенту санкций, а именно:

- предостережения (требования прекратить нарушение положений Регламента в срок, указанный Обществом);
- штрафа в размере 200 000 (двести тысяч) рублей за каждый факт нарушения или невыполнения требований Регламента;
- расторжения договора.

  В случае невыполнения требований предостережения (не устранения выявленного нарушения) в указанный срок, в случае выявления повторного нарушения требований Регламента, а также в случае, когда ущерб, вызванный данным событием, превысил один миллион рублей, Общество вправе в одностороннем внесудебном порядке отказаться от исполнения договора, заключенного с контрагентом, и потребовать компенсации вызванных прекращением договора убытков. Договор будет считаться прекращенным с момента направления Обществом в адрес контрагента уведомления об отказе от договора;
- запрета дальнейших коммерческих отношений с Обществом (внесение в «черный список»).

Вид применяемых санкций в каждом случае определяется на основании решения Общества и в соответствии с положениями договоров, дополнительных соглашений и иных документов, регламентирующих отношения контрагента и Общества.

В случае выявления факта нарушения или невыполнения требований Регламента сотрудниками УИБ составляется акт, в котором фиксируются:

- дата и время нарушения;
- описание выявленного события;
- номера пунктов Регламента, которые были нарушены или не выполнены;
- лицо, допустившее нарушение или невыполнение Регламента;
- срок устранения выявленного нарушения;
- последствия (ущерб), вызванные данным событием;
- санкция, которая подлежит применению к контрагенту.

Экземпляры акта направляются контрагенту и руководителю подразделения-куратора, Обществом принимается решение о характере (виде) санкций в отношении контрагента, допустившего нарушение или невыполнение Регламента.

Контрагент обязан в срок, указанный в акте, устранить выявленные нарушения и направить в адрес Общества ответ об устранении нарушения. Нарушение контрагентом требований акта в части срока устранения нарушения является основанием для применения других санкций в соответствии с Регламентом.

В случае применения штрафных санкций срок оплаты составляет 10 рабочих дней с момента получения контрагентом акта о выявленном нарушении. В случае отсутствия оплаты штрафа Общество оставляет за собой право в одностороннем порядке удержать сумму штрафа при выполнении оплаты по договору.

3. ОСНОВНЫЕ ТРЕБОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Требования к управлению учетными записями пользователей

3.1.1. Каждый пользователь должен иметь один уникальный идентификатор (логин), который используется им для доступа к информационным активам. Учетная запись пользователя, создаваемая для работы контрагентов, должна иметь ограниченный срок действия, согласуемый УИБ.

3.1.2. Предоставление доступа контрагентов к информационным активам Общества должно выполняться на основании запроса руководителя организации после согласования запроса руководством УИБ. В данном запросе контрагент обязан передать следующие сведения о работниках, для которых запрашивается доступ:

- Ф.И.О.;
- должность;
- адрес электронной почты;
- контактный номер телефона;
- описание должностных обязанностей / обоснование необходимости доступа.

3.1.3. Необходимым условием для согласования доступа к информационным активам Общества является предварительное подписание контрагентом Соглашения о неразглашении конфиденциальной информации (NDA) по форме Общества, а также согласие соблюдать требования настоящего Регламента и нести ответственность в случае нарушения положений Регламента.

3.1.4. Работа пользователей с системами ЛВС должна производиться только с использованием доменных учетных записей. Исключением являются сервисы, где использование доменных учетных записей технически невозможно. Запрещается использование локальных учетных записей пользователей, за исключением случаев проведения работ по настройке или устранению неполадок в работе ПО.

3.1.5. Каждый пользователь обязан осуществлять доступ к информационным активам Общества только с использованием личной учетной записи. Передача доступа к своей учетной записи другим лицам строго запрещена.

3.1.6. В общем случае использование прав локального администратора представителями контрагентов запрещено. Права локального администратора могут быть выданы учетной записи пользователя в случае наличия производственной необходимости и по согласованию с УИБ.

3.1.7. Использование «гостевых» учетных записей (учетных записей без пароля) для доступа к ИТ-инфраструктуре не допускается.

