

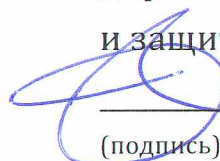
**УТВЕРЖДАЮ**

Заместитель директора КАЗ

им. С.П. Горбунова –

директор по безопасности, режиму

и защите государственной тайны

 / А.Ю. Пашкеев/  
(подпись)

«\_\_» ноября 2025г.

### **Технические условия**

**на разработку проектной, рабочей документации по оснащению инженерно-техническими средствами охраны (ИТСО)  
объекта «Реконструкция и техническое перевооружение лётно-испытательной базы, этап 2 АО «Туполев», г. Казань, РТ»**

2025г.

## Оглавление

1. Сокращения и условные обозначения.....	3
2. Перечень объектов: .....	4
3. Назначение системы ИТСО.....	6
4. Система контроля и управления доступом (СКУД).....	7
5. Система охранного видеонаблюдения (СОТ) .....	11
5.1. Требования к центральному оборудованию .....	11
5.2. Требования к оконечному оборудованию:.....	11
6. Система технологического видеонаблюдения (СТН) .....	14
6.1. Требования к центральному оборудованию .....	14
6.2. Требования к оконечному оборудованию .....	14
7. Система охранной сигнализации (ОС).....	17
7.1. Охранная сигнализация должна обеспечивать .....	17
7.2. Тревожно-вызывная сигнализация должна обеспечивать.....	19
8. Сети передачи данных .....	21
9. Наружные сети связи .....	22

## 1. Сокращения и условные обозначения

КАЗ – Казанский авиационный завод им. С.П. Горбунова – филиал АО «Туполев»

АРМ - автоматизированное рабочее место;

ИТСО – инженерно-технические средства охраны;

ТВС - тревожно-вызывная сигнализация;

ЛВС - локальная вычислительная сеть;

СПД – сеть передачи данных ИТСО;

ОС - система охранной сигнализации;

КИТС - комплекс информационно-технических систем;

СВН - система охранного видеонаблюдения;

СТН – система технологического видеонаблюдения;

СГЭ - система гарантированного электропитания;

СКУД - система контроля и управления доступом;

СУРВ – система учета рабочего времени;

ТСД – технические средства досмотра;

СОА – системообразующая аппаратура;

СХД - система хранения данных.

## 2. Перечень объектов:

Настоящие технические условия распространяются на следующие объекты, предусмотренные техническим заданием:

<i>n/n</i>	<i>Наименование объекта</i>	<i>Инженерные средства охраны</i>	<i>Технические средства охраны</i>
1.	Строительство здания ИТС		+
2.	Здание пультовой объекта «Сопка»		+
3.	Здание АТС		+
4.	Строительство здания для хранения химических реагентов		+
5.	Площадка под модульное здание ОПН и СКП		+
6.	Строительство девиационного круга		+
7.	Строительство закрытой стоянки на одно рабочее место		+
8.	Канализационная насосная станция №7		+
9.	Строительство ограждения БПРМ- 291	+	+
10.	Строительство ограждения ДПРМ- 291	+	+
11.	Строительство ограждения ДПРМ- 111	+	+
12.	Строительство ограждения БПРМ- 111	+	+
13.	Строительство ограждения СОПКА	+	+

Инженерные средства охраны включают в себя:

1. Периметральное ограждение с противоподкопной сеткой и спиральным барьером безопасности;
2. Ворота, калитки, шлагбаумы (в т.ч. противотаранные);
3. КПП;
4. др. конструкции, сооружения, ограждения, запорные устройства и механизмы, средства предупреждения потенциального нарушителя.

Технические средства охраны включают в себя:

1. Систему охраны периметра (СОП);
2. Систему охранного освещения (СОО);



3. Систему гарантированного электроснабжения ТСО (СГЭ);
4. Система контроля и управления доступом (СКУД);
5. Система охранного видеонаблюдения (СОТ);
6. Система технологического видеонаблюдения (СТН);
7. Система охранной и тревожной сигнализации (СОС);
8. Наружные сети связи (ССН);
9. Система передачи данных (СПД);
10. др. автоматизированные системы, обеспечивающие работу подразделений охраны

Конкретные разделы проектной документации, описывающие перечисленные системы определить в ходе проектирования.

