КЫРГЫЗ РЕСПУБЛИКАСЫНЫН
МИНИСТРЛЕР КАБИНЕТИНЕ
КАРАШТУУ
ЖАРАНДЫК АВИАЦИЯ
МАМЛЕКЕТТИК АГЕНТТИГИ

ГОСУДАРСТВЕННОЕ
АГЕНТСТВО ГРАЖДАНСКОЙ
АВИАЦИИ
ПРИ КАБИНЕТЕ МИНИСТРОВ
КЫРГЫЗСКОЙ РЕСПУБЛИКИ

БУЙРУК
ПРИКАЗ

2024-ж. 24-сентябрь № 875

Бишкек ш.
г.Бишкек

Жарандык авиация уюмдарында көзөмөл, видеобайкоо системаларын орнотуу боюнча нускамалык материалды бекитүү жөнүндө

Кыргыз Республикасынын Министрлер Кабинетине караштуу Жарандык авиация мамлекеттик агенттигинин 2022-жылдын 24-ноябрындагы №787 буйругу менен бекитилген “17-КРАЭ. “Авиациялык коопсуздук” Кыргыз Республикасынын Авиациялык эрежелеринин 20-пунктунун 10-пунктчасына ылайык, **буйрук кылам:**

1. Тиркемеге ылайык жарандык авиация уюмдарында көзөмөл, видеобайкоо системаларын орнотуу боюнча нускамалык материал бекитилсин.
2. Кыргыз Республикасынын Министрлер кабинетине караштуу Жарандык авиация мамлекеттик агенттигинин авиациялык коопсуздук бөлүмү бул буйрукту бардык кызыкчылыгы бар жактарга маалымат үчүн жеткирсин.
3. Бул буйруктун аткарылышын көзөмөлдөө директордун орун басары К.Т.Төлөгөнөвго жүктөлсүн.

Об утверждении инструктивного материала по установке систем видеонаблюдения, контроля доступа в организациях гражданской авиации

В соответствии с подпунктом 10 пункта 20 Авиационных правил Кыргызской Республики «АПКР 17. «Авиационная безопасность», утвержденных приказом Государственного агентства гражданской авиации при Кабинете Министров Кыргызской Республики от 24 ноября 2022 года №787, **приказываю**:

1. Утвердить инструктивный материал по установке систем видеонаблюдения, контроля доступа в организациях гражданской авиации согласно приложению.

2. Отделу авиационной безопасности Государственного агентства гражданской авиации при Кабинете Министров Кыргызской Республики довести настоящий приказ до сведения всех заинтересованных лиц.

3. Контроль за исполнением настоящего приказа возложить на заместителя директора К.Т. Төлөгөнова.

Директордун милдетин
убактылуу аткаруучу **Д.К. Бостонов**

Приложение к приказу
Государственного агентства
гражданской авиации
при Кабинете Министров
Кыргызской Республики
№ 885 от «24» 09 2024г.

Инструктивный материал
по установке систем видеонаблюдения, контроля доступа в организациях гражданской авиации

ИЗМЕНЕНИЯ

О внесении изменений в настоящий Инструктивный материал сообщается всем заинтересованным организациям согласно соответствующему перечню рассылок органа ГА. Ниже приводится форма для регистрации поправок.

ЛИСТ РЕГИСТРАЦИИ
изменений

№ изменения	№ документа, дата утверждения документа	ФИО лица, внесшего изменения	Подпись

Содержание

1. Система видеонаблюдения (CCTV)

1. Система видеонаблюдения должна быть масштабируема, с возможностью добавления внешних систем хранения, новых рабочих мест операторов.

2. Условия эксплуатации для наружных камер составляют от -30 до +45 градусов по Цельсию.

3. В устанавливаемых камерах имеется поддержка аналитики (оставленный предмет, убранный предмет, пересечение зоны, подсчет объектов, обработка багажа, зон досмотра проезда автотранспорта на территорию и т.д.).

4. Система расширяема без покупки дополнительных лицензий. Лицензии, установленные для полнофункциональной работоспособности программного комплекса, включая сервер управления системой и рабочие станции, должны быть без срока истечения.

5. Система обеспечивает длительность и высокое качество видеоархива. Срок хранения видеоархива с учетом постоянной записи на всех камерах и с высоким разрешением должен быть не менее 40 дней (для подключения основных жестких дисков используются интерфейсы SAS или SATA).