3.1.8. Доступ ко всем ресурсам и сервисам предоставляется в соответствии с принципом минимальной необходимости.

3.1.9. Запрещается самостоятельное повышение привилегий, а также иные методы несанкционированного расширения доступов учетной записи.

3.1.10. Учетная запись пользователя подлежит отключению в следующих случаях:

- наличие признаков инцидента ИБ, затрагивающих пользователя;
- отсутствие входов в сервисы ИТ-инфраструктуры Общества за последние 2 месяца;
- уведомление контрагента о прекращении доступа его представителю;
- завершение работ по проекту, для которого выдавался доступ.

3.2. Требования к парольной защите

3.2.1. Первоначальный пароль к учетной записи генерируется работниками УИТ и передается контрагенту по СМС, в защищенных мессенджерах, голосовой связью либо при личной встрече. Запрещается передача паролей по электронной почте или через третьих лиц. Пользователь обязан сменить полученный пароль при первом входе в систему. Пароль к учетной записи пользователя должен удовлетворять следующим требованиям:

- длина не менее 12 символов;
- должен содержать заглавные и строчные буквы, цифры, а также специальные символы: (! @ # $ % ^ & * ( ) - _ + = ~ [ ] { } | \ : ; ' " < > , . ? /);
- не должен совпадать со словарными словами, а также содержать личные данные пользователя, которые бы позволяли вычислить значение пароля, например:
  - Ф. И. О., номера телефонов, памятные даты (дни рождения и т. д.);
  - последовательно расположенные на клавиатуре символы («12345678», «QWERTY», и т. д.);
  - общепринятые термины и сокращения («USER», «TEST», «ADMIN» и т. п.);
- пароль не должен совпадать с последовательностями символов, использованных в качестве 10 предыдущих паролей пользователя к доменной учетной записи;
- пароль к доменной учетной записи не должен совпадать с паролями, используемыми пользователем для доступа к другим системам (например, домашний Интернет, бесплатная электронная почта, форумы и т. п.).

3.2.2. Смена паролей должна производиться не реже одного раза в 90 дней.

3.2.3. В случае ввода неправильного пароля 10 раз подряд учетная запись пользователя блокируется до рассмотрения причин блокировки работниками УИБ.

3.2.4. Пользователям запрещается передача паролей от своих учетных записей третьим лицам в каком-либо виде.

3.2.5. Запрещается хранить пароли (сертификаты, ключи доступа и т. д.) на бумажных носителях и на электронных носителях в открытом виде, т. е. без использования средств шифрования, в частности, запрещено хранение паролей в текстовых файлах и документах.

3.2.6. Запрещается передавать пароли (сертификаты, ключи доступа и т. д.) в открытом виде, т. е. без использования средств шифрования, в частности, строго запрещена передача паролей в тексте сообщений электронной почты.

3.2.7. В случае использования ПО или оборудования, которое поставляется вместе со стандартными паролями, заданными производителем, уполномоченные представители контрагента изменяют такие пароли на случайно сгенерированные и удовлетворяющие требованиям ИБ, после чего сообщают пароль уполномоченным работникам УИТ.

3.2.8. Рекомендуется хранить пароли в специализированном ПО (менеджерах паролей), например, KeePass.

3.2.9. Запрещается использовать пароли в анкетных опросах, намекать на формат паролей, называть их в присутствии посторонних лиц, отвечать на любые запросы в отношении паролей, а также вводить пароли от служебных учетных записей на каких-либо сторонних ресурсах.

3.2.10. Пользователям запрещается устанавливать и использовать одинаковые пароли для доступа к различным информационным активам Общества, за исключением случаев использования единой (доменной) учетной записи.

3.2.11. Для снижения рисков возникновения инцидентов ИБ пользователи обязаны:

- в случае подозрения на то, что пароль от учетной записи стал известен третьим лицам, незамедлительной поменять пароль и сообщить о возможном факте компрометации учетной записи в УИБ, а также своему непосредственному руководителю;
- в случае получения от кого-либо просьбы сообщить пароль от учетной записи незамедлительно сообщить о случившемся в УИБ;
- незамедлительно менять пароль к своей учетной записи по требованию УИБ.