### 3. Назначение системы ИТСО

Системы ИТСО должны представлять собой совокупность взаимосвязанных технических и инженерных средств охраны периметра, территории и корпусов объекта, обеспечивающих безопасное функционирование объекта, препятствующих проникновению на объект, и предоставляющих персоналу охраны необходимую информацию о состоянии безопасности охраняемых объектов. Основанием для построения ИТСО на объекте являются:

- Постановление Правительства РФ от 01.03.2024 №258 "Об утверждении требований к антитеррористической защищенности объектов (территорий) промышленности, находящихся в ведении или относящихся к сфере деятельности Министерства промышленности и торговли Российской Федерации, и формы паспорта безопасности этих объектов (территории) ";
- Свод правил СП 132.13330.2011: «Обеспечение антитеррористической защищенности зданий и сооружений. Общие требования проектирования»;
- Методические рекомендации в области проектирования инженерно-технических средств охраны и роботизации с применением типовых технических решений на объектах Государственной корпорации «Ростех» № МР-НИЦ ТСО-01-1.1-2021 утвержденные распоряжением №253 от 29.12.2021.

#### 4. Система контроля и управления доступом (СКУД)

СКУД должна разрабатываться как расширение существующей системы контроля и управления доступом Lyrіx производства ААМ Системз (Россия).

Система контроля и управления доступом должна обеспечивать:

- Контроль доступа персонала, посетителей в охраняемую зону, ее сектора и на критические элементы;
- Контроль доступа персонала, посетителей в серверные, аппаратные и кроссовые помещения объекта;
- Контроль приема/сдачи ключей от помещений корпуса в автоматическом режиме, средствами автоматизированной ключницы, интегрированной с СКУД и ОС.

Центральное оборудование существующей системы СКУД размещается в серверном помещении Корпуса 130. Размещение центрального оборудования и АРМ проектируемого расширения системы СКУД определить проектом. Предусмотреть расширение существующего оборудования для подключения оконечных устройств проектируемых объектов. Версия и функциональные возможности предусматриваемых проектом лицензий на ПО системы СКУД должны быть не ниже, чем у действующих лицензий. Предусматриваемые лицензии должны иметь возможность работать с существующим ПО системы СКУД предприятия в едином комплексе. В случае, если версия ПО, функционирующая на объекте, более не поставляется либо не поддерживается производителем, предусмотреть проектом обновление ПО системы объекта до актуальной версии.

Предусмотреть организацию КПП на удаленных объектах для размещения постов охраны. КПП оборудовать видеодомофонами, передачу сигналов которых выводить в помещения охраны, а также в помещения дежурного персонала.

На КПП предусмотреть мониторы сверки фотографии из базы данных с проходящим сотрудником и посетителем.

При выборе типа и количества турникетов предусмотреть необходимость обеспечения пиковой пропускной способности каждого турникета 30 человек в минуту. Турникеты должны иметь автоматические планки «Антипаника», складывающиеся по сигналу аварийной разблокировки или при пропадании питания. Материал корпуса турникета и его преграждающих планок, а также двойной распашной секции ограждения - нержавеющая сталь. При необходимости для входной группы



предусмотреть дополнительные полуростовые ограждения, исключающие возможность беспрепятственного несанкционированного прохода внутрь административно-бытовой части, минуя турникеты-триподы и двойную распашную секцию ограждения с магнитным УБ.

Серверные помещения, коммутационные, электрощитовые, помещение охраны, насосная станция пожаротушения, ИТП, ТП-1, ТП-2, РП-10кВ, периметральные входные двери 1го этажа корпусов необходимо оснастить системой контроля доступа. При возникновении аварийной ситуации, предусмотреть автоматическую, а также ручную разблокировку дверей на путях эвакуации.

Предусмотреть точки учета рабочего времени с выводом в единую систему СУРВ действующую на предприятии.