2. Система контроля доступа

6. До установки системы контроля доступа принимаются следующие меры:

1) четко определяются контролируемые и неконтролируемые зоны и пункты доступа к ним;

2) проводится тщательное обследование для определения охраняемой зоны ограниченного доступа. Эта процедура предполагает:

а) определение групп, которым будет предоставлен доступ;

б) назначение уровней доступа к различным зонам для всех лиц, которым предоставлен доступ (матрица права доступа);

в) оценку потока лиц, переходящих границы зоны. Необходимо ввести график автоматического проектирования маршрутов доступа и групп, которые их используют.

3) оптимизируются маршруты. То есть разрабатываются следующие варианты для различных маршрутов:

а) закрытие определенных маршрутов – предоставление механической защиты;

б) человекоуправляемые пункты контроля; и/или

в) автоматизированный контроль доступа. При этом необходимо учесть различные факторы, а именно:

- меры безопасности для близкорасположенных зон;

- поток доступа вдоль маршрута;

- оценка осуществляемых мер контроля.

7. После получения оптимальной модели доступа, необходимо выбрать электронную систему контроля доступа и запланировать физические и функциональные запасы. На этом этапе уточняются эксплуатационные требования для каждой детали системы, а также для программного обеспечения.

8. При выборе электронной системы контроля доступа учитываются следующие требования:

1) система контроля доступа должна быть автономной и способной интегрироваться в общую систему обеспечения безопасности и защиты;

2) сеть системы должна предусматривать выход из строя системы связи и функционировать при пониженном качестве уровня связи;

3) время реакции системы должно быть менее полсекунды, а время изменения в соответствии с новыми данными – менее пяти секунд в зависимости от схемы доступа;

4) программа чтения удостоверения личности должна быть точной и не поддаваться влиянию внешних факторов;

5) центр контроля и информация о системе должны защищаться специальными мерами безопасности от кибер атак;

6) система должна быть проста в эксплуатации и обслуживании;

7) корректировка информации и личных данных, а также отчеты по безопасности должны автоматически передаваться уполномоченным лицам;

8) данные с системы контроля доступа должны передаваться в центр контроля в простой форме, способствующей необходимым действиям;

9) должна существовать возможность легкого изменения основных данных системы в зависимости от обстоятельств.

9. Процесс установки тщательно контролируется с целью обеспечения защиты элементов сети. При установке системы контроля доступа необходимо предусмотреть аварийный источник питания или запасной аккумулятор.

10. Разрабатываются и при необходимости с заинтересованными государственными органами согласовываются испытательные методы для тестирования системы контроля доступа, которые подробно излагаются в программе авиационной безопасности организации гражданской авиации.

11. Система контроля доступа должна соответствовать законодательству Кыргызской Республики по технике безопасности.

3. Система опознавания лица человека, транспортных средств

12. Камеры, используемые в организациях гражданской авиации для распознавания лиц и транспортных средств соответствуют требованиям, связанным с высоким уровнем безопасности, интенсивным пассажирским и

транспортным движением, а также специфическими условиями эксплуатации. Основные требования для таких камер включают:

1) разрешение камеры:

- минимум 4K (8 МП) для четкого захвата мелких деталей, таких как черты лица и номера транспортных средств, даже на большом расстоянии или в движении;

- для транспортных средств требуется особенно высокое разрешение для распознавания номеров автомобилей.

2) высокая частота кадров (FPS):

- 30 FPS и выше для плавного захвата движения лиц и транспортных средств, что особенно важно в аэропортах, где люди и транспорт находятся в постоянном движении;

- для транспортных средств, передвигающихся с высокой скоростью, может потребоваться частота до 60 FPS для точного распознавания;

3) интеграция с системами искусственного интеллекта (AI):

- камеры должны быть оснащены или поддерживать интеграцию с AI-алгоритмами, которые могут в реальном времени обрабатывать и анализировать видеопоток, чтобы мгновенно распознавать лица и номерные знаки автомобилей;

- важно наличие функций сравнения с базами данных (например, база данных пассажиров или транспортных средств);

4) расширенный угол обзора и зона покрытия:

- камеры для аэропортов должны обладать широким углом обзора (120-180 градусов) для покрытия больших пространств, таких как парковки, зоны высадки пассажиров или входные зоны терминалов;