3.3. Требования по использованию технологий удаленного доступа

3.3.1. Удаленный доступ предоставляется контрагентам на основании запроса руководителя организации после согласования запроса руководством УИБ. Запрос должен содержать обоснование необходимости удаленного доступа для каждого пользователя.

3.3.2. Все удаленные подключения к ЛВС Общества должны осуществляться с использованием технологии VPN, доступных протоколов IPSec, L2TP over IPSec или SSL. Должна обеспечиваться двухфакторная аутентификация пользователей при удаленном доступе к ЛВС с использованием защищенных протоколов авторизации.

3.3.3. Удаленный доступ предоставляется пользователям в соответствии с принципом минимальной необходимости.

3.3.4. При предоставлении удаленного доступа для каждого пользователя или группы пользователей должна быть настроена политика безопасности, определяющая перечень активов Общества, к которым предоставляются доступ, и права доступа.

3.3.5. Все устройства, используемые для удаленного доступа, должны иметь средства защиты, включающие антивирусные решения, межсетевые экраны, системы обнаружения вторжений, а также средства контроля приложений и устройств.

3.3.6. Запрещается передавать управление удаленным соединением третьим лицам.

3.3.7. Удаленное управление рабочими станциями и серверами, находящимися в ЛВС Общества, осуществляется при помощи протокола RDP и соответствующих утилит, входящих в состав операционной системы Microsoft Windows. Для Unix-подобных систем обязательно использование протокола SSH с авторизацией по сертификату.

3.3.8. Строго запрещается использование сторонних утилит удаленного администрирования (RAT), таких как TeamViewer, RemoteUtilities, RMS, RAdmin, AmmyyAdmin и т. п. Исключением являются случаи, когда использование таких утилит согласовано руководством УИБ.

3.3.9. При удаленном управлении системами, входящими в ЛВС Общества, запрещено копирование информации на личные устройства.

3.4. Требования по физической безопасности помещений обработки информации

i. В случае необходимости получения доступа в помещения обработки информации (центры обработки данных, кроссовые и т. п.) представителям контрагента руководитель организации должен заранее (не менее чем за 3 рабочих дня до планируемой даты начала работ) направить в Общество письмо, в котором указать:

- перечень помещений, в которые необходим доступ, а также состав проводимых работ;
- дату и время начала работ, а также их продолжительность;
- список лиц, которым требуется доступ в помещения: Ф.И.О., паспортные данные, должности, адреса электронной почты и контактные номера телефонов;
- список техники, вносимой на территорию Общества: марка, модель, серийный и инвентарный номер.

ii. Доступ в помещения обработки информации должен быть согласован руководством УИБ и осуществляться в сопровождении сотрудников службы охраны.

iii. Использование фото-, видео-, аудио- и иной записывающей техники (например, фото-, видеокамер, встроенных в мобильные телефоны) при работе в помещениях обработки информации без разрешения УИБ запрещено.

3.5. Требования по использованию ИТ-инфраструктуры Общества

3.5.1. При работе с сетью Интернет из сетей Общества контрагентам запрещено скачивать и устанавливать программное обеспечение на рабочие станции и серверы Общества без согласования с УИБ.

3.5.2. При работе с сетью Интернет с использованием активов Общества контрагентам запрещено посещать веб-ресурсы, не имеющие непосредственного отношения к работе. Деятельность контрагентов при работе в сети Интернет может контролироваться,

протоколироваться и периодически проверяться уполномоченными работниками УИБ. Использование информационных ресурсов Общества контрагентом означает согласие с тем, что за его деятельностью осуществляется контроль.

3.5.3. При работе с сетью Интернет с использованием активов Общества контрагентам запрещено пересылать и/или размещать на внешних ресурсах (публичных файловых серверах, форумах и т. д.) конфиденциальную информацию Общества, в частности, сведения, составляющие коммерческую тайну, персональные данные, хранимые и обрабатываемые в ЛВС, а также контактные данные работников Общества.