В корпусе ИТС предусмотреть автоматизированную систему хранения ключей для исключения возможности несанкционированного доступа, протоколирования приема/сдачи ключей, автоматизированной постановки/снятия помещений с охраны. Применить оборудование производства «ЭВС».

Требования по составу, параметрам и размещению оборудования СКУД:

- по типу управления СКУД должна выполняться универсальной (сетевой) - включающей в себя функции как автономных, так и централизованных систем, работающих в сетевом режиме под управлением одного или нескольких устройств управления и переходящих в автономный режим при возникновении отказов в сетевом оборудовании, устройствах управления или обрыве связи;
- идентификаторы (персональные пропуска) должны иметь уникальный идентификационный признак (код, номер), который не должен повторяться; идентификаторы (персональные пропуска) должны обеспечивать высокую безопасность обмена информацией между идентификатором и считывателем со взаимной аутентификацией, кодированием передаваемых данных распределёнными ключами шифрования для считывания/записи. Применить смарт-карты доступа по типу HID IC2020-24 (iCLASS+HID Prox) с высокой защитой от клонирования, со следующими характеристиками: Смарт-карта; Чип iCLASS SE; Рабочая частота: 13.56 МГц; Facility Code – согласовать при закупке. Формат: H10304. 37- бит.
- связь между контроллерами и управляющим сервером должно осуществляться по протоколу TCP/IP;

- подключение к сетевому оборудованию должно осуществляться с использованием стандартных CAT5e кабелей или выше с разъемами RJ-45.

На контрольно-пропускных пунктах, в местах прохода физических лиц предусмотреть установку технических средств, предназначенных для досмотра (ТСД) людей и находящихся при них вещей в целях выявления предметов и веществ, которые ограничены или запрещены для проноса на территорию предприятия и выноса за его пределы.

В ходе проектирования СКУД согласовать с Заказчиком характеристики и марку рекомендуемых для установки технических средств досмотра, а также предусмотреть возможность интеграции существующей на объекте системы контроля и управления доступом.

Состав технических средств досмотра определить на основании требований руководящих документов.

Предусмотреть интеграцию на программном уровне с действующей системой охранного видеонаблюдения объекта.

Система электропитания контроллеров СКУД должна обеспечивать защитное отключение при перегрузках и коротких замыканиях в цепях нагрузки, а также восстановление электропитания после устранения причины неисправности.

Все внешние элементы технических средств системы, находящиеся под напряжением, должны иметь защиту от случайного прикосновения, а сами технические средства иметь зануление или защитное заземление в соответствии с ПУЭ.

Для подключения считывателей предусмотреть применение экранированного кабеля парной скрутки. Для подключения остальных элементов СКУД предусмотреть медные огнестойкие самозатухающие кабели.

Провода и кабели должны прокладываться в лотках. В зонах отсутствия лотковых трасс — в гофрированных трубах из ПВХ-пластика, размещённых за фальшпотолком. В зонах без фальшпотолка кабель и провода прокладываются в гофрированных трубах или кабель-каналах, закреплённых на стене, или в штробах. При монтаже кабельных линий необходимо использовать гофрированные трубы и кабель-каналы должны быть из самозатухающегося пластика.



Подвод кабелей к входной группе (турникеты-триподы, двойная распашная секция ограждения с магнитным УБ) выполнить в стальных трубах, проложенных в стяжке пола, с выводом всех кабелей в помещение охраны.

Контроллеры в помещениях и коридорах разместить в запотолочном пространстве со стороны защищаемого помещения.

## **5. Система охранного видеонаблюдения (СОТ)**

Решения системы охранного видеонаблюдения должны разрабатываться как составная часть существующей системы видеонаблюдения SecurOS Enterprise производства ISS, с выводом в единый существующий ситуационный центр, расположенный на 2-м этаже Корпуса 130 (центральная проходная).

Проектируемая система должна включать в себя окончное оборудование – камеры видеонаблюдения и центральное оборудование – лицензии ПО и, при необходимости, сервера системы видеонаблюдения в составе программно-аппаратного комплекса.