- для распознавания лиц может использоваться комбинация камер с узким углом обзора, ориентированных на конкретные проходы и коридоры, чтобы детально фиксировать лица пассажиров;

5) освещение и ИК-подсветка:

- для обеспечения стабильной работы в различных условиях освещения камеры должны иметь автоматическую настройку уровня экспозиции;

- камеры должны быть оснащены ИК-подсветкой для ночного видения, чтобы эффективно работать в условиях низкой освещенности, как в терминалах, так и на парковках;

6) антибликовое покрытие и динамический диапазон (WDR):

- в аэропортах часто бывает много источников света и отражений (например, от окон или металлических поверхностей). Камеры должны иметь функцию широкого динамического диапазона (WDR), чтобы адаптироваться к резким перепадам освещения и предотвращать блики;

- антибликовое покрытие поможет снизить влияние света на изображение, особенно при съемке на парковках или в зонах с большим количеством окон;

7) Надежность и устойчивость к внешним условиям:

- в аэропортах и иных организациях гражданской авиации камеры могут устанавливаться как внутри терминалов, так и снаружи на транспортных подъездах. Камеры должны соответствовать стандартам защиты IP66 или IP67 для защиты от пыли, дождя, снега и экстремальных температур;

- устойчивость к ударам и вандализмоустойчивость (например, стандарт IK10) особенно важна в публичных местах;

8) скорость обработки и хранение данных:

- камеры должны обеспечивать реальную скорость обработки данных для немедленного распознавания и уведомления службы авиационной безопасности в случае обнаружения подозрительных лиц или транспортных средств;

- важна поддержка систем видеонаблюдения с возможностью хранения данных на облачных серверах для последующего анализа;

9) поддержка биометрической аутентификации:

- камеры должны поддерживать биометрические системы распознавания лиц, которые используются для аутентификации пассажиров, например, при прохождении через зоны контроля безопасности или на посадку на рейс;

- системы должны быть совместимы с нормативными актами в сфере обработки биометрических данных;

10) интеграция с другими системами безопасности:

- камеры должны быть интегрированы в общую систему безопасности аэропорта или организации гражданской авиации, включая системы контроля доступа, системы распознавания номеров автомобилей (ANPR) и другие аналитические системы для контроля периметра;

- они должны поддерживать стандарты ONVIF и другие протоколы для бесперебойной работы в комплексных системах наблюдения и безопасности;

11) оптическая и цифровая стабилизация:

- Важна стабилизация изображения для предотвращения смазывания при съемке подвижных объектов, особенно на подъездах к терминалу или зданию, где автомобили могут двигаться на высокой скорости;

12) высокая точность при работе с массовыми потоками людей:

- в аэропортах необходимо учитывать плотные потоки пассажиров, поэтому камеры должны иметь высокую точность идентификации даже при большом количестве людей в кадре.

13. Эти требования позволяют обеспечивать безопасность в аэропортах и в организациях гражданской авиации, и эффективно управлять пассажиропотоком и транспортом на территории, минимизируя риск ошибок в распознавании и обеспечивая высокий уровень защиты данных.

4. Системы защитной сигнализации и замкнутая телевизионная система (ЗТС)

14. При установке и использовании системы защитной сигнализации учитываются следующие требования:

а) система защитной сигнализации обнаруживает проникновение или попытки проникновения нарушителя в контролируемую зону, определяя при этом места проникновения и подачу сигнала тревоги силам реагирования;

б) система защитной сигнализации обеспечивает непрерывное наблюдение за охраняемой зоной и при использовании в сочетании с ЗТС может распространить охват на те зоны, которые обычно недоступны для патрулирования (например, крыши или запертые помещения). Систему защитной сигнализации следует рассматривать как один из компонентов системы защиты периметра, а не как самостоятельную систему;

в) система защитной сигнализации не допускает "мертвых зон", при этом сводится к минимуму возможность воздействия на окружающую среду и ложные срабатывания. При этом организация гражданской авиации, до установления системы защитной сигнализации определяет следующие критерии:

- зону и/или оборудование, защиту которых необходимо обеспечить;
- уровень или степень угрозы;
- требуется ли подключение к другим электронным системам, например, системе ЗТС или автоматизированным системам контролирования доступа;
- будут ли в защищаемой зоне находиться сотрудники охраны или средства сигнализации для сил реагирования;
- характер сил реагирования или требуемые меры по осуществлению контроля;

г) система защитной сигнализации обеспечивает надежность и удобна в техническом обслуживании;

д) система защитной сигнализации проста в эксплуатации и не подвергается несанкционированному доступу;

е) система защитной сигнализации снабжена запасным питанием в случае отключения основного электропитания;

ж) система соответствует установленным в Кыргызской Республике нормам безопасности труда.