3.5.4. При работе с сетью Интернет контрагентам запрещено использование социальных сетей, систем мгновенного обмена сообщениями (мессенджеров) и других средств коммуникации, применение которых не согласовано с УИБ.

3.5.5. При работе с ИТ-инфраструктурой Общества контрагентам запрещено использование вычислительных ресурсов Общества в целях получения личной материальной выгоды, например, осуществление торговых операций, майнинга криптовалют и т. д.

3.5.6. Допускается использование только подключения к сети Интернет, которое предоставляется сотрудниками УИТ. Запрещается использование сторонних программно-аппаратных решений для доступа к внешним сетям, например, 3G-модемов, LTE-модемов и т. п.

3.5.7. Контрагентам запрещается самостоятельно (без согласования с УИТ и УИБ) вносить изменения в сетевые настройки серверов и рабочих станций, в частности, изменять настройки IP-адресов и маршрутизации сетевого трафика.

3.5.8. При работе с ИТ-инфраструктурой Общества контрагентам запрещается размещать и передавать угрожающую, клеветническую, непристойную информацию, а также любую иную информацию, нарушающую нормы действующего законодательства Российской Федерации. Также запрещается посещать веб-ресурсы, содержащие указанные типы информации.

3.5.9. При передаче конфиденциальной информации (коммерческой тайны, персональных данных и т. д.) через сообщения электронной почты контрагентам необходимо использовать средства шифрования.

3.5.10. Запрещается передача почтовых вложений, являющихся исполняемыми файлами, а также архивов, содержащих исполняемые файлы. В частности, речь идёт о файлах с расширениями .exe, .dll, .sys, .scr, .pif, .js, .cmd, .bat, .ps1 и т. п.

3.5.11. Запрещается установка устаревших версий программного обеспечения, в особенности версий ПО, снятых с поддержки производителем, в том числе операционных систем. Исключение составляют случаи, когда установка определённой версии ПО вызвана производственной необходимостью и согласована УИБ.

3.6. Требования по использованию съемных носителей и портативных устройств

3.6.1. Использование контрагентами съемных носителей информации, таких как флэш-карты, съемные и внешние жесткие диски, карты памяти (SD, CF, MemoryStick и др.), CD/DVD-R/W, магнитооптических дисков, подключаемых внешних устройств (ноутбуков, PDA, смартфонов) и др. при работе с ИТ-инфраструктурой Общества должно быть согласовано с УИБ.

3.6.2. Запрещается копирование конфиденциальной информации (коммерческой тайны, персональных данных и т. д.) Общества на съемные носители, принадлежащие контрагенту.

3.6.3. Все носители информации и портативные устройства, вносимые контрагентами на объекты Общества, должны быть учтены в специальной книге учета, а их внос организован согласно процедуре, описанной в разделе 3.4.

3.6.4. Все носители информации и иные электронные устройства, подключаемые к ЛВС, должны быть просканированы антивирусным ПО на предмет наличия вредоносного ПО.

3.6.5. Все портативные устройства, вносимые контрагентами на объекты Общества, должны иметь установленное антивирусное ПО с актуальными версиями антивирусных баз и программных модулей.

3.6.6. На все портативные устройства, вносимые контрагентами на объекты Общества, должны быть установлены обновления безопасности операционных систем и прикладного ПО.

3.7. Требования по использованию облачных сервисов

3.7.1. Для обмена информацией между контрагентами и Обществом могут использоваться облачные сервисы, такие как хранилище NextCloud и платформа Microsoft Project. Представителям контрагента могут быть созданы локальные учётные записи в сервисе NextCloud и предоставлен доступ к директориям работников Общества по согласованию с владельцем директории и УИБ.

3.7.2. Для организации доступа контрагента к облачному сервису работник подразделения-куратора должен сформировать заявку в систему Service Desk с указанием следующих данных представителя контрагента:

- Ф.И.О;
- должность;
- адрес электронной почты;
- контактный номер телефона;
- список папок (директорий) или проектов, к которым необходим доступ;
- требуемый уровень прав доступа (только чтение / чтение и запись);
- описание должностных обязанностей / обоснование необходимости доступа.

