ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«ИРКУТСКАЯ НЕФТЯНАЯ КОМПАНИЯ»

Приложение

УТВЕРЖДЕНО
Приказом ООО «ИНК»
от 06 июля 2023 г.
№ 1750/00-п

Введен в действие с
06 июля 2023 г.

СТАНДАРТ

ТРЕБОВАНИЯ ЗАКАЗЧИКА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

СТ.02.74

Редакция 1

Иркутск
2023

ООО «ИНК»

Паспорт документа

Процесс	Управление информационной безопасностью
Владелец процесса	Начальник службы информационной безопасности и технических средств охраны
Подразделение-разработчик	Отдел информационной безопасности
Разработчик (ФИО, должность)	Васильева В. М., руководитель группы аудита и методологии отдела информационной безопасности
Ответственный за актуализацию (должность)	Начальник отдела информационной безопасности
Область распространения	ООО «ИНК», Дочерние общества и юридические лица, заключившие с ООО «ИНК» Соглашение о взаимодействии, Общества, которые являются или потенциально могут стать контрагентами ООО «ИНК»
Введен (впервые/взамен)	Впервые
Настоящий внутренний нормативно-методический документ является интеллектуальной собственностью Общества с ограниченной ответственностью «Иркутская нефтяная компания». Любые права в отношении настоящего внутреннего нормативного-методического документа, включая исключительные права в связи с его разработкой, переработкой, распространением, использованием любым иным образом, в соответствии с законодательством РФ принадлежат ООО «ИНК».	

Информация о предыдущих редакциях документа

№ редакции	Краткое описание изменений по сравнению с предыдущей редакцией

Содержание

1 Общие положения

1.1 Назначение документа

1.1.1 Настоящий Стандарт «Требования Заказчика в области информационной безопасности» устанавливает общие требования к Контрагентам/Субподрядчикам при подключении к информационным системам Заказчика и/или использования иных информационных сервисов Заказчика, в части обеспечения информационной безопасности, а именно сохранение конфиденциальности, целостности и доступности информационных активов, обеспечения непрерывности бизнес- и производственных процессов за счёт применения процессов управления информационной безопасностью.

1.1.2 Целью настоящего Стандарта являются:

- обеспечение непрерывности и безопасности бизнес- и производственных процессов Заказчика;
- обеспечение конфиденциальности, целостности и доступности информации, обрабатываемой в информационных системах Заказчика;
- минимизация вероятности реализации угроз безопасности и потенциального ущерба от реализации угроз;
- защита и поддержание позитивного имиджа и деловой репутации Заказчика.

1.1.3 Требования настоящего Стандарта распространяются на Контрагентов и Субподрядчиков, которые для выполнения своих обязательств в интересах Заказчика подключаются к информационным системам Заказчика или используют информационные сервисы Заказчика.

1.1.4 Стандарт не отменяет и не заменяет существующие нормы законодательства РФ и государственные нормативные требования (далее–действующее законодательство) в области осуществления навигационной деятельности, но дополняет и детализует дополнительные требования Заказчика.

1.1.5 В случае возникновения расхождений или противоречий между положениями настоящего Стандарта и действующим законодательством в отношении использования и толкования настоящего Стандарта преимущественную силу имеют положения норм действующего законодательства.

1.2 Термины и определения

Термин	Определение
Заказчик	ООО «ИНК» и Общества
Информационная безопасность	состояние защищенности информации, при котором обеспечивается ее конфиденциальность, целостность и доступность
Информационная система	совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств

Информационная система Заказчика	совокупность информационных систем Заказчика, используемых для обработки информационных ресурсов, включая корпоративные информационные системы, системы электронного документооборота, автоматизированные системы управления технологическими процессами и технологические сети связи
ИТ-сервис, информационный сервис	совокупность программно-аппаратных средств, необходимых для предоставления пользователю определённой функциональности
Конфиденциальность информации	обязательное для выполнения лицом, получившим доступ к определённой информации, требование не передавать такую информацию третьим лицам без согласия ее владельца.
Куратор	представитель Заказчика, назначенный руководителем подразделения Заказчика, осуществляющий контроль за выполнением работ или оказанием услуг согласно договору
Общества	дочерние Общества и юридические лица, заключившие с ООО «ИНК» Соглашение о взаимодействии
Контрагент	физическое или юридическое лицо, выступающее стороной договора и принявшее обязательства по исполнению условий такого договора
Сотрудник Контрагента	лицо, находящееся в трудовых отношениях с Контрагентом и выполняющее работы в рамках заключенного между Заказчиком и Контрагентом договора

1.3 Сокращения и обозначения

Сокращение	Расшифровка
АРМ	Автоматизированное рабочее место
КСПД	Корпоративная сеть передачи данных
Общества	Дочерние общества и юридические лица, заключившие с ООО «ИНК» Соглашение о взаимодействии

.

2 Требования Заказчика в области информационной безопасности

2.1 Общие требования

2.1.1.1 Предоставление доступа к информационным системам Заказчика возможно в случае привлечения его к совместной хозяйственной, финансовой и иной деятельности на основе заключенных гражданско-правовых договоров и только в том объеме, который необходим для выполнения работ или оказания услуг по договору, а также при условии принятия Контрагентом обязательств по неразглашению и исключению неправомерного использования полученных в ходе выполнения работ или оказания услуг сведений.

2.2 Требования при удаленном подключении к информационным системам Заказчика

2.2.1.1 Удаленное подключение Контрагента к КСПД Заказчика возможно при наличии обоснования необходимости такого доступа согласно действующего договора.