15. При установке и использовании ЗТС учитываются следующие требования:

- обеспечение непрерывного, круглосуточного наблюдения;
- возможность дистанционного контролирования периметра и других защищаемых зон;
- наблюдение в ночное время и при неблагоприятных погодных условиях;

- видеозапись событий для целей воспроизведения и использования в качестве доказательств;

- проверка правильности срабатывания сигнализации;

- установление личности и проверка разрешений на доступ в сочетании с системой контролирования доступа;

- координация ответных действий в связи с сигнализацией и других оперативных мер;

- общее повышение уровня безопасности;

- способность работать при низких уровнях освещенности;

- защита от несанкционированного вмешательства;

- способность работать и передавать изображения в различных климатических и иных условиях - нагрев, образование льда, сильный дождь, конденсация, пыль, снег, туман, сильный дождь или дым, свет или уличное освещение, огни сигнализации, отражение солнечных лучей от водной поверхности или окон, а также лучи восходящего или заходящего солнца;

- возможность осуществлять запись и воспроизведение изображений на протяжении минимум 300 ч.

16. Все охранные системы ЗТС подлежат обязательному приемо-сдаточному тестированию и впоследствии должны регулярно проверяться по установленной методике. Методика тестирования системы ЗТС должна включать проверку, измерение, регистрацию и учет как минимум следующих обязательных показателей:

1) зона охвата;

2) различимость цели;

3) высота изображения цели;

4) постоянная времени системы.

17. Испытание системы ЗТС должна подтвердить, что при наблюдении заданной зоны охвата имеет место минимальное перекрытие соседних секторов. Степень перекрытия определяется в процентном отношении к ширине изображения для соседних по горизонтали зон или к высоте изображения для соседних по вертикали зон. Минимальное перекрытие составляет 5 и 10 %.

18. Различимость цели является показателем того, насколько легко можно заметить цель на экране монитора при самых плохих условиях освещения. Используя должным образом замаскированную цель с самыми плохими условиями освещения и места нахождения, оператор должен указать, является ли цель:

а) легко различимой, т. е. цель можно сразу распознать, при этом ошибки невозможны;

б) достаточно легко различимой, т. е. цель необходимо отыскать, но невозможно пропустить, причем время обнаружения не превышает допустимой постоянной времени системы;

в) трудно различимой, т. е. цель можно обнаружить только после тщательного и продолжительного поиска в течение периода времени, превышающего допустимую постоянную времени системы;

г) совсем неразличимой.

Приемлемыми результатами являются только условия, указанные в подпунктах а) и б).

19. Различимость цели проводится при помощи следующих тест-объектов:

а) кукла, одетая в камуфляжную куртку;

б) портфель, запачканный грязью;

в) номерные знаки, запачканные грязью;

г) персональный или транспортный пропуск.

20. Высота изображения испытательной цели представляет собой высоту цели на экране монитора в процентном отношении к высоте изображения по вертикали. Минимальные приемлемые значения высоты изображения цели в процентах от высоты изображения на экране монитора составляют:

- для обнаружения - 10 %;
- для распознавания - 50 %;
- для идентификации - 100 %.

21. При использовании системы ЗТС совместно с системой защитной сигнализации постоянная времени системы измеряется от момента подачи сигнала тревоги до момента, когда оператор устанавливает, по какому из мониторов необходимо вести наблюдение, и обнаруживает визуальное отображение цели на экране. Если система ЗТС используется отдельно, то постоянную времени системы можно определить исходя из применяемых оператором фиксированных схем поиска и повторяющихся периодов поиска. В этом случае роль оператора заключается в реагировании на поданный сигнал тревоги и выполнении ответных действий в течение установленной постоянной времени.

22. Эксплуатация и техническое обслуживание системы защитной сигнализации и ЗТС осуществляется обученными и допущенными к работе с техникой специалистами.