Обязательным условием для согласования доступа к облачному сервису является предварительное подписание контрагентом соглашения о неразглашении конфиденциальной информации (NDA) по форме Общества, а также согласие соблюдать требования настоящего Регламента и нести ответственность в случае нарушения (неисполнения) положений Регламента.

3.7.3. При работе с облачными сервисами запрещается размещение вредоносного и потенциально опасного ПО и иных материалов, нарушающих действующее законодательство Российской Федерации.

3.7.4. При работе с облачными сервисами запрещается размещение персональных данных физических лиц, а также материалов, содержащих коммерческую тайну.

3.7.5. Запрещается использование облачных сервисов для передачи материалов личного характера, фото-, видео- или иной информации, не относящейся к деятельности Общества.

3.7.6. В целях экономии дискового пространства пользователи проводят пересмотр информации, находящейся в используемых ими директориях облачного хранилища, и удаляют информацию, потерявшую свою актуальность и утратившую свою ценность для выполнения служебных задач. Пересмотр должен проводиться не реже чем один раз в год.

3.7.7. Представителям контрагента запрещается передавать файлы, полученные через облачные сервисы, лицам, не имеющим доступа к соответствующей директории или проекту. Также запрещается передача аутентификационных данных к облачному сервису третьим лицам.

3.7.8. В случае изменения должностных обязанностей или увольнения представителя контрагента его учётная запись в облачном сервисе незамедлительно блокируется.

3.8. Требования по защите от вредоносного программного обеспечения

3.8.1. Все серверы и рабочие станции контрагента, с которых осуществляется доступ к ИТ-инфраструктуре Общества, производится хранение и обработка данных Общества, а также иные системы, задействованные для выполнения работ по договорным обязательствам с Обществом, должны быть оснащены антивирусным ПО.

3.8.2. Допускается использование только лицензионных антивирусных средств, легитимно закупленных у поставщиков таких программных и программно-аппаратных комплексов.

3.8.3. Антивирусное ПО, используемое контрагентом, должно всегда иметь актуальные версии антивирусных баз и программных модулей. Установленные защитные решения должны получать обновления из достоверных источников не реже трех раз в день.

3.8.4. Запрещается частичное или полное отключение антивирусного ПО (выключение модулей, отключение защиты, завершение работы программы и т. д.). Также запрещается изменение конфигурации антивирусного ПО, приводящее к снижению уровня обеспечения информационной безопасности. Настройки антивирусных решений должны включать эвристические и сигнатурные методы обнаружения, автоматическое лечение зараженных объектов, протоколирование событий.

3.8.5. Не реже одного раза в неделю должно производиться автоматизированное антивирусное сканирование всех серверов и рабочих станций контрагента.

3.8.6. При обнаружении вредоносного ПО или других признаков инцидента ИБ на системах, используемых в работе с ЛВС Общества, а также хранящих и обрабатывающих данные Общества, контрагент обязан:

- проинформировать УИБ;
- прекратить использование зараженной системы (отключить компьютер от сети);
- проинформировать непосредственного руководителя.

3.9. Требования к выполнению работ на сетевой инфраструктуре Общества

3.9.1. Создание новых сетевых соединений (подключений) между сегментами сети и установка сетевого оборудования без согласования с УИБ запрещена. Методы сетевого взаимодействия с внешними сетями должны быть согласованы с УИБ и отражены в проектной, а также в рабочей документации.

3.9.2. Все телекоммуникационное оборудование должно находиться в выделенных защищаемых помещениях или телекоммуникационных шкафах, оборудованных в соответствии с требованиями по физической безопасности. Все неиспользуемые интерфейсные порты коммуникационного оборудования должны быть отключены.

3.9.3. Все кабели кабельной системы должны быть проложены в коробах, фальшполах/потолках или иным способом, исключающим их вывод наружу. Все коммутационные панели должны быть расположены в контролируемых защищаемых помещениях или запираемых и опломбированных шкафах.