### **5.1. Требования к центральному оборудованию**

Центральное оборудование системы должно размещаться в выделенном помещении серверной АБЧ корпуса, оснащенной системами кондиционирования, вентиляции, энергоснабжения, удаления продуктов тушения при сработке системы АГПТ. Предусмотреть оснащение серверами и СХД. При расчете параметров новых серверов принять время хранения видеоархива - не менее 60 суток постоянной записи.

Версия и функциональные возможности предусматриваемых проектом лицензий на ПО системы видеонаблюдения должны быть не ниже, чем у действующих лицензий. Предусматриваемые лицензии должны иметь возможность работать с существующим ПО системы охранного видеонаблюдения предприятия в едином комплексе. В случае если версия ПО, функционирующая на объекте, более не поставляется либо не поддерживается производителем, предусмотреть проектом обновление ПО системы объекта до актуальной версии.

Предусмотреть АРМ в помещении охраны (дежурного персонала) проектируемых объектов.

### **5.2. Требования к окончному оборудованию:**

Предусматриваемые проектом типы камер и точки их размещения должны обеспечивать:

- Наблюдение за периметром строений, объектов.
- Наблюдение за всеми входами/въездами в корпуса, территории.
- Видеонаблюдение на КПП и постах (пунктах) управления обеспечением охраны здания должно обеспечивать наблюдение за действиями сил

обеспечения безопасности, получения крупного плана проходящих через КПП сотрудников.

- Видеонаблюдение в серверных, аппаратных и кроссовых помещений;
- Обзорное наблюдение за местами размещения технологического оборудования.
- В административной части здания – видеонаблюдение за коридорами, выходами на лестничные площадки.
- При наличии режимных помещений – отдельные камеры для наблюдения за входами в такие помещения.

Требования к применяемым видеокамерам:

- Видеонаблюдение должно строиться на цифровых цветных видеокамерах с режимом работы «день/ночь».
- Для возможности настройки углов обзора камеры должны оснащаться моторизованным объективом. Фокусное расстояние объективов определить проектом исходя из точек размещения камер.
- Разрешение камер предусмотреть: не менее 2 МП для внутренних камер, не менее 4 МП для камер обзорного наблюдения зоны размещения технологического оборудования, не менее 4 МП для наружных камер.
- Электропитание камер должно осуществляться по технологии PoE.
- Должна поддерживаться отдельная настройка параметров изображения для режимов «день» и «ночь».
- Для работы в ночном режиме должна предусматриваться встроенная в камеру ИК подсветка.
- Для возможности интеграции оборудования по протоколу ONVIF2.6.
- Возможность сжатия изображения кодеком H.264/H.265
- Видеокамеры, предназначенные для контроля периметра контролируемых объектов, должны размещаться в герметичных термокожухах, имеющих солнцезащитный козырек, а также быть ориентированы на местности под углом к линии горизонта (лучи восходящего и заходящего солнца не должны попадать в объектив видеокамеры).
- Корпус видеокамер должен соответствовать степени защиты не ниже IP66 и ударопрочности не хуже IK10.
- Камеры должны иметь устойчивость к электростатическим разрядам согласно ГОСТ Р 51317.4.2: класс жесткости 4; контактный разряд - амплитуда: 8кВ, воздушный разряд - 15кВ.



- Камеры должны иметь устойчивость к наносекундным импульсным помехам согласно ГОСТ Р 51317.4.4: класс жесткости 4; амплитуда 4кВ по схеме «провод – земля» (2кВ - по схеме «провод – провод»). Частота повторения 100кГц.
- Камеры должны иметь устойчивость к микросекундным импульсным помехам большой энергии согласно ГОСТ Р 51317.4.5: класс жесткости 5; амплитуда 4кВ; длительность 6,5/700мкс;

Камеры должны иметь российское происхождение: в части аппаратной составляющей, что должно подтверждаться наличием оборудования в реестре Минпромторга СТ-1 и в части программного обеспечения камер что должно подтверждаться записью в реестре Российского программного обеспечения Минцифры РФ и иметь гарантийный срок службы не менее 5 лет.

Кабельные линии должны обеспечивать стабильную передачу видеосигнала с учетом помех от работы высокочастотного технологического оборудования. Для подключения камер видеонаблюдения к активному оборудованию необходимо использовать экранированные кабели категории не ниже Cat 6A.

Провода и кабели должны прокладываться в лотках. В зонах отсутствия лотковых трасс — в гофрированных трубах из ПВХ-пластика, размещённых за фальшпотолком. В зонах без фальшпотолка кабель и провода прокладываются в гофрированных трубах или кабель-каналах, закреплённых на стене, или в штробах. При монтаже кабельных линий необходимо использовать Гофрированные трубы и кабель-каналы должны быть из самозатухающего пластика.

## **6. Система технологического видеонаблюдения (СТН)**

Проектом предусмотреть создание системы технологического видеонаблюдения.

Проектируемая система должна включать в себя окончное оборудование – камеры видеонаблюдения и центральное оборудование – лицензии ПО и сервера системы видеонаблюдения в составе программно-аппаратного комплекса. Применяемое ПО должно быть включено в Единый реестр российских программ для электронных вычислительных машин и баз данных.

### **6.1. Требования к центральному оборудованию**

Центральное оборудование проектируемой системы должно размещаться в выделенном помещении серверной проектируемых объектов, оснащенной системами кондиционирования, вентиляции, электроснабжения, удаления продуктов тушения при сработке системы АГПТ. При расчете параметров серверов принять время хранения видеоархива - не менее 60 суток постоянной записи.

Проектируемая система должна функционировать независимо от системы охранного видеонаблюдения.

Система должна обеспечивать использование алгоритмов анализа изображений в режиме реального времени, в частности мониторинг присутствия оператора технологического оборудования на рабочем месте, создание соответствующих событий (закладок) в архиве видеозаписей, предоставление протокола зарегистрированных событий для дальнейшего анализа (отчет о времени нахождения оператора в рабочей зоне).

### **6.2. Требования к окончному оборудованию**

Предусматриваемые проектом типы камер и точки их размещения должны обеспечивать видеонаблюдение за местами размещения:

- Технологического оборудования, рабочих мест операторов и действующего инструмента данного оборудования;
- Зон проведения испытаний изделий;
- Опасных производственных объектов;
- Опасных объектов обеспечения.

Требования к применяемым видеокамерам:

- Видеонаблюдение должно строиться на цифровых цветных видеокамерах с режимом работы «день/ночь».



- Для возможности настройки углов обзора камеры должны оснащаться моторизированным объективом. Фокусное расстояние объективов определить проектом исходя из точек размещения камер.
- Разрешение камер предусмотреть не менее 4 МП.
- Электропитание камер должно осуществляться по технологии PoE.
- Для работы в ночном режиме должна предусматриваться встроенная в камеру ИК подсветка.
- Для возможности интеграции оборудования по протоколу ONVIF2.6.
- Возможность сжатия изображения кодеком H.264/H.265.
- Корпус видеокамер должен соответствовать степени защиты не ниже IP66 и ударопрочности не хуже IK10.
- Камеры должны иметь устойчивость к электростатическим разрядам согласно ГОСТ Р 51317.4.2: класс жесткости 4; контактный разряд - амплитуда: 8кВ, воздушный разряд - 15кВ.
- Камеры должны иметь устойчивость к наносекундным импульсным помехам согласно ГОСТ Р 51317.4.4: класс жесткости 4; амплитуда 4кВ по схеме «провод – земля» (2кВ - по схеме «провод – провод»). Частота повторения 100кГц.
- Камеры должны иметь устойчивость к микросекундным импульсным помехам большой энергии согласно ГОСТ Р 51317.4.5: класс жесткости 5; амплитуда 4кВ; длительность 6,5/700мкс.

Камеры должны иметь российское происхождение: в части аппаратной составляющей, что должно подтверждаться наличием оборудования в реестре Минпромторга СТ-1 и в части программного обеспечения камер что должно подтверждаться записью в реестре Российского программного обеспечения Минцифры РФ.

Кабельные линии должны обеспечивать стабильную передачу видеосигнала с учетом помех от работы высокочастотного технологического оборудования. Для подключения камер видеонаблюдения к активному оборудованию необходимо использовать экранированные кабели категории не ниже Cat 6A.

Провода и кабели должны прокладываться в лотках. В зонах отсутствия лотковых трасс — в гофрированных трубах из ПВХ-пластика, размещённых за фальшпотолком. В зонах без фальшпотолка кабель и провода прокладываются в гофрированных трубах или кабель-каналах, закреплённых

на стене, или в штробах. При монтаже кабельных линий необходимо использовать Гофрированные трубы и кабель-каналы должны быть из самозатухающего пластика.

## **7. Система охранной сигнализации (ОС)**

Система охранной сигнализации должна разрабатываться как составная часть комплекса инженерно-технических средств охраны.

Система охранной сигнализации должна включать в себя решения охранной сигнализации и решения тревожно-вызывной сигнализации.

Сигналы системы выдать в помещения Ситуационного центра управления безопасностью (Корпус 130, здание центральной проходной), помещение дежурного в корпусе ЛИС.

Предусмотреть оснащение двумя рубежами охраны помещения первого этажа, а также, при необходимости, специальных помещений.

Организовать управление охранной сигнализацией на посту охраны на первом этаже АБЧ.

ОС должна разрабатываться как расширение существующей системы охранной сигнализации на базе оборудования Lyrìx производства ААМ Системз (Россия).

### **7.1. Охранная сигнализация должна обеспечивать**

- обнаружение несанкционированного (проникновения) доступа в охраняемые зоны;
- выдачу сигнала о срабатывании средств обнаружения (СО) персоналу подразделения обеспечения безопасности и протоколирование этого события; ведение архива всех событий, происходящих в системе, с фиксацией всех необходимых сведений для их последующей однозначной идентификации (тип и номер устройства, тип и причина события, дата и время его наступления и т.п.);
- исключение возможности бесконтрольного снятия с охраны (постановки под охрану);
- осуществление функции приема (снятия) средств обнаружения (группы СО) на контроль (с контроля);
- представление поступающей информации о несанкционированном проникновении нарушителей в охраняемые зоны в реальных буквенно-цифровых координатах объекта и на графических планах объекта;
- формирование звукового сигнала при изменении состояния контролируемых средств и устройств в системе, а также при возникновении отказов и неисправностей аппаратуры системы;



- автоматическое диагностирование центральной и периферийной аппаратуры (при наличии) из единого ситуационного центра Корпуса 130, постов охраны, а также линий связи между ними с указанием адреса отказавшего сменного блока или устройства;
- централизованное управление параметрами основных средств обнаружения; автоматический и ручной дистанционный контроль работоспособности подключенных средств обнаружения с АРМ оператора;
- регистрацию действий оператора по обработке сигналов и управлению системой;
- возможность проверки работоспособности и тестирования аппаратуры без нарушения функционирования системы в автоматическом режиме и (или) по запросам оператора;
- расширение и изменение конфигурации системы силами обслуживающего персонала с использованием эксплуатационной документации на систему; защиту от ошибочных действий оператора;
- ввод и корректировку баз данных параметрирования системообразующей аппаратуры (СОА);
- сохранение вводимых данных параметрирования центральной аппаратурой при отключении напряжения электропитания;
- регистрацию времени поступления сигналов срабатывания СО и обработки их оператором;
- реализацию централизованной тактики постановки (снятия) на охрану (с охраны) участков блокирования;
- удостоверение личности (ей) абонентов, осуществляющих снятие с охраны СО по персональному коду или идентификатору (карте);
- регистрацию и протоколирование тревожных и текущих событий;
- приоритетное отображение событий от средств тревожно-вызывной сигнализации (ТВС) (при наличии) перед другими событиями;
- возможность перехода контроллеров системы в автономный режим работы и формирования ими сигналов оповещения при изменении состояния контролируемых СО при отказе связи с пунктом централизованного управления; автоматическую передачу сообщений, зарегистрированных за время работы системы в автономном режиме работы системы охранной сигнализации на пункты централизованного управления при восстановлении централизованного режима работы;

- интеграцию с существующими на предприятии системами (СВН, СКУД) на системном (программном уровне) с передачей информации в Корпус 130;
- повторное подтверждение команд, формируемых для управления работой системы в необходимых случаях;
- возможность контроля и регистрации действий оператора;
- идентификацию операторов по условному имени (логин) и личному паролю при смене дежурства.

