

Техническое задание
на оказание услуг по сопровождению и технической поддержке центра компетенций по
управлению процессами и регламентацией на базе системы управления эксплуатацией
цифровых сервисов с использованием отечественного программного обеспечения
(АСУИИиК) ПАО «Россети»

1. Общие сведения

1.1. Термины, определения и сокращения

Сокращение, термин	Расшифровка сокращения, определение
Аппаратные компоненты	Тип компонентов Объекта услуг, включающий категории Аппаратная ИВИ (серверное оборудование, сетевое оборудование, СХД), Прочее оборудование (ВКС, телефония)
АРМ	Автоматизированное рабочее место
АСУИИиК	Автоматизированная система управления инцидентами, изменениями и конфигурациями на базе программного обеспечения BPMSoft, САСП Заказчика.
База знаний	Информационный ресурс заказчика, содержащий информацию по ИС и другую нормативную документацию.
Время решения	Время, в течение которого Служба технической поддержки Исполнителя должна решить запрос пользователя Объекта Услуг и описать решение без учёта времени уточнения у пользователя недостающей для решения запроса информации. Выполнение заявки также может откладываться (приостанавливаться) по другим, не зависящим от Исполнителя, причинам, из-за отсутствия пользователя или его неготовности к проведению необходимых работ
Время реакции	Интервал времени между моментом регистрацией заявки пользователя Объекта Услуг специалистом Службы технической поддержки Исполнителя и моментом назначения заявки на Специалиста Службы технической поддержки Исполнителя.
ГК	Группа компаний «Россети»
Договор	Договор, к которому данное ТЗ является неотъемлемым приложением
ЕСПП	Единая служба поддержки пользователей
Заказчик	Акционерное общество «Россети Цифра» (АО «Россети Цифра»)
Запрос на обслуживание (ЗНО)	Запрос пользователя Объекта услуг на информацию, консультацию или действие по управлению доступом к функциям и данным Объекта услуг, который не связан с возникновением сбоя в работе Объекта услуг или необходимостью внесения изменений в Объект услуг
Запрос на изменение (ЗНИ)	Заявка пользователя Объекта Услуг на выполнение доработки или изменения Объекта Услуг. ЗНИ включает в себя детали предлагаемого изменения.
Заявка	Обращение, составляемое пользователем Объекта услуг и передаваемое

	в ЕСПП с целью дальнейшего получения Услуг от Исполнителя
ИБ	Информационная безопасность
ИВИ	Информационно-вычислительная инфраструктура
Инженерные компоненты	Тип компонентов Объекта услуг, включающий категорию Инженерные системы (система электропитания, система охлаждения, система пожаротушения, СКУД, прочие инженерные системы ЦОД)
Инициатор	Инициатором является представитель Заказчика, который направил запрос в САСП
Информационная система, ИС	Программное или программно-аппаратное решение Заказчика, предназначенное для автоматизации деятельности одного или нескольких подразделений
Инцидент	Незапланированное прерывание или снижение качества работы Объекта Услуг
Исполнитель	Исполнитель по договору на оказание услуг, определяется в результате закупочной процедуры
ИТ	Информационные технологии
Класс критичности	Категория, присваиваемая информационной системе или ее компонентам в зависимости от степени важности и влияния на бизнес-процессы организации
Куратор	Функциональный заказчик, одно или несколько подразделений Заказчика.
Объект Услуг, Объект	Одна из централизованных информационных систем ПАО «Россети»
ОРД	Организационно-распорядительный документ
Опротестованная заявка	Заявка Заказчика, не принятая им после исполнения, обоснованно возвращённая на доработку.
ПАО	Публичное акционерное общество
ПО	Программное обеспечение
Пользователь Заказчика	Сотрудники Заказчика, использующие Объект услуг в служебных целях. Также пользователями могут выступать сотрудники сторонних организаций, контрагентов Заказчика
Порядок	Порядок оказания Услуг, являющийся Приложением к настоящему ТЗ
Представитель	Сотрудники ИТ-подразделения Заказчика, отвечающего за обеспечение

Заказчика	эксплуатации Объекта услуг, а также сотрудники функционального заказчика
Прикладное ПО (ППО)	Прикладное программное обеспечение — ПО BPMSoft, предназначенное для решения практических задач и предназначенный на непосредственное взаимодействие с пользователями.
ПЭ	Промышленная эксплуатация
Регламентные работы	Работы, производимые для поддержания работоспособности Объекта услуг и его компонентов, с обязательным согласованием с Заказчиком
САСП	Система автоматизации службы поддержки пользователей ПАО «Россети». В соответствии с настоящим ТЗ используется система АСУИИиК ПАО «Россети» на базе ПО BPMSoft
Сервис-менеджер	Сотрудник со стороны Исполнителя, который отвечает за решение вопросов, связанных с организацией предоставления Услуг
Системное ПО (СПО)	Системное программное обеспечение - ПО, необходимое для обеспечения функционирования сервера или АРМ (ОС, необходимые драйверы)
Служба технической поддержки	Структурное или функциональное подразделение Исполнителя, предназначенное для оказания Услуг по предоставлению доступа и технической поддержке пользователей Объекта услуг в процессе его эксплуатации Пользователям
Соглашение	Соглашение об уровне Услуг, Service Level Agreement (SLA), в котором определены целевые показатели качества услуг.
Специалист Службы технической поддержки	Сотрудник Исполнителя, который осуществляет рассмотрение, анализ и обработку поступающих заявок Пользователей в Службу технической поддержки.
Стороны	Совместно Заказчик и Исполнитель
Технологическое окно	Регулярные, заранее определённые и согласованные отрезки времени, в течение которых внедрение изменений может быть выполнено с минимальным негативным воздействием на Объекты Услуг.
ТЗ	Техническое задание
Услуги	Услуги, оказываемые в соответствии с условиями договора, в т.ч. данного ТЗ
Фиктивная заявка	Заявка, самостоятельно созданная Специалистом Службы технической поддержки для искусственного увеличения объема оказанных услуг с целью обоснования нарушений Соглашения
ЦИС	Централизованные Информационные Системы

--	--

1.2. Заказчик и Исполнитель

1.2.1. Заказчик: Акционерное общество «Россети Цифра» (АО «Россети Цифра»)

1.2.2. Исполнитель по договору на оказание услуг, определяется в результате закупочной процедуры.

1.3. Полное и краткое наименование Услуг

1.3.1. Полное наименование: Услуги по сопровождению и технической поддержке центра компетенций по управлению процессами и регламентацией на базе системы управления эксплуатацией цифровых сервисов с использованием отечественного программного обеспечения (АСУИИиК) ПАО «Россети».

1.3.2. Краткое наименование: Услуги.

1.4. Место и сроки оказания Услуг

1.4.1. Место оказания Услуг: на территории Исполнителя.

1.4.2. Централизованные информационные системы устанавливаются на серверах Заказчика. Пользователям Заказчика предоставляется доступ и техническая поддержка в соответствии с настоящим ТЗ.

1.4.3. Сроки оказания Услуг: с даты подписания договора по «31» июля 2028г.

2. Характеристика Услуг

2.1. Объекты Услуг

2.1.1. Объектами Услуг являются Информационные системы Заказчика, указанные в Приложении 1.

2.2. Цели оказания Услуг

2.2.1. Обеспечение единства управления и непрерывности вертикально-интегрированных бизнес-процессов Заказчика, автоматизация которых осуществляется с использованием Объектов Услуг, включенных в ТЗ.

2.3. Результаты оказания Услуг

2.3.1. Результатами оказания Услуг являются:

- Объекты Услуг, функционирующие с соблюдением требований надежности в соответствии со степенью критичности для каждого Объекта Услуг;
- отработанные с соблюдением условий Соглашения заявки Пользователей;
- решённые с соблюдением условий Соглашения инциденты и устранённые сбои в работе Объектов Услуг;
- выполненные в согласованные сторонами сроки доработки / изменения Объектов Услуг в соответствии с ЗНИ, при условии, что соответствующая услуга входит в объем Услуг для Объекта Услуг;
- ведение и постоянная актуализация базы знаний по всему объему Объекта Услуг.

2.4. Общие требования к качеству Услуг

2.4.1. Качество оказываемых Исполнителем Услуг должно соответствовать требованиям действующего законодательства Российской Федерации и условиям заключенного Договора.

2.4.2. Общие требования к качеству оказываемых Исполнителем Услуг определены положениями следующих государственных стандартов:

- ГОСТ ИСО 9001-2015. «Системы менеджмента качества. Требования»;
- ГОСТ 34.201-2020. «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначения документов при создании автоматизированных систем»;
- ГОСТ Р 59793-2021. «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»;
- ГОСТ Р 57193-2016. «Информационная технология. Системная инженерия. Процессы жизненного цикла систем»;
- ГОСТ Р ИСО/МЭК 14764-2002. «Информационная технология. Сопровождение программных средств».

2.4.3. Дополнительные и специальные требования к условиям и качеству оказания Исполнителем Услуг содержатся в карточках услуг в Приложении 2 к настоящему ТЗ.

2.4.4. При оказании Услуг Исполнитель обязан соблюдать внутренние регламенты и процедуры, утверждённые Заказчиком. Документы с описанием соответствующих регламентов и процедур, не включенных в объем передаваемых документов в соответствии с условиями ТЗ, предоставляются по требованию Исполнителя в согласованные сторонами сроки. Перечень передаваемых Заказчиком Исполнителю документов, необходимых для оказания Услуг, указан в Приложении 3 к настоящему ТЗ.

2.5. Требования к персоналу Исполнителя.

2.5.1. В случае неоднократного нарушения требований настоящего документа Исполнителем при оказании той или иной услуги, Заказчик вправе осуществить проверку подготовленности персонала Исполнителя для сопровождения Объектов Услуг.

3. Общие требования к Услугам

3.1. Основные стандарты непрерывности Объектов Услуг по классам Критичности

3.1.1. В отношении Объектов Услуг установлены следующие требования в части соответствия основным стандартам непрерывности по классам Критичности:

- К-1, критически важные – Объекты Услуг, работающие непрерывно, выход из строя которых влечёт за собой невозможные потери для бизнеса, в т.ч. угрозу жизни и здоровью персонала и населения;
- К-2, критические для бизнеса – критические для управления организацией Заказчика Объекты Услуг, как правило, с непрерывным режимом работы,

выход из строя которых влечёт за собой значительные потери и ущерб для Заказчика;

- К-3, важные для бизнеса – обычные Объекты Услуг, с режимом работы, соответствующим Рабочему времени Заказчика;
- К-4, поддерживающие – не критические для управления организацией Заказчика Объекты Услуг, в случае отказа которых организация Заказчика остается способным осуществлять свою основную деятельность без заметной потери качества

3.1.2 Основные стандарты непрерывности Объектов Услуг по Классам критичности приведены в таблице ниже. Время указано календарное. Класс критичности определяет требования к режимам эксплуатации ИТ-решения, к уровню предоставления услуг (SLA).

Класс Критичности

№ п/п	Наименование характеристики	Классификация критичности Объекта Услуг			
		Критически важные (К-1)	Критические для бизнеса (К-2)	Важные для бизнеса (К-3)	Поддерживающие (К-4)
1	Целевая доступность	99,96%	99,73%	99,20%	98,00%
2	Возможные внеплановые простои в месяц	18 мин	~2 ч	~6 ч	~14 ч
3	Время восстановления при аварии (RTO)	30 мин	4 ч	24 ч	72 ч
4	Срок утраты данных при аварии (RPO)	~0	8 ч	24 ч	24 ч
5	Требуемый режим работы системы	24x7	24x7	8x5	8x5
6	Доступность ИТ специалистов	24x7	24x7/8x5	8x5	8x5
7	Время проведения техобслуживания	В зависимости от Объекта Услуг 23:00-03:00 / 20:00-06:00			

3.2. Ограничения в части оказания Услуг

3.2.1. Услуги не включают устранение последствий, возникших в результате:

- злонамеренных действий Заказчика или третьих лиц по отношению к Объекту услуг;

- действий Заказчика или третьих лиц, если они были совершены вопреки эксплуатационной документации на Объект услуг;
- проблем, относящихся к сторонним программным, аппаратным или инженерным компонентам инфраструктуры Заказчика, не входящим в состав Объекта услуг, посредством которых Пользователи получают доступ к Объекту услуг;
- использования Заказчиком Объекта услуг способом или в целях, для которых они не были предназначены.

3.2.2. Услуги не включают обучение Пользователей работе с Объектом услуг за исключением разработки и передачи инструкций при предварительном согласовании их с Заказчиком, а также не включают выдачу сертификатов, подтверждающих квалификацию Пользователей для работы с Объектом услуг.

3.2.3. Технологические окна обслуживания Объектов Услуг должны использоваться для выполнения операций настройки, обновления, обслуживания программных компонентов Объектов Услуг. В данный период функции Объектов Услуг полностью или частично становятся недоступными для Пользователей. Технологические перерывы на обслуживание каждого Объекта услуг указаны в Приложении 1 к настоящему ТЗ. ЕСПП и Заказчик оповещается о проведении данных работ предварительно согласованным способом.

3.2.4. Исполнитель имеет право вносить согласованные Заказчиком изменения в характеристики Объекта услуг в случае, если это требуется для обеспечения работы Объекта услуг.

4. Требования к видам обеспечения

4.1. Требование к документационному обеспечению

4.1.1. Обновление и доработка Объектов Услуг должны сопровождаться:

- предоставлением информации Пользователям по составу устанавливаемых обновлений / выполненных доработок Объекта Услуг в формате документа «Список изменений»;
- передачей Исполнителем Заказчику обновленного пакета эксплуатационной документации, если обновление или доработка Объекта Услуг включает создание новых или изменение существующих прикладных функций Объекта Услуг, требующих соответствующих изменений в документации.

4.1.2. Предоставление Объектов Услуг Заказчику в качестве сервиса должно сопровождаться передачей Исполнителем Заказчику пакета эксплуатационной документации Объекта Услуг в бумажном и/или электронном виде.

4.1.3. Вся документация на предоставляемый Заказчику в качестве сервиса Объектов Услуг, в том числе руководства Пользователя и Администратора Объектов Услуг, должна быть разработана на русском языке. Срок предоставления Заказчику документации не должен превышать более 4 недель с момента заключения Договора.

4.2. Требования к организационному обеспечению

4.2.1. Стороны до начала оказания Услуг обмениваются сведениями об ответственных за оказание Услуг лицах, их контактных телефонах и адресах электронной почты.

4.2.2. Взаимодействие Сторон должно быть организовано в соответствии с Порядком оказания услуг, приведённом в Приложении 4 к настоящему ТЗ.

4.3. Требования к программному обеспечению

4.3.1. Доступ Исполнителю к функциональности Объекта услуг должен быть обеспечен в том числе на АРМ под управлением ОС «Альт рабочая станция», с установленным офисным пакетом «Р7-Офис. Профессиональный» и web-браузером «Яндекс.Браузер».

4.3.2. На ИВИ Объекта услуг должно быть установлено антивирусное ПО, включенное в реестр российского ПО, с ежедневно обновляемыми антивирусными базами;

4.3.3. Используемая в составе Объекта услуг ОС должна иметь установленные актуальные обновления безопасности.

4.4. Требования к защите информации и информационной безопасности

4.4.1. Общие требования

4.4.1.1. Требования к защите информации и конфиденциальности, указанные в данном разделе ТЗ, дополняют требования, указанные в соответствующем разделе Договора. В случае противоречия требований данного раздела с положениями Договора, считать верными положения Договора.

4.4.1.2. Оказание Услуг должно выполняться в соответствии с правилами информационной безопасности (Приложение 5 к настоящему ТЗ).

4.4.1.3. Исполнитель гарантирует конфиденциальность информации Заказчика, полученной в процессе оказания Услуг, в случае передачи информации, составляющей коммерческую тайну, Исполнитель обязуется подписать соответствующее соглашение по утверждённой у Заказчика форме.

4.4.1.4. Исполнитель обязан провести инструктаж работникам, привлекаемым к оказанию Услуг (в том числе удаленно) по соблюдению Правил информационной безопасности и режима конфиденциальности информации, установленных Заказчиком, и предоставить Заказчику расписки об ознакомлении работников с локальными нормативными актами Заказчика о защите конфиденциальной информации.

4.4.1.5. Любая информация о функционировании информационной инфраструктуры Заказчика, ставшая известной Исполнителю, не должна без разрешения или поручения Заказчика передаваться третьим лицам. При этом, информация, содержащаяся в заявках Заказчика в Службу технической поддержки Исполнителя, в случае если такие заявки входят в состав Услуг, может быть передана представителям производителя компонентов Объектов Услуг, если такие действия (передача информации) требуются для оказания Услуг.

4.4.1.6. Специалисты Исполнителя обязаны не препятствовать записи журналов событий, связанных с их вмешательством в работу Объекта Услуг.

4.4.1.7. В случае проведения расследования инцидентов ИБ Исполнитель должен обеспечить полное содействие всех задействованных в

обслуживании Объекта услуг специалистов, а также работников, имеющих отношение к инциденту, предоставить необходимые пояснения, в том числе при необходимости в письменном и официальном виде.

4.4.2. Требования к организации удалённого доступа

4.4.2.1. Требования к режиму удалённого доступа в части организации защищённого доступа сторонних организаций в КСПД Заказчика приведены в приложении 5.

4.4.3. Требования к АРМ специалистов Исполнителя

4.4.3.1. АРМ специалистов Исполнителя, используемые для оказания Услуг (в том числе удаленно) должны соответствовать следующим требованиям:

- на АРМ должно быть установлено антивирусное ПО, включенное в реестр российского ПО, с ежедневно обновляемыми антивирусными базами;
- используемая ОС должна иметь установленные актуальные обновления безопасности;
- пароль учетной записи должен состоять не менее чем из 12 символов, включая прописные буквы, цифры и специальные символы;
- на АРМ сотрудников Исполнителя, задействованных в оказании услуг в соответствии с настоящим ТЗ, не должно быть установленного ПО для организации удаленного доступа к информации или ОС (в т.ч. программ типа TeamViewer, RAdmin);
- АРМ должен находиться на территории, определённой условиями договора и/или технического задания. Не допускается указание услуг с использованием мобильных АРМ или общедоступных АРМ.

5. Перечень и порядок оказания Услуг

5.1. Требования к составу и содержанию Услуг

5.1.1. Перечень Объектов Услуг и содержание Услуг приведены в Приложениях 1 и 2 к настоящему ТЗ.

5.2. Порядок оказания Услуг

5.2.1. Порядок оказания Услуг приведён в Приложении 4 к настоящему ТЗ.

5.2.2. Исполнитель в соответствии с указанным в карточках Услуг (см. Приложение 2) графиком активирования осуществляет подготовку и предоставление Заказчику бухгалтерских и отчётных документов.

5.2.3. Формы отчётных документов приведены в Приложении 6 к настоящему ТЗ.

6. Перечень приложений

Приложение 1. Перечень Объектов Услуг;

Приложение 2. Содержание Услуг;

Приложение 3. Перечень передаваемых документов;

Приложение 4. Порядок оказания Услуг;

Приложение 5. Правила информационной безопасности;

Приложение 6. Формы отчётных документов (общие);

Приложение 1

Перечень Объектов Услуг

№ п/п	Наименование ИС	Код ИС	Функциональный заказчик	Класс критичност и	Технологическо е окно	Перечень услуг, включенных в объем ТЗ
1	Автоматизированная система управления инцидентами, изменениями и конфигурациями	АСУИИиК	Департамент технической политики ИТ-решений	К-3	22:00-03:00	Услуга 1 – Центр компетенций АСУИИиК

Содержание Услуг

- 1) Сопровождение и техническая поддержка центра компетенций по управлению процессами и регламентацией на базе системы управления эксплуатацией цифровых сервисов с использованием отечественного программного обеспечения (АСУИИиК)**

Общее описание

АСУИИиК – автоматизированная система управления инцидентами, изменениями и конфигурациями на базе программного обеспечения BPMSoft, позволяет осуществлять управление обращениями пользователей, а также эксплуатацией цифровых сервисов. Система предназначена для обеспечения выравнивания методологии бизнес-процессов Заказчика при эксплуатации цифровых сервисов, а также обеспечения единства управления цифровыми сервисами и непрерывности вертикально-интегрированных бизнес-процессов ГК «Россети».

Зона охвата Услуг Центра компетенций АСУИИиК

п/п	Наименование компонента Объекта Услуг	Тип компонента Объекта Услуг	Категория Услуги компонента Объекта Услуг
1.	Управление запросами на обслуживание и инцидентами	Программные компоненты	Прикладное ПО
2.	Управление уровнем и каталогом услуг	Программные компоненты	Прикладное ПО
3.	Управление доступом	Программные компоненты	Прикладное ПО
4.	Управление изменениями и релизами	Программные компоненты	Прикладное ПО
5.	Управление конфигурациями	Программные компоненты	Прикладное ПО
6.	Управление проблемами	Программные компоненты	Прикладное ПО
7.	Управление знаниями	Программные компоненты	Прикладное ПО
8.	Управление активами	Программные	Прикладное ПО

		компоненты	
9.	Управление искусственным интеллектом	Программные компоненты	Прикладное ПО
10.	Управление сервисами (портальный, почтовый и глобальный поиск)	Программные компоненты	Прикладное ПО
11.	Устранение инцидентов	Программные компоненты	Прикладное ПО
12.	Управление регламентными работами	Программные компоненты	Прикладное ПО
13.	Управление интеграциями	Программные компоненты	Прикладное ПО
14.	Настройка конфигурации системы	Программные компоненты	Прикладное ПО
15.	Интеграция с каталогом пользователей Заказчика	Интеграционные механизмы	Прикладное ПО
16.	Интеграция с почтовой системой Заказчика	Интеграционные механизмы	Прикладное ПО

Зона охвата Услуг

Зона охвата Услуг*	Прикладное ПО BPMSoft	Системное ПО	ИВИ	Интеграционные механизмы
	[v]	[x]	[x]	[x]

* [x] – компонент не входит в зону охвата Услуги, [v] – компонент входит.

Услуга 1. Центр компетенций АСУИИиК

Название	Описание
Код услуги	БИЗ.ИС.АСУИИиК-01
Название Услуги	Центр компетенций в части разработки методологии управления процессами эксплуатации цифровых сервисов на базе АСУИИиК
Категория Услуги	Бизнес-услуга
Перечень работ в составе Услуги	– Проведение детального анализа существующих ИТ бизнес-процессов; – Создание, актуализация унифицированных регламентов

	управления и поддержки ИТ-сервисов и инфраструктуры; – Оптимизация и стандартизация ИТ бизнес-процессов; – Создание общей модели ИТ бизнес-процессов, включающей описание всех этапов и взаимосвязей между ними; – Разработка и актуализация единых регламентов по ИТ процессам управления эксплуатацией цифровых сервисов; – Обеспечение интеграции и согласованности ИТ процессов ГК; – Определение и документирование функциональных требований к ИТ-решениям и инфраструктуре; – Разработка модели финансирования ИТ-проектов, учитывающей распределение затрат между ДО, источники финансирования и механизмы контроля расходов;
График оплаты	Ежеквартально
Режим предоставления Услуги	В согласованный сторонами временной интервал
Соглашение об уровне оказания услуг	Время реакции: 1 ч. Время решения ЗНИ: по согласованию Сторон
Объем услуги	Количество конфигурационных единиц - в соответствии с составом и зоной охвата Объекта услуг. Количество Пользователей - не более 150 пользователей.
Порядок предоставления услуги	В соответствии с Приложением 4 к ТЗ
Штрафные санкции	При нарушении согласованных Сторонами сроков Заказчик вправе взимать с Исполнителя штраф в размере 0,01 % за каждый день просрочки, но не более чем 3 % от стоимости Услуги в отчетный период

Перечень передаваемых документов*

№ п/п	Наименование документа	Формат документа
1.	Инструкция по установке	электронный
2.	Инструкция по эксплуатации (Диагностика и устранение неисправностей, Мониторинг, Резервное копирование)	электронный
3.	Операционные инструкции пользователя	электронный
4.	Руководство администратора	электронный
5.	Описание настроек и доработок в том числе описание интеграции	электронный
6.	Загрузка организационной структуры	электронный
7.	Описание API	электронный
8.	Карточки мониторинга	электронный
9.	Описание режимов резервного копирования	электронный

* Перечень работ в составе Услуги и передаваемая документация могут быть изменены.

Порядок оказания Услуг

1. Общие положения

- 1.1. В настоящем документе (далее – Порядок) представлено описание порядка взаимодействия между сотрудниками Заказчика и сотрудниками Исполнителя в рамках оказания Услуг. Настоящий документ является неотъемлемым приложением к ТЗ.
- 1.2. В целях удобства понимания Порядка, под термином Заказчик понимается как организация Заказчика, так и пользователи Объекта Услуг Заказчика. Под термином Исполнитель понимается как организация Исполнителя, так и сотрудники Исполнителя, привлекаемые им для оказания Услуг.
- 1.3. Язык взаимодействия со Службой технической поддержки Исполнителя и ЕСПП, в том числе с использованием САСП – русский.

2. Термины, определения и сокращения

- 2.1. Термины, сокращения и определения приведены в соответствующем разделе ТЗ.

3. Обязанности Исполнителя

- 3.1. Исполнитель принимает и обрабатывает заявки Заказчика в целях оказания Услуг в соответствии с ТЗ.
- 3.2. Исполнитель использует для оказания Услуг САСП Заказчика. Поддержка работоспособности САСП осуществляется силами и за счёт Заказчика.
- 3.3. Исполнитель обрабатывает поступающие заявки Пользователей в САСП в соответствии с п.6 настоящего Порядка.
- 3.4. Исполнитель оказывает Услуги только по заявкам, если иное не указано в описании Услуг.
- 3.5. В случае привлечения Исполнителем к оказанию Услуг третьих лиц (других подрядных организаций), Исполнитель несет ответственность за их действия как за свои собственные.
- 3.6. Исполнитель несет ответственность за качественное оказание Услуг в соответствии с требованием настоящего ТЗ.
- 3.7. Исполнитель обязан качественно и корректно классифицировать обращения (Инцидент, ЗНО, ЗНИ).

4. Обязанности Заказчика

- 4.1. ЕСПП Заказчика регистрирует заявки пользователей в САСП и обеспечивает направление заявок на линию поддержки Исполнителя.
- 4.2. Заказчик по запросу Исполнителя обеспечивает предоставление Исполнителю всей необходимой информации и документации для оказания Услуг.

4.3. Заказчик при обращении в Службу технической поддержки Исполнителя руководствуется следующим принципом: направляемая в САСП заявка должна содержать запрос, который Исполнитель может решить в рамках одной Услуги. Если у Заказчика есть потребность в решении вопроса, соответствующего разным услугам или Объектам услуг, то Исполнитель вправе отказать в выполнении заявки с уведомлением Заказчику о необходимости направить данные вопросы отдельными заявками.

5. Ответственные лица

5.1. Для определения порядка взаимодействия, а также для распределения ответственности за полученный результат со стороны Заказчика и Исполнителя назначаются ответственные лица в соответствии с таблицей ниже.

Роль	Краткое описание
Руководитель проекта	Со стороны Заказчика. Осуществляет контроль качества предоставления Услуг
Сервис-Менеджер	Со стороны Исполнителя. Отвечает за решение вопросов, связанных с организацией предоставления Услуг
Основной инженер	Со стороны Исполнителя. Отвечает за решение вопросов, связанных с непосредственным оказанием Услуг

6. Обработка заявок

6.1. Общие положения

6.1.1. В настоящем Разделе приводятся основные принципы обработки заявок.

6.1.2. Основанием для оказания услуг Исполнителем является заявка, зарегистрированная в САСП.

6.1.3. Исполнитель обеспечивает следующую последовательность обработки заявки:

- после получения заявки на свою линию исполнения уточняет информацию по заявке (Объект Услуг, его компонент, услуга, прочая информация) и вносит ее в САСП;
- после уточнения данных по заявке назначает заявке приоритет и приступает к ее решению;
- обеспечивает решение заявок, зарегистрированных в САСП в установленные сроки в соответствии с требованиями, указанными в карточке Услуг;
- вносит в САСП информацию о состоянии решения заявок;

- при необходимости запрашивает дополнительную информацию у Заказчика, необходимую для решения заявки;
 - осуществляет мониторинг исполнения заявок и соответствующую эскалацию;
 - при необходимости привлечения специалистов Заказчика и/или других подрядных организаций Исполнитель самостоятельно контактирует с ними и осуществляет общую координацию действий при исполнении заявки;
 - информирует Заказчика о статусе и ходе работ по заявке по запросу;
 - обеспечивает отражение хода работ в САСП.
- 6.2. Регистрация, классификация и назначение обращения
- 6.2.1. Подача заявки осуществляется посредством отправки Заказчиком, инициирующим обращение, сообщения по электронной почте на адрес САСП или созданием заявки непосредственно в САСП.
- 6.2.2. Инициатором заявки является сотрудник Заказчика, который направил запрос в САСП. Взаимодействие по заявке происходит с инициирующим заявку сотрудником Заказчика, даже если он направил заявку от имени другого сотрудника.
- 6.2.3. Полученные заявки регистрируются в САСП Исполнителем. После регистрации заявки в САСП специалист ЕСПП заполняет необходимые атрибуты заявки и выполняет функциональную эскалацию на соответствующую характеру запроса линию исполнения.
- 6.2.4. Номер, дата регистрации, тема и описание заявки направляется Заказчику автоматически из САСП.
- 6.2.5. В случае нарушения сотрудником Заказчика принципа формирования заявки в САСП, описанного в п. 4.3 настоящего Порядка, специалист ЕСПП вправе отклонить некорректно составленную заявку, указав в комментарии рекомендации по разнесению комплекса вопросов по отдельным заявкам.
- 6.2.6. Заявка должна содержать следующую обязательную информацию:
- ФИО пользователя, организация пользователя, адрес электронной почты пользователя и его контактный телефон;
 - тема (наименование Объекта Услуг, по которому создается обращение, краткое изложение описания запроса);
 - подробное описание заявки:
 - О для Инцидентов:
 - фактический результат функционирования,
 - ожидаемый результат функционирования,
 - указание на способ воспроизведения сбоя,
 - текст ошибки (при наличии),
 - учётная запись, под которой получена ошибка;
 - О для ЗНО:
 - описание подробного запроса,
 - ожидаемый результат оказания услуги,
 - наличие предварительных согласований (при наличии);
- 6.2.7. К содержимому заявки могут быть приложены дополнительные материалы, которые могут быть полезны Исполнителю:
- скриншот (снимок с экрана), форматы файлов: jpg, gif, png;
 - текстовые и табличные документы с развернутым и / или наглядным описанием заявки;

- видеозапись, фиксирующая действия Пользователя, приводящие к ошибке.
- 6.2.8. Для каждой заявки Исполнитель указывает значения приоритета в соответствии с приведённой ниже таблицей:

Приоритет	Описание проблемы и влияние на бизнес
Критический	Критическое влияние на бизнес: Дальнейшая работа с функционалом Объекта Услуг невозможна. Объект Услуг не выполняет требуемые функции. Заказчик не может решить проблему самостоятельно. Проблемы данного уровня: - зависание или масштабный сбой Объекта Услуг; - повреждение данных Объекта Услуг; - недоступность критически важного функционала Объекта Услуг.
Высокий	Значительное влияние на бизнес: Логика работы функционала Объекта Услуг серьёзно нарушена. Существует обходное решение, но оно не очевидно для Заказчика, либо невозможно без специальных средств. Проблемы данного уровня: - значительный сбой Объекта Услуг.
Средний	Формальное влияние на бизнес: Незначительные проблемы, которые не влияют на функционирование Объекта Услуг и работу Заказчика. Проблемы данного уровня: - незначительный сбой Объекта Услуг; - запрос на обслуживание.
Низкий	Отсутствует влияние на бизнес: Обнаружение ошибок и проблем, не приводящих к остановке или деградации работы Объекта услуг или его компонентов.

6.2.9. Заказчик вправе запросить изменение приоритета заявки с предоставлением обосновывающих факторов или материалов. Специалист Службы технической поддержки производит оценку возможности изменения приоритета, принимает решение и уведомляет Заказчика о принятом решении.

6.3. Диагностика и решение заявки

6.3.1. После направления заявки на исполнение Исполнитель обязан:

- принять заявку в работу;
- провести первичный анализ;
- внести информацию о результатах анализа и планируемых мерах по исполнению заявки в САСП.

6.3.2. Исполнитель выполняет работы по заявке и вносит в САСП подробную информацию о ходе работ и полученном результате.

6.3.3. Исполнитель имеет право запросить у Заказчика дополнительную информацию, обоснованно необходимую для анализа и выработки методов решения заявки. При этом работы по анализу заявки могут быть приостановлены до момента получения запрошенной информации от Заказчика.

6.3.4. Время ожидания дополнительной информации не учитывается при подсчете времени исполнения заявки.

6.3.5. Если в течение 5 (пяти) рабочих дней с момента отправки Исполнителем запроса на предоставление уточняющих данных по заявке ответа от Заказчика не поступило, то такая заявка снимается с исполнения (отклоняется). При отклонении заявки Исполнитель добавляет обоснованный комментарий о невозможности обработки заявки, т.к. по ней не была представлена вся необходимая информация.

6.3.6. В случае необходимости привлечения служб Заказчика или его представителей для исполнения заявки, время ожидания ответа или исполнения такими службами не учитывается при подсчете времени выполнения заявки.

6.3.7. Исполнитель может предложить Пользователю временное решение, в случае если постоянное решение требует большее время реализации.

6.3.8. В случае если для решения заявки необходимо участие Заказчика или его подрядных организаций (например, для физической перезагрузки сервера, восстановления БД из резервной копии и т.д.), Исполнитель самостоятельно организует и координирует такие работы. Время исполнения заявки на стороне Заказчика и его подрядных организаций не учитывается при подсчете времени исполнения заявки.

6.3.9. Если в случае поступления заявки Исполнитель выясняет, что причиной возникновения описанной в ней проблемы является инфраструктурный инцидент на стороне Заказчика (незапланированная остановка работы аппаратного комплекса, снижение производительности или функциональности, т.е. сбой или отказ аппаратного ПО, а также в случае, если ошибка связана с функционированием системного либо базисного ПО), Исполнитель уведомляет об этом Менеджера по контролю качества оказания услуг Заказчика, делает соответствующий комментарий, после окончания работ на стороне Заказчика – проверяет работу Объекта Услуг и закрывает заявку. Время исполнения заявки на стороне Заказчика и его подрядных организаций не учитывается при подсчете времени исполнения заявки.

6.3.10. Если с целью исполнения заявки Исполнителем установлена необходимость выполнения дополнительных работ, входящих в состав другой Услуги, ему необходимо проинформировать Заказчика и продолжить исполнение заявки, при необходимости создать дополнительные запросы от имени Заказчика самостоятельно или получить ее от Заказчика. В случае, когда от Заказчика требуется согласование выполнения работ, такое согласование запрашивается через

автоматизированные средства оповещения САСП, а работы приостанавливаются до момента получения результата согласования от Заказчика.

6.4. Закрытие заявок

6.4.1. После завершения работ по заявке Исполнитель вносит соответствующую информацию в САСП и переводит заявку в статус завершения работ.

6.4.2. Заказчик, получив уведомление о завершении работ по заявке, должен выполнить проверку результата выполнения работ по заявке. Если результат устраивает Заказчика, то он принимает работы по заявке. В противном случае он отклоняет работы по заявке.

6.4.3. Если работы отклонены, и заявка возвращена на исполнение, то такая заявка считается опротестованной и исполнение работ по ней начинается заново.

6.4.4. Срок работ по опротестованной заявке согласуется Сторонами в рабочем порядке.

6.4.5. Заявка, выполнение которой согласовано или результаты работ приняты, считается выполненной и закрытой.

6.4.6. Если Пользователь, направивший заявку, не принял и не отклонил работы по заявке, то по истечению 5 (пяти) рабочих дней Заявка считается закрытой.

6.4.7. Срок исполнения заявок рассчитывается как разность между временем получения Исполнителем заявки на исполнение и временем последнего перевода заявки Исполнителем в статус завершения работ.

7. Уведомление Заказчика

7.1. При проведении работ, связанных с полной или частичной недоступностью функций ИС, Специалист Службы технической поддержки уведомляет Заказчика о проведении таких работ одним из следующих способов на свое усмотрение:

- Уведомление по электронной почте путем рассылки информации о недоступности ИС в адрес Менеджера по контролю качества оказания услуг;
- Уведомление путем сообщения, выдаваемого пользователям при попытке использования ИС;
- Уведомление путем телефонного звонка;
- Уведомление путем рассылки сообщений посредством мессенджера или SMS.

Правила информационной безопасности

1. Общие сведения

1.1. Термины, сокращения и определения приведены в соответствующем разделе ТЗ.

1.2. Цель документа

1.2.1. Документ определяет правила работы с информацией конфиденциального характера, правила безопасной работы на объектах критической информационной инфраструктуры, действия при возникновении компьютерных инцидентов и иных нештатных ситуаций Исполнителя.

1.3. Корпоративный центр кибербезопасности

1.3.1. У Заказчика действует Корпоративный центр кибербезопасности по организации процессов обнаружения, предотвращения, а также реагирования на компьютерные атаки в отношении объектов критической информационной инфраструктуры.

2. Общие положения

2.1. Субъектами, на которые распространяется действие Правил, являются работники Исполнителя, привлеченные им подрядные организации и физические лица, задействованные в оказании Услуг (далее по тексту – Работники).

2.2. Объектами защиты в контексте обеспечения безопасности информационной инфраструктуры Заказчика и информации конфиденциального характера являются:

- корпоративные информационные системы (в том числе машинные носители информации, автоматизированные рабочие места, серверы, средства обработки буквенно-цифровой, графической, видео- и речевой информации, микропрограммное, общесистемное, прикладное программное обеспечение), обеспечивающие устойчивость финансово-хозяйственной деятельности;
- автоматизированные системы управления (в том числе автоматизированные рабочие места, промышленные серверы, программируемые логические контроллеры, производственное, технологическое оборудование (исполнительные устройства), имеющее функции как локального, так и дистанционного управления, либо имеющее функционирующие интерфейсы сетевого взаимодействия, микропрограммное, общесистемное, прикладное программное обеспечение), обеспечивающие надежное снабжение потребителей электроэнергией;
- корпоративные и технологические информационно-телекоммуникационные сети (в том числе телекоммуникационное оборудование, программное обеспечение, система

управления, линии связи), формирующие единое информационное пространство и цифровую среду взаимодействия;

- цифровые устройства и периферийное оборудование (в том числе принтеры, сканеры, ip-телефоны, цифровые камеры, смартфоны);
- сети электросвязи, используемые для организации взаимодействия объектов и передачи информации, места выхода в сеть Интернет;
- архитектура и конфигурация информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, информация (данные) о параметрах (состоянии) управляемого (контролируемого) объекта или процесса (в том числе входная (выходная) информация, управляющая (командная) информация, контрольно-измерительная информация, персональные данные, иная информация конфиденциального характера, в том числе представляющая коммерческую ценность в силу неизвестности третьим лицам.

2.3. Работники обязаны неукоснительно соблюдать настоящие Правила при работе с информационными системами, автоматизированными системами управления, информационно-телекоммуникационными сетями, включая их элементы (автоматизированные рабочие места, серверы, коммутационное, сетевое и иное оборудование), а также при работе с информацией конфиденциального характера.

3. Правила безопасной работы на объектах критической информационной инфраструктуры

3.1. Работникам запрещено:

- 1) осуществлять фото- и видеосъемку экранов АРМ, офисных помещений, мест расположения средств вычислительной техники в случае, если данные действия не являются необходимыми для выполнения трудовых функций, закрепленных в должностной инструкции Работника;
- 2) осуществлять скрытую аудио- и видеозапись совещаний и переговоров;
- 3) выбрасывать информацию в печатном виде в мусорные корзины (бумажные носители должны уничтожаться с применением устройств по измельчению бумаги («шредер»);
- 4) выполнять печать и сканирование документов с конфиденциальной информацией на общедоступных МФУ (расположенных в коридорах, залах, рекреациях, иных местах и помещениях, в которые возможен неконтролируемый доступ посторонних лиц);
- 5) обсуждать сведения, относящиеся к конфиденциальной информации, в присутствии третьих лиц или в местах, где такая информация может быть услышана третьими лицами;
- 6) оставлять бумажные или электронные носители с информацией в переговорных комнатах и других общедоступных местах, включая общедоступные МФУ;
- 7) осуществлять попытки самостоятельного внесения изменений в настройки операционных систем и параметров безопасности средств защиты информации, установленных на АРМ.

3.2. Работник обязан незамедлительно сообщать в Подразделение ИБ Заказчика по электронной почте ib@fskees.ru или телефону 7 (495) 748-55-00 (доб. 5123) информацию о следующих фактах:

- при выявлении подозрительной активности на АРМ;

- при выявлении вирусной активности;
 - при утрате носителей служебной информации и мобильных АРМ (ноутбук, планшет, смартфон);
 - при раскрытии парольной информации;
 - при утрате или компрометации носителей сертификатов ключа проверки электронной подписи (ключевых носителей);
 - в случае обнаружения неопознанных ключевых носителей, носителей информации;
 - в случае обнаружения неопределенных технических средств (устройств) несанкционированное подключенных к АРМ, ЛВС;
 - в случае обнаружения уязвимостей в любых элементах АРМ, серверов, ЛВС, информационных систем и автоматизированных систем управления;
 - в случае обнаружения ошибок в настройке и работе информационных систем и автоматизированных систем управления, сетей связи, приводящих к доступу в области, не предусмотренной изначальной заявкой на доступ;
 - в случае обнаружения в открытом доступе в любом виде учетных данных (паролей и имен пользователей);
 - при обнаружении несанкционированного доступа других лиц к информации или АРМ;
 - в случаях попыток получения парольной информации третьими лицами;
 - в случаях прекращения работоспособности средств защиты информации.
- 3.3. Все оборудование, имеющее интерфейсы сетевого взаимодействия, должно быть закреплено за работниками.