2.2.1.2 Куратор инициирует процесс предоставления доступа. Срок предоставления права на удаленное подключение не может превышать срока действия действующего договора, заключенного сторонами.

2.2.1.3 Для формирования заявки на доступ Контрагент передает Куратору:

- Реквизиты действующего договора
- ФИО и даты рождения сотрудников Контрагента, которым необходимо настроить удаленное подключение
- Перечень ИТ-сервисов, к которым необходим доступ

2.2.1.4 Куратор передает сотрудникам Контрагента данные для удаленного подключения (индивидуальную учётную запись и пароль).

2.2.1.5 Сотрудники Контрагента обязаны использовать для удаленного подключения к информационным ресурсам Заказчика только индивидуальные учетные записи и пароль, выданные Заказчиком.

2.2.1.6 Сотрудники Контрагента обязуются:

- Обеспечить конфиденциальность данных (индивидуальная учетная запись и пароль), которые предоставлены Заказчиком для удаленного подключения;
- Не передавать данные для удаленного подключения (индивидуальная учетная запись и пароль) другим третьим лицам;
- Не использовать учетные данные (индивидуальная учетная запись и пароль), выданные другим сотрудникам Контрагента или иным третьим лицам;
- Блокировать АРМ при покидании рабочего места;
- Выполнять в информационных системах Заказчика, к которым предоставлен доступ, только те операции, которые требуются для выполнения работ или оказания услуг по действующему договору;

- Нести ответственность за действия, которые выполняются ими в информационных системах Заказчика.

2.2.1.7 Сотрудники Контрагента обязаны незамедлительно проинформировать Куратора или техническую поддержку Заказчика по тел. 8(3952) 211-352 вн.25–25 в следующих случаях:

- подозрительная активность на АРМ, вирусная активность;
- утрата носителей, содержащих информацию Заказчика;
- несанкционированный доступ к носителям, содержащим информацию Заказчика, в том числе АРМ;
- нарушение конфиденциальности или подозрение на нарушение конфиденциальности учетных данных для удаленного подключения.

2.3 Требования при подключении оборудования Контрагента к КСПД Заказчика

2.3.1.1 Подключение АРМ Контрагента (ПК, ноутбук) к КСПД Заказчика возможно при наличии обоснования необходимости такого доступа согласно действующего договора и при наличие разрешения на подключение.

2.3.1.2 Куратор для получения разрешения на подключение АРМ Контрагента к КСПД предоставляет департаменту телекоммуникационных систем и отделу информационной безопасности Заказчика:

- Перечень сотрудников Контрагента, которые будут работать на АРМ (ФИО);
- Перечень АРМ (MAC-адреса);
- Перечень ИТ-сервисов, к которым необходимо предоставить доступ: IP-адрес, port (если требуется).

2.3.1.3 При наличии разрешения подключение АРМ Контрагента выполняют только сотрудники департамента телекоммуникационных систем Заказчика.

2.3.1.4 Сотрудникам Контрагента запрещено:

- несанкционированное подключение АРМ к сетевым розеткам, находящимся на объектах Заказчика, а также подключение напрямую к оборудованию Заказчика;
- подключение оборудования, для которого не получено разрешение на подключение, в том числе стороннего активного сетевого оборудования (Wi-Fi роутер, коммутатор и т.п);
- осуществлять работу при наличии признаков на АРМ наличия вредоносной активности или при отсутствии антивирусной защиты;
- допускать к работе на АРМ других лиц (кроме работников подразделений Заказчика);
- хранить на АРМ личную информацию, не имеющую отношения к исполняемым обязанностям;
- оставлять АРМ незаблокированным при покидании рабочего места.

2.3.1.5 При работе на АРМ Контрагента, подключенном к КСПД Заказчика, необходимо обеспечить:

- исправное состояние АРМ;
- наличие у пользователей навыков работы с используемым аппаратным и программным обеспечением;
- выполнение на АРМ только тех действий и процедур, которые определены для реализации работ и услуг согласно действующего договора;
- наличие на АРМ лицензионного программного обеспечения, актуальной версии операционной системы;
- обновление операционной системы (дата обновления -не старше 1 месяца на момент проверки);
- антивирусную защиту АРМ (дата обновления антивирусных баз не старше 7 календарных дней на момент проверки);
- парольную защиту АРМ:
  - блокировка АРМ во время отсутствия сотрудника Контрагента;
  - пароль вводится непосредственно владельцем пароля;
  - пароль периодически меняется, не реже 1 раза в 4 месяца;
- блокировку USB-портов (при необходимости);
- невозможность использования АРМ как точку доступа Wi-Fi.

2.4 Ответственность Контрагента за невыполнение требований Заказчика в области информационной безопасности

2.4.1.1 Контрагент несет ответственность в полном объеме за любой прямой либо косвенный ущерб, который причинен либо может быть причинен бизнес-процессам, производственным процессам, информационным системам, оборудованию Заказчика по причине реализации угроз информационной безопасности или нарушения требований настоящего Стандарта.

2.4.1.2 Отдел информационной безопасности Заказчика оставляет за собой право отключить АРМ Контрагента от КСПД Заказчика, заблокировать учетные данные сотрудников Контрагента, инициировать штрафные санкции в адрес Заказчика в случае обнаружения:

- вредоносной (аномальной) активности на АРМ Контрагента;
- нелегитимного подключения оборудования Контрагента;
- осуществления Контрагентом нелегитимных операций в информационных системах Заказчика, не предусмотренных в рамках решения задач или оказания услуг по действующему договору;
- иных нарушениях пунктов настоящих требований.

2.4.1.3 Повторное подключение АРМ Контрагента или разблокировка доступа возможно после устранения Контрагентом выявленных нарушений.