## **7.2.Тревожно-вызывная сигнализация должна обеспечивать**

- информирование персонала подразделения охраны о срабатывании устройств ТВС;
- определение места вызова;
- скрытность установки и удобство пользования тревожно-вызывным устройством;
- невозможность отключения устройств ТВС, с фактом фиксации срабатывания устройства;
- отличительность сигналов срабатывания устройств ТВС от сигналов срабатывания средств обнаружения.

Периметр здания с входящим в него КПП, дверями, воротами (технологическими при наличии) и калитками (при наличии) следует разделять на отдельные охраняемые участки (зоны) с подключением их отдельными шлейфами сигнализации.

Индикация состояния, постановка и снятие с охраны участков охраны должны производиться с поста охраны и из ситуационного центра корпуса 130 по установленным приоритетам и правам доступа с помощью устройств из состава охранной сигнализации.

Средства тревожно-вызывной сигнализации должны обеспечивать возможность их скрытной установки в следующих местах:

- контрольно-пропускные пункты;
- пункты досмотра объекта;
- помещения, предназначенные для размещения сил обеспечения охраны предприятия;
- специальные и выделенные помещения (по согласованию с Заказчиком).

Системообразующая аппаратура ОС должна быть универсальной (распределенной) - включающей в себя функции как автономных, так и



централизованных систем, работающих в сетевом режиме с управлением от центрального или нескольких распределенных устройств управления и переходящих в автономный режим при возникновении отказов в сетевом оборудовании, центральном устройстве или обрыве связи.

По информационной ёмкости должно обеспечиваться подключение всех средств обнаружения с возможностью наращивания не менее 10%.

Приёмно-контрольное оборудование должно обеспечивать резистивный контроль состояния шлейфа с подключённым к нему СО, даже в случае снятия СО с охраны.

По информативной ёмкости должны использоваться системы большой информативности, поддерживающие не менее 7 видов извещений типа: - "Норма", "Тревога", "Взят под охрану", "Снят с охраны", "Номер шлейфа (адреса, зоны)", "Номер (код) ответственного лица", "Неисправность".

ОС должна обеспечивать время передачи информации от момента срабатывания средства обнаружения до момента отображения тревожного сообщения не более 3 сек.

В проекте применить охранную сигнализацию на базе сетевых контроллеров. Предусмотреть интеграцию (управление и мониторинг) проектируемой системы в ранее созданный единый ситуационный центр технических средств охраны.

Предусмотреть интеграцию на программном уровне в единый программно-аппаратный комплекс SecurOS производства ISS.

Для выбора климатического исполнения уличного оборудования использовать: СНиП 2.01.07-85 «Нагрузки и воздействия» и СНиП 23-01-99 «Строительная климатология».

Для подключения извещателей предусмотреть экранированные медные кабели для групповой прокладки, не распространяющие горение, с пониженным дымовыделением.

Провода и кабели должны прокладываться в лотках. В зонах отсутствия лотковых трасс — в гофрированных трубах из ПВХ-пластика, размещённых за фальшпотолком. В зонах без фальшпотолка кабель и провода прокладываются в гофрированных трубах или кабель-каналах, закреплённых на стене, или в штробах. При монтаже кабельных линий необходимо использовать Гофрированные трубы и кабель-каналы должны быть из самозатухающего пластика.

## 8. Сети передачи данных

Проектом предусмотреть подсистему передачи данных для обеспечения взаимодействия всех компонентов систем ИТСО друг с другом.

Сеть передачи данных для систем СКУД, СОТ, ОС должна быть выделена в физически независимую сеть с собственным комплектом коммутационного оборудования.

Проектом предусмотреть коммутаторы российского производства, что должно подтверждаться наличием указанных коммутаторов в реестре «Телекоммуникационного оборудования российского происхождения» (ТОРП) Минпромторга России. Проектное оборудование должно иметь возможность интеграции и взаимодействия с существующим на предприятии.

Топологию сети применить по типу «иерархическая звезда». В рамках проектирования объекта предусмотреть оборудование уровня агрегации и уровня доступа. Проектом предусмотреть использование управляемых коммутаторов уровня L3/L2+ для оборудования уровня доступа и управляемых коммутаторов уровня L3 для оборудования уровня агрегации. Предусмотреть систему централизованного мониторинга и управления коммутаторами. Система мониторинга и управления должна быть включена в реестр российского ПО. Размещение пункта централизованного мониторинга и управления коммутаторами согласовать с группой информационной безопасности.

Для связи коммутаторов доступа с коммутаторами агрегации предусмотреть волоконно-оптические линии. Скорость подключения между коммутаторами агрегации и коммутаторами доступа принять 10Гбит/с. Скорость подключения между коммутаторами агрегации и коммутаторами ядра (существующими) принять 40Гбит/с. Допускается использование подключения/подключений на скорости 10Гбит/с при условии обеспечения неблокируемой передачи данных.

Для подключения оконечного оборудования предусмотреть коммутаторы с поддержкой технологии PoE с поддержкой энергопотребления до 30 Вт на порт. Скорость портов для подключения оконечного оборудования принять 1Гбит/с.

При проектировании предусмотреть меры по обеспечению отказоустойчивости сети передачи данных:

Для коммутаторов агрегации предусмотреть использование дублирующего коммутатора в горячем резерве.

Предусмотреть дублированные подключения между коммутаторами



доступа и коммутаторами агрегации.

Кабельные линии, используемые для основного и резервного подключения проложить по физически разнесенным трассам, в случаях если организация физически разнесенных трасс на всем участке от коммутатора агрегации до коммутатора доступа невозможна, предусмотреть разнесенные трассы на максимально возможной протяженности.

Предусмотреть резервирование блоков питания коммутаторов (в случаях если установка второго блока питания предусмотрена конструкцией коммутатора).

Проектируемое коммутационное оборудование должно обеспечиваться технической и гарантийной поддержкой производителя в формате 24/7 и отправкой оборудования на замену неисправного на следующий рабочий день.

Кабельные линии должны обеспечивать стабильную передачу видеосигнала с учетом помех от работы высокочастотного технологического оборудования.

## 9. Наружные сети связи

Для организации связи систем КИТСО между корпусами, проектом предусмотреть следующие технические решения:

- для объектов размещенных на территории КАЗ выполнить оптическую кольцевую систему двумя независимыми трассами из корпуса центральной проходной. Емкость кабелей – не менее 12 волокон, тип кабеля – одномодовый. Кабельные линии проложить в существующей, проектируемой кабельной канализации, а также по кабеленесущим системам.

- удаленные объекты подключить к тревожно вызывной сигнализации в соответствии с техническими условиями организации оказывающей услуги ведомственной охраны. Подключение системы контроля и управления доступом, системы видеонаблюдения, путем привлечения оператора связи, оказывающего соответствующие услуги, либо построением радиорелейного канала связи, оснащенного соответствующими средствами защиты информации.

В соответствии с требованиями Информационной безопасности СПД должна быть физически отделена от ЛВС и других сетей КАЗ.

Выбор оборудования и версий программного обеспечения производить с учетом требований Указ Президента Российской Федерации от 30.03.2022 г. №166.

Проектно-сметной документацией предусмотреть выполнение пуско-наладочных работ с учетом обеспечения ввода в эксплуатацию проектируемых систем, сложности наладки, интеграции и обеспечения непрерывности работы действующих систем при добавлении проектируемого оборудования.

Разработал:

А.А. Никитин

Согласовано:

Р.М. Тарасов

Согласовано:

А.Р. Штепа