4. Правила работы с учетными записями

4.1. Заказчик использует 3 типа учетных записей:

- «пользователь»;
- «администратор»;
- «сервисная».

4.2. Доступ к АРМ, корпоративному персонифицированному ящику электронной почты, сетевым папкам и сети Интернет для Исполнителя предоставляется по заявке руководителя структурного подразделения Заказчика (куратора соглашения, договора) в САСП после согласования заявки с Подразделением ИБ.

4.3. Создание учетной записи типа «Администратор» и «Сервисная», повышение уровня доступа существующей учетной записи осуществляется по согласованию с Подразделением ИБ.

4.4. Все учетные записи должны быть персонифицированы, за исключением случаев, когда необходимость работы под обезличенной учетной записью обусловлена техническими требованиями информационной системы, автоматизированной системы управления или оборудования информационно-телекоммуникационной сети.

4.5. В случае необходимости использования одной учетной записи несколькими работниками, подразделением – владельцем информационной системы должен быть разработан и утвержден ОРД перечень лиц, допущенных к работе в информационной системе (автоматизированной системе управления, оборудования информационно-телекоммуникационной сети) под указанной учетной записью.

4.6. Учетные записи, неиспользовавшиеся в течение 4 месяцев, должны быть автоматически заблокированы.

4.7. В случае прекращения трудовых отношений с Работником, учетные записи, принадлежащие работнику, должны быть заблокированы.

4.8. Разблокирование учетных записей, сброс пароля на действующих учетных записях, предоставление доступа к учетной записи уволенного работника, иные действия с учетными записями осуществляются по согласованию с Подразделением ИБ.

4.9. В случае применения механизмов двухфакторной аутентификации с использованием связанного с учетной записью телефонного номера, номер, используемый для получения второго фактора, должен принадлежать Работнику или быть закрепленным за Работником.

5. Правила работы с паролями

5.1. Требования к сложности пароля:

- строчные латинские буквы: abcd...xyz;
- прописные латинские буквы: ABCD...XYZ;
- цифры: 123...90;
- специальные символы: !%()+ и т.д.

5.2. Пароли не должны основываться на типовых шаблонах и идущих подряд на клавиатуре или в алфавите символов (qwerty, 1234567, abcdefgh и т.д.), а также не должны основываться на каком-либо одном слове, выданном идентификаторе, имени, кличке, паспортных данных, номерах страховок.

5.3. Требования к длине пароля:

- для работников с правами «пользователя» длина пароля должна составлять не менее 8 символов;
- для работников с правами «администратора» (локального / доменного) длина пароля должна составлять не менее 15 символов;
- для «сервисных» идентификаторов, разделяемых ключей (shared keys) длина пароля должна составлять не менее 14 символов;
- для SNMP Community Strings длина пароля должна составлять не менее 10 символов.

5.4. Периодичность обязательной смены пароля:

- административных учетных записей - каждые 60 дней;
- пользовательских учетных записей - каждые 90 дней;
- сервисных учетных записей - не реже двух раз в год;
- shared keys SNMP Community Strings - не реже одного раза в год.

5.5. Пароли не должны храниться и передаваться в незашифрованном виде по публичным сетям (локальная вычислительная сеть, интернет, электронная почта).

5.6. В ходе работы не должны использоваться пароли по умолчанию. Должны быть назначены пароли, отличные от установленных производителем.

5.7. При компрометации пароля, владелец учетной записи должен незамедлительно сменить все пароли.

5.8. При использовании паролей запрещено:

- хранить и записывать пароли на бумаге, и том числе на предметах, а также в местах, доступных третьим лицам;
- хранить и записывать пароли в электронном виде без использования криптографической защиты;
- передавать и сообщать третьим лицам личный пароль (за исключением случаев хранения руководителями или ответственными работниками подразделений паролей в соответствии с обязанностями, указанными в положении о подразделении и(или) должностных инструкциях);
- регистрировать третьих лиц под своим паролем;
- передавать парольные фразы пользователям при помощи почтовых сообщений либо иным открытым способом через Интернет без использования парольной или криптографической защиты;
- вводить свой пароль в случае, если он может быть просмотрен случайно или намеренно третьими лицами;
- использовать одни и те же пароли для разных информационных систем (автоматизированных систем управления, оборудования информационно-телекоммуникационной сети);
- создавать учетные записи, профили на сторонних интернет-сервисах и информационных системах (включая общедоступные сервисы электронной почты) с использованием пароля от корпоративного АРМ.
- использовать функцию «Запомнить пароль» в программном обеспечении.

5.9. В случае отсутствия технической возможности использования паролей, соответствующих требованиям настоящего раздела, требования к паролям устанавливаются на этапе проектирования или разработке эксплуатационной документации на ИС, ИТС.

6. Правила работы на АРМ

6.1. Работники должны обладать необходимыми навыками работы с используемым аппаратным и программным обеспечением.

6.2. В случае необходимости организации АРМ для Исполнителя, АРМ создается по обращению руководителя структурного подразделения Заказчика, куратора соглашения, договора после согласования с Подразделением ИБ.

6.3. К ИТС Заказчика запрещено подключать личные средства вычислительной техники (персональный компьютер, ноутбук, смартфон, планшет, модем, роутер, точку доступа, ip видеокамеру, цифровую приставку для ТВ и т.д.) в том числе с целью зарядки, передачи файлов и т.д.

6.4. Доступ Работника к АРМ осуществляется:

- с применением персональной доменной учетной записи;
- с применением локальной персонифицированной или общей учетной записи;
- с применением средств защищенного удаленного доступа.

6.5. Использование локальных учетных записей допускается:

- в случаях, предусмотренных эксплуатационной или проектной документацией на эксплуатируемую систему;
- в случаях проведения работ по техническому обслуживанию АРМ (для работников технической поддержки);
- в отдельных случаях, после получения согласования со стороны Подразделения ИБ.

6.6. Удаленное подключение к АРМ допускается:

- в случаях, предусмотренных эксплуатационной или проектной на эксплуатируемую систему;
- в случаях введения приказом Заказчика удаленного режима работы, за исключением подключения к АРМ, входящих в состав автоматизированных систем управления, иных технологических систем;
- в отдельных случаях, после получения согласования со стороны Подразделения ИБ.

6.7. Все АРМ (включая мобильные и виртуальные) должны быть оснащены средствами антивирусной защиты.

6.8. Доступ к настройкам BIOS АРМ, настройкам МФУ, сетевого и коммутационного оборудования должен быть заблокирован паролем.

6.9. При организации защищенного удаленного доступа к АРМ или информационным системам с использованием механизмов двухфакторной аутентификации посредством отправки SMS-кодов не допускается использование телефонных номеров, принадлежащих третьим лицам, в том числе родственникам или знакомым работника, коллегам.

6.10. Организация удаленного подключения подрядных организаций к корпоративным АРМ осуществляется по согласованию с Подразделением ИБ.

6.11. По окончании сеанса работы на АРМ или при необходимости оставления рабочего места Работник должен заблокировать экран средств вычислительной техники (блокирование экрана на персональном компьютере осуществляется нажатием сочетания клавиш Win + L или нажатием сочетания клавиш Ctrl + Alt + Del и выбором опции «Блокировать компьютер»).

6.12. При работе на АРМ запрещено:

- эксплуатировать средства вычислительной техники при отключенных или неустановленных средствах антивирусной защиты и встроенных в операционную систему средствах обеспечения безопасности (MS Windows Defender);
- оставлять рабочее место без блокирования экрана средств вычислительной техники;
- использовать АРМ в нерабочее время не по прямому назначению;
- осуществлять работу на АРМ, не удовлетворяющих требованиям информационной безопасности;
- допускать к работе на своем АРМ третьих лиц, за исключением работников службы технической поддержки и работников Подразделения ИБ;
- срывать пломбы или печати, вскрывать корпус персонального компьютера, осуществлять самостоятельную сборку и разборку средств вычислительной техники;
- использовать уязвимости и недокументированные возможности установленного ПО;
- вносить изменения в аппаратную и программную конфигурацию АРМ;
- хранить личную, не имеющую отношения к выполнению должностных обязанностей, информацию на АРМ и сетевых ресурсах;
- производить загрузку АРМ с внешних и сетевых носителей;
- получать доступ к BIOS или UEFI персонального компьютера;
- использовать АРМ с локальными учетными записями;
- препятствовать работе средств защиты информации или обходить их;
- самостоятельно подключать к АРМ периферийные и внешние устройства, в том числе:
 - принтеры, сканеры и multifunctional устройства;
 - модемы и адаптеры связи;
 - мобильные телефоны, планшеты и другие подобные устройства;
 - личные носители информации;
 - устройства двойного назначения - скрывающие встроенный функционал.
- использовать АРМ с одновременным подключением к ЛВС и другим сетям;
- оставлять средства вычислительной техники (ноутбук, смартфон, планшет) в общедоступных местах без присмотра;
- осуществлять подключение (проводное или беспроводное) к АРМ личных мобильных устройств (смартфон, планшет, модем или другие внешние устройства), в том числе с целью зарядки;
- производить самостоятельное удаление / установку программного обеспечения на АРМ.

6.13. При увольнении Работника информация на жестком диске персонального компьютера Работника и сетевых ресурсах подлежит передаче непосредственному руководителю Работника, после чего персональный компьютер и другие средства вычислительной техники, полученные работником, должны быть сданы в структурное подразделение, осуществляющее выдачу средств вычислительной техники.

6.14. При приемке АРМ уволенного Работника должна быть выполнена процедура удаления информации и установлена новая копия операционной системы и прикладного ПО.

6.15. При передаче средств вычислительной техники в ремонт, в иных случаях передачи средств вычислительной техники третьим лицам (включая списание и утилизацию) жесткие диски должны быть демонтированы.

6.16. Передача средств вычислительной техники с жесткими дисками, передача жестких дисков в ремонт осуществляется после согласования с Подразделением ИБ.

6.17. При списании, утилизации жестких дисков, иных носителей информации должна быть выполнена процедура удаления информации без возможности её восстановления.

6.18. Физический доступ в помещения с АРМ должен обеспечиваться с использованием средств контроля и управления доступом или иными способами контроля, позволяющими исключить несанкционированным доступ в помещение посторонних лиц.

6.19. Доступ в помещения с АРМ, серверные и кроссовые помещения, иные помещения с размещенными элементами информационной инфраструктуры Исполнителю (в том числе с целью оказания Услуг, выполнения работ по техническому обслуживанию, проведения аудита, прохождения стажировки и т.д.), предоставляется по согласованию с подразделением, ответственным за обеспечение безопасности и режима.

6.20. Доступ в помещения с АРМ, серверами, коммутационным оборудованием осуществляющими обработку информации технологического характера (в том числе информации о значимых объектах критической информационной инфраструктуры) третьим лицам предоставляется только при непосредственном сопровождении представителя Заказчика, ответственного за эксплуатацию или обеспечение безопасности информационной инфраструктуры.

6.21. При завершении договора на оказание Услуг Исполнитель обязан гарантированно удалить всю информацию Заказчика, ставшую известной ему в связи с оказанием Услуг, с АРМ Работников.

7. Правила работы с информационными системами

7.1. При работе с информационными системами (автоматизированными системами управления, оборудовании информационно-телекоммуникационной сети) запрещено:

- использовать уязвимости и недокументированные возможности программного и аппаратного обеспечения;
- использовать (в любых целях) ошибки системы;
- осуществлять деструктивные воздействия на программное обеспечение и данные в информационных системах (автоматизированных системах управления);
- несанкционированно изменять или уничтожать данные в информационных системах

или на внешних (отчуждаемых) носителях;

- несанкционированно устанавливать на автоматизированные рабочие места любые дополнительные программные и аппаратные компоненты и устройства;
- осуществлять доступ под чужими учетными данными;
- выполнять резервное копирование информации на личные носители, облачные сервисы, внешние сервисы электронной почты;
- публиковать в открытом доступе информацию об архитектуре и конфигурации корпоративных и технологических информационно-телекоммуникационных сетей, сетей электросвязи, используемых для организации взаимодействия объектов и передачи информации, в том числе для выхода в сеть «Интернет».

7.2. При работе с технологическими системами (в том числе автоматизированными системами управления) Работник должен уделять особое внимание безопасности информации.

7.3. Порядок работы с технологическими системами указывается в эксплуатационной или проектной документации на данные системы.

8. Правила работы в ЛВС

8.1. Работнику для выполнения служебных обязанностей предоставляется доступ в ЛВС со стационарного АРМ.

8.2. Удаленный доступ к внутрикорпоративным web-сервисам и информационным системам, в том числе с использованием сторонних средств вычислительной техники, должен осуществляться через «единое окно» по защищенному каналу связи с применением средств терминального доступа или VPN шлюза по протоколу HTTPS с применением двухфакторной аутентификации, в том числе с применением персональных сертификатов, выдаваемых удостоверяющим центром Заказчика.

8.3. К средствам вычислительной техники (персональный компьютер, ноутбук, планшет), с которых осуществляется удаленный доступ к информационным системам, в том числе к корпоративным АРМ, применяются все требования настоящих Правил.

8.4. В случае осуществления удаленного или локального доступа к ЛВС Заказчика с АРМ Исполнителя, доступ предоставляется только при условии соблюдения требований настоящих Правил работниками, а также при наличии в указанном соглашении / договоре ответственности за нарушение требований настоящих Правил. При этом АРМ указанной организации должны удовлетворять требованиям Правил.

8.5. При работе в ЛВС без предварительного согласования с Подразделением ИБ не допускается:

- устанавливать удаленный доступ к АРМ и ЛВС, подключать любые устройства к

ЛВС;

- осуществлять доступ к ЛВС с личных устройств;
- осуществлять сетевой доступ к другим АРМ;
- подключать средства вычислительной техники, имеющие встроенные и внешние устройства беспроводной связи к ЛВС;
- подключать АРМ к беспроводным сетям.

8.6. При работе в ЛВС запрещено:

- подключать к ЛВС средства вычислительной техники с отключенными или неустановленными средствами защиты, а также с настройками, неудовлетворяющими требованиям информационной безопасности;
- проводить сканирование и анализ ЛВС и сетевых узлов;
- осуществлять перехват трафика в ЛВС;
- осуществлять атаки на АРМ, ЛВС, серверы, коммутационное и иное оборудование, включая информационные системы и автоматизированные системы управления;
- использовать уязвимости протоколов и конфигураций сетевого оборудования в ЛВС;
- организовывать точки входа и шлюзы для внешних сетей;
- создавать точки беспроводного доступа на территории Заказчика.

9. Правила работы в сети Интернет

9.1. Доступ к ресурсам сети Интернет предоставляется Работникам для выполнения ими трудовых функций.

9.2. Подразделение ИБ постоянно поддерживает в актуальном состоянии список запрещенных Интернет-ресурсов и блокирует доступ к ним на различных уровнях.

9.3. При работе в сети Интернет запрещено:

- обходить механизмы фильтрации запрещенных Интернет-ресурсов с помощью специализированных интернет-сервисов (анонимайзеры, прокси-серверы, VPN-серверы);
- организовывать туннелирование внешних сетей;
- переходить по баннерам и рекламным объявлениям;
- переходить по подозрительным ссылкам;
- использовать ресурсы:
 - непристойного содержания;
 - не связанных с исполнением трудовых функций Работников;
 - нарушающих требования действующего законодательства;
- распространять информацию, запрещенную законодательством Российской Федерации, включая материалы террористического, национального, расистского, сексуального, религиозного, развлекательного и другого характера, а также информацию, оскорбляющую честь, достоинство и деловую репутацию юридических и физических лиц;
- игнорировать системные сообщения АРМ и предупреждения об ошибках;
- несанкционированно размещать от имени Заказчика любую информацию, в том числе публиковать информацию в социальных сетях, Интернет-мессенджерах, форумах;

- использовать внешние адреса электронной почты для ведения служебной переписки;
- публиковать в сети Интернет корпоративные адреса электронной почты и телефонов Заказчика;
- приобретать, хранить и распространять информацию, запрещенную законодательством, или способную причинить вред имиджу Заказчика или нанести материальный ущерб Заказчику;
- предпринимать самостоятельные действия по устранению неполадок при подключении к сети Интернет при их возникновении;
- осуществлять работу в сети Интернет с использованием учетных записей с административными правами доступа;
- использовать ресурсы¹:
 - игрового и развлекательного характера;
 - социальных сетей;
 - пиринговых сетей;
 - почтовых сервисов;
 - файлообменных сервисов и облачных хранилищ, за исключением файлообменных сервисов Заказчика;
 - форумов и конференций (в части публикации сообщений);
 - сервисов коммуникаций (Telegram, WhatsApp, Instagram, Skype (за исключением корпоративной версии) и иных сервисов), за исключением случаев, когда использование такого сервиса необходимо в рамках исполнения должностных обязанностей в соответствии с положением о структурном подразделении и(или) должностной инструкцией;
 - сервисов видеотелефонной связи (Zoom, Google Meet, TrueConf и др.) за исключением использования корпоративных версий указанного программного обеспечения в рамках исполнения должностных обязанностей;
 - удаленных АРМ, находящихся за пределами ЛВС, способами, выходящими за рамки утвержденных проектных решений, в том числе с использованием программ удаленного доступа (rAdmin, TeamViewer и др.);
- снижать установленный уровень защиты информации;
- сохранять и запускать файлы, полученные из сети Интернет, за исключением случаев, когда использование таких файлов необходимо в рамках исполнения должностных обязанностей в соответствии с положением о структурном подразделении и(или) должностной инструкцией.

