План действий по обеспечению кибербезопасности

Опубликовано с санкции Генерального секретаря

Издание второе, январь 2022 г.

Международная организация гражданской авиации

Термины и определения[1]

Информационная безопасность

Сохранение конфиденциальности, целостности и доступности информации. Также сюда могут быть включены другие свойства, такие как подлинность, подотчетность, неотказуемость и достоверность [BS ИСО/МЭК 27000:2018].

Инцидент

Одно или несколько нежелательных или неожиданных событий в области информационной безопасности, которые со значительной степенью вероятности могут привести к нарушению операционной деятельности и поставить под угрозу информационную безопасность [ИСО/МЭК 27035-1].

Субъект угрозы (или исполнитель)

Субъект, который частично или полностью несет ответственность за инцидент, который воздействует (или может воздействовать) на организацию или систему.

Кибербезопасность

Комплекс технологий, средств контроля и мер, а также процессов и практических методов, предназначенных для обеспечения конфиденциальности, целостности, доступности и общей защиты систем, сетей, программ, устройств, информации и данных от атак, повреждений, несанкционированного доступа, использования и/или эксплуатации.

Матрица риска

Инструмент для ранжирования и отображения компонентов рисков (угроза, вероятность, воздействие/последствия и уязвимость), реализованных мер по снижению риска и, в конечном счете, остаточных рисков.

Обмен информацией

Процесс, посредством которого одна организация предоставляет информацию другой или нескольким другим организациям в целях содействия принятию решений на основе оценки риска и распространения передовой практики.

Политика в области кибербезопасности

Политика в области кибербезопасности документально отражает намерения и направления деятельности организации в части управления угрозами для кибербезопасности, как это заявлено высшим руководством. Это письменный документ организации, в котором изложены методы защиты организации от угроз для кибербезопасности, а также порядок действий при возникновении инцидентов или событий.

[1] По-прежнему находятся на рассмотрении.

СМИБга: система менеджмента информационной безопасности гражданской авиации

Модель для создания, реализации, эксплуатации, мониторинга, пересмотра, обновления и совершенствования защиты информационных активов для достижения целей гражданской авиации на основании оценки риска и уровней принятия риска организации, предназначенных для обработки рисков и управления ими. Источник: ИСО 27000:2009.

Событие

Выявленное наступление состояния системы, службы или сети, указывающего на возможное нарушение политики обеспечения информационной безопасности или отказ средств контроля, или ранее неизвестная ситуация, которая может иметь значение для безопасности [ИСО/МЭК 27035]. Следует отметить, что "событие" необходимо понимать в широком смысле, а не как термин "событие, затрагивающее безопасность полетов", который охватывает только события, которые имеют или могут иметь значение в контексте безопасности полетов.

Уязвимость

Слабое звено в информационной системе, процедурах обеспечения безопасности системы, внутренних средствах контроля или процессе реализации, которое может быть использовано или вызвано субъектом угрозы. Это может быть система, которая прямо или косвенно поддерживает функционирование авиационной системы.

.

КРАТКАЯ СПРАВКА

39-я сессия Ассамблеи Международной организации гражданской авиации (ИКАО) подтвердила важность и безотлагательность защиты критических систем инфраструктуры гражданской авиации от кибератак, а также принятия глобальных обязательств со стороны ИКАО, ее государств-членов и отраслевых заинтересованных сторон в отношении действий с целью совместно и систематически решать проблемы кибербезопасности в гражданской авиации и устранять соответствующие угрозы и риски. Резолюция A39-19 *"Решение проблем кибербезопасности в гражданской авиации"* определила действия, которые в этой связи должны предпринять государства и другие заинтересованные стороны. 39-я сессия Ассамблеи ИКАО также поручила ИКАО разработать всесторонний план работы в области кибербезопасности.

Во исполнение поручения Ассамблеи Исследовательская группа Секретариата по кибербезопасности (SSGC) разработала стратегию кибербезопасности для гражданской авиации.

40-я сессия Ассамблеи ИКАО приняла измененную резолюцию A40-10 *"Решение проблем кибербезопасности в гражданской авиации"*, которая призывает государства осуществлять стратегию кибербезопасности и подчеркивает важность разработки плана устойчивой реализации этой стратегии, а также продолжения работы по созданию надежного механизма обеспечения кибербезопасности.

План действий по обеспечению кибербезопасности (ПДоК) служит основой для совместной работы государств, отрасли, заинтересованных сторон и ИКАО в деле развития потенциала для выявления, предотвращения, обнаружения кибератак против гражданской авиации, реагирования на них и восстановления после таких атак, а также для создания надежного механизма сотрудничества. Он разработан с тем, чтобы предложить ряд принципов, мер и действий, направленных на достижение целей семи основополагающих элементов указанной стратегии.

Глава 1

ВВЕДЕНИЕ

1.1 ИСХОДНАЯ ИНФОРМАЦИЯ

1.1.1 В нынешнем контексте гражданской авиации прогнозