

**Техническое задание на выполнение работ по разработке мероприятий по взаимодействию с Национальным координационным центром по компьютерным инцидентам для объектов критической информационной инфраструктуры ООО «Самарские коммунальные системы»**

**1. Общая информация**

**1.1. Терминология**

- АРМ – Автоматизированное рабочее место;
- ЗОКИИ – Значимый объект критической информационной инфраструктуры;
- Субъект КИИ – Общество с ограниченной ответственностью «Самарские коммунальные системы»;
- АСУ ТП – автоматизированная системы управления технологическим процессом;
- КНС – канализационные насосные станции;
- НФС – насосно-фильтровальная станция;
- ГОКС – система контроля и управления котельной городских очистных канализационных сооружений;
- СЗИ – Средство защиты информации;
- НКЦКИ – Национальный координационный центр по компьютерным инцидентам;
- ГосСОПКА – Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак;

**1.2. Наименование субъекта критической информационной инфраструктуры**

Субъект критической информационной инфраструктуры: Общество с ограниченной ответственностью «Самарские коммунальные системы», 443056, Самарская обл., г. Самара, ул. Луначарского, д. 56.

**1.3. Наименование систем – объектов значимого объекта критической информационной инфраструктуры**

Объектом подключения к НКЦКИ является ООО «Самарские коммунальные системы», производственный комплекс водоснабжения-водоотведения ООО «Самарские коммунальные системы» включающий в себя:

- Система контроля и управления котельной городских очистных насосных сооружений (далее – ГОКС) расположенных по адресу г. Самара, ул. Обувная 136
- Автоматизированная система контроля и управления котельной насосно-фильтровальной станции – 2 (далее НФС-2) расположенной по адресу г. Самара, Студеный овраг
- Автоматизированная система контроля и управления котельной насосно-фильтровальной станции – 3 (далее НФС-3) расположенной по адресу г. Самара, Южное шоссе 3А;
- Автоматизированная система контроля и управления канализационной насосной станции (далее-КНС-13) расположенной по адресу г. Самара, 1-я Кряжская ул., 61, посёлок Кряж.

#### 1.4. Перечень нормативных правовых актов, методических документов и национальных стандартов, которых необходимо придерживаться при выполнении работ по разработке мероприятий по взаимодействию с НКЦКИ

При разработке мероприятий по взаимодействию с НКЦКИ объектов критической информационной инфраструктуры необходимо придерживаться требования следующих документов и нормативных правовых актов:

- Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
- Приказ ФСБ России от 24.07.2018 № 366 «О Национальном координационном центре по компьютерным инцидентам»;
- Приказ ФСБ России от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»;
- Приказ ФСБ России от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»;
- Приказ ФСБ России от 06.05.2019 № 196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»;
- Приказ ФСБ России от 19.06.2019 № 281 «Об утверждении порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации»;
- Приказ ФСБ России от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации»;

## **2. Описание услуг, которые должен оказывать Исполнитель**

При оказании содействия в создании и организации взаимодействия субъекта КИИ с НКЦКИ включает в себя разработку организационно-распорядительной документации по информированию и взаимодействию с НКЦКИ в ходе следующих мероприятий:

- Сопровождение в направлении запроса в НКЦКИ на получение Методических рекомендаций;
- После получения Методических рекомендаций, разрабатывается пакет организационно-распорядительных документов с отражением сотрудничества с НКЦКИ;
- Выполняется разработка регламента организационных требований к процессам, персоналу, технологиям субъекта КИИ в соответствии с нормативными правовыми актами по вопросам взаимодействия с ГосСОПКА;
- Разработка и помощь согласование плана реагирования на компьютерные инциденты;

## **3. Результат выполнения работ**

По завершении работ настоящего технического задания Исполнитель предоставляет Заказчику необходимую отчетную документацию. Полный перечень представлен ниже:

- Официальное письмо-запрос в НКЦКИ на имя директора для получения Методических рекомендаций;
- Упорядочение правил и процедур, указанных в полученных Методических рекомендациях, точный список ОРД будет согласован после интерпретации МР, в который могут входить инструкции, журналы, формы;
- Регламентации правил и процедур реагирования на компьютерные инциденты, обеспечение действий в нештатных ситуациях;

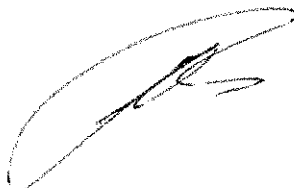
В случае, если после получения заявки Заказчика, Исполнителем выявлена невозможность полностью завершить выполнение работ в сроки, установленные Заказчиком, Исполнитель обязан в кратчайшее время уведомить об этом Заказчика. При этом, Заказчик оставляет за собой право потребовать от Исполнителя письменное обоснование, предлагаемых Исполнителем, сроков выполнения данных работ.

## **4. Дополнительные сведения**

- Исполнитель не имеет права привлекать внешних исполнителей;
- Обязательное наличие лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации, предусмотренных подпунктами «а», «б», «г», «д», «е» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации №79;
- Срок исполнения обязательств: 10 рабочих дней с даты подписания контракта;

- Приказы, распоряжения, акты и другие необходимые для выполнения требований Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» документы, разработанные Исполнителем, Заказчик утверждает самостоятельно;
- Заказчик направляет разработанные Исполнителем документы регуляторам самостоятельно.

Начальник УИТ



Т.В. Бирюков