9.4. Не допускается организация подключения к сети Интернет на АРМ и серверах технологического сегмента.

10. Правила работы с электронной почтой

¹ Для получения исключительного доступа в случае производственной необходимости, необходимо сформировать в службу технической поддержки заявку на получение доступа с обоснованием необходимости использования данных сервисов и согласовать эту заявку с подразделением ИБ.

10.1. Доступ к корпоративной электронной почте предоставляется Работникам только в целях исполнения трудовых функций.

10.2. Вся служебная переписка должна осуществляться только с использованием персонального адреса корпоративной электронной почты.

10.3. Работник должен проверять вложения в сообщениях электронной почты на наличие исполняемых файлов, при их наличии - не запускать исполняемый файл и сообщить о получении такого письма в службу технической поддержки Service Desk. Рекомендуется открывать только вложения, имеющие следующий формат: документы (Word, Excel, PDF, txt и т.д.), изображения (JPG, PNG и т.д.).

10.4. Рекомендуется подтверждать отправку отправителем писем.

10.5. При работе с электронной почтой запрещено:

- осуществлять массовую и адресную рассылку информации, не связанной со служебной необходимостью (спам);
- направлять конфиденциальную информацию без применения средств криптографической защиты информации по открытым (незащищенным) каналам передачи данных, в том числе через сети общего пользования и сеть Интернет;
- использовать любые другие сервисы электронной почты кроме корпоративных, если иное не предусмотрено исполнением должностных обязанностей;
- снижать установленный уровень защиты информации сообщений;
- открывать письма, поступившие от неизвестных адресатов с неизвестными вложениями;
- переходить по внешним ссылкам, указанным в электронных письмах, в случае если получение такого письма не связано с выполнением должностных обязанностей;
- осуществлять рассылку сообщений, не имеющих отношения к выполнению должностных обязанностей.
- регистрировать учетные записи, профили на сторонних Интернет-ресурсах (включая социальные сети) с указанием адресов электронной почты Заказчика, за исключением случаев, связанных с выполнением должностных обязанностей.

10.6. При получении массовой рассылки от подразделения ИБ Работники обязаны усилить бдительность к получаемой электронной почте.

10.7. При получении подозрительного письма Работник должен:

- при получении письма сомнительного содержания и/или от неизвестного пользователя с вложением не открывать его, в случае открытия - не открывать вложения, не переходить по указанным в письме ссылкам;
- при случайном открытии письма и подозрительном поведении АРМ, запрещается отключать АРМ от питания;
- сообщить в подразделение ИБ о факте получения и открытия вложения подозрительного письма;
- выполнить следующие действия при подтверждении, что данное письмо является SPAM-рассылкой:
 - нажать на данное письмо правой кнопкой мыши;
 - выбрать пункт нежелательная почта;

- выбрать пункт заблокировать отправителя.

11. Правила работы с носителями информации

11.1. Использование внешних носителей информации «по умолчанию» не допускается.

11.2. При необходимости использования внешнего носителя для записи (копирования) информации на корпоративном АРМ Работником должна быть направлена заявка в САСП с описанием причин такой необходимости.

11.3. Работники подразделения ИБ могут блокировать порты подключения внешних носителей информации в случаях нарушения Работником требований при работе с носителями информации, при угрозе распространения вредоносного программного обеспечения, иных случаях, связанных с рисками нарушения конфиденциальности, целостности и доступности информации.

11.4. В случае использования внешнего носителя для передачи конфиденциальной информации, такой носитель должен быть промаркирован, а вся информация на носителе должна быть зашифрована. При шифровании должны использоваться криптоалгоритмы, разрешенные к применению на территории Российской Федерации.

11.5. Учет и маркировка носителей, содержащих конфиденциальную информацию (в том числе персональные данные), осуществляется уполномоченным работником структурного подразделения Заказчика, осуществляющего обработку данной информации.

11.6. По достижению целей обработки информации (в том числе - конфиденциальной) на носителе, вся информация на носителе должна быть уничтожена без возможности её восстановления.

11.7. Подключение внешних носителей информации к ИС, АРМ и серверам (в том числе коммутационному оборудованию) допускается только для работников, осуществляющих эксплуатационную и техническую поддержку указанного оборудования. Используемый носитель информации должен быть промаркирован и подлежать учету.

11.8. В случае необходимости подключения внешнего носителя информации к АРМ или серверам, размещенным в технологическом сегменте и не оснащенных средствами антивирусной защиты, необходимо предварительно выполнить проверку носителя на отдельном (изолированном от технологического сегмента и сети Интернет) АРМ, с установленным АВПО с актуальными антивирусными базами.

11.9. При работе с носителями информации запрещено:

- несанкционированно подключать и использовать внешние носители информации как к АРМ и серверам, так и к другому оборудованию;
- подключать личные носители информации к АРМ;

- использовать корпоративные носители информации Заказчика в личных целях, в том числе для удаленной работы на личных персональных компьютерах.

12. Правила работы с носителями ключевой информации

12.1. Заказчик применяет следующие виды ключевой информации:

- усиленная квалифицированная электронная подпись;
- неквалифицированная электронная подпись.

12.2. Неквалифицированная электронная подпись используется для:

- шифрования информации, в том числе сообщений электронной почты;
- организации доступа к информационным системам Заказчика;
- организации защищенного удаленного доступа;
- иных случаях, предусмотренных ОРД Заказчика.

12.3. Выпуск сертификатов ключа проверки электронной подписи осуществляется в порядке, предусмотренным соответствующим ОРД Заказчика.

12.4. При работе с носителями сертификата ключа проверки электронной подписи (токенами) не допускается:

- извлечение закрытого ключа из контейнера;
- передача носителя и(или) пароля на контейнер третьим лицам;
- использование чужих носителей сертификата ключа проверки электронной подписи;
- оставление носителя в АРМ по окончании сеанса работы с электронной подписью за исключением случаев, когда постоянное присутствие носителя обусловлено требованиями информационной системы и/или эксплуатационной документацией на информационную систему.

12.5. При прекращении трудовых отношений Работник должен сдать имеющиеся у него носители сертификата ключа проверки электронной подписи в Подразделение ИБ.

Формы отчётных документов (общие)

Форма 1. Сводный отчёт по объёму оказанных Услуг

за период с ____ по ____

Отчет должен формироваться на основании данных САСП.

№ п/п	Наименование ИС	Наименование Услуги	Объём оказанных Услуг, шт.	*Объём Услуг с отклонением от уровня оказания Услуг, шт.	**Штрафные санкции по Услуге, %
1					
2					
3					

* Подсчитывается на основании Детального отчета по заявкам.

** Определяется на основании Соглашений об уровне оказания услуг для каждой Услуги (нарушение исполнения заявок, снижение доступности, ИБ-инциденты).

ЗАКАЗЧИК

ИСПОЛНИТЕЛЬ

_____/_____/

_____/_____/

М.П.

М.П.

Форма 2. Детальный отчёт по заявкам Пользователей
за период с ____ по ____

Отчет должен формироваться на основании данных САСП.

№ п/п	Тип заявки	Номер заявки	Тема заявки	Получатель	Наименование ИС	Комплексная услуга	Услуга	Операция/Работа	Сервис	Дата и время регистрации	Дата и время назначения на Исполнителя	Дата и время решения	Дата закрытия	*Нарушение Соглашения
1														ДА / НЕТ
2														ДА / НЕТ

* Указывается на основании Соглашений об уровне оказания услуг для каждой Услуги (нарушение сроков, опротестованные заявки, фиктивные).

ЗАКАЗЧИК

ИСПОЛНИТЕЛЬ

_____/_____
М.П.

_____/_____
М.П.