3.9.4. На коммутационных панелях должна находиться маркировка кабелей в соответствии с текущей таблицей подключений и соединений. Телекоммуникационное оборудование должно быть промаркировано (например, наклейками на передней панели) таким образом, чтобы его можно было однозначно идентифицировать, например, по инвентарному номеру.

3.10. Требования к обработке персональных данных

3.10.1. Передача (доступ) персональных данных осуществляется в порядке, установленном внутренними документами Общества, в соответствии с действующим законодательством, регламентирующим обработку персональных данных.

3.10.2. Доступ к системам, содержащим персональные данные, предоставляется по согласованию с работником, ответственным за данную систему, и УИБ. Запрос доступа осуществляется путём направления заявки через систему Service Desk или служебной записки в СЭД DIRECTUM от работника Общества, ответственного за взаимодействие с контрагентом.

3.10.3. Доступ к системам, содержащим персональные данные, предоставляется в соответствии с принципом минимальных привилегий (отсутствием избыточности прав доступа) при наличии мотивированного обоснования. Обоснование доступа должно включать описание поставленной задачи, её регулярность, а также преследуемые цели.

3.10.4. Запрещается копирование избыточных для решения выполняемой задачи персональных данных в локальные хранилища (носители информации).

3.10.5. После окончания работы со скопированными персональными данными (либо при приостановке работы на длительный срок) скопированные данные должны быть удалены из локального хранилища.

3.10.6. Запрещается хранение и обработка персональных данных из систем, входящих в ИТ-инфраструктуру Общества, на системы, не принадлежащие Обществу, в том числе на

личные носители информации и облачные сервисы, за исключением случаев, согласованных УИБ, когда такие сервисы соответствуют требованиям законодательства.

3.10.7. Запрещается импорт персональных данных в другие системы без согласования УИБ, а также владельца актива, в котором хранятся и обрабатываются данные на текущий момент.

3.10.8. Запрещается злоупотреблять возможностью доступа к персональным данным и использовать их в личных целях. В случае обращения третьих лиц с просьбами о доступе к персональным данным необходимо проинформировать УИБ.

Приложение
к Регламенту использования информационных ресурсов
АО «Карабашмедь»

Оговорка для включения в договоры АО «Карабашмедь»[1]:

Исполнитель[2] обязан выполнять требования Регламента использования информационных ресурсов АО «Карабашмедь» (далее – Регламент), размещенного на официальном сайте Заказчика[3]: https://karmed.ru. Стороны руководствуются редакцией Регламента, действующей на момент заключения Договора / дополнительного соглашения к Договору[4].

Подписывая настоящий договор (соглашение), Исполнитель подтверждает, что ознакомился с текстом Регламента полностью, принимает на себя обязательства, которые относятся к обязательствам контрагента в соответствии с Регламентом. Также Исполнитель подтверждает, что согласен с условиями об ответственности, предусмотренными Регламентом, считает их соразмерными и не нарушающими его права и законные интересы.

В случае нарушения Исполнителем обязанностей, предусмотренных Регламентом, Заказчик вправе применить к Исполнителю ответственность, установленную Регламентом.

[1] Настоящая оговорка обязательна для включения во все договоры, а также в соглашения о конфиденциальности, стороной которых является Акционерное общество «Карабашмедь». Договоры, соглашения, заключенные до начала действия Регламента, должны быть дополнены указанной оговоркой посредством заключения отдельного дополнительного соглашения или при оформлении очередного дополнительного соглашения к договору.

[2] Наименование контрагента приводится так, как указано в договоре (исполнитель, подрядчик, поставщик и т. д.).

[3] Наименование Общества приводится так, как указано в договоре (заказчик, покупатель и т. д.).

[4] Следует указать Договор или дополнительное соглашение к Договору в зависимости от того, в какой документ включена оговорка.

Лист регистрации изменений

Номер изменения	Номер раздела	Номер страницы	Дата введения изменения	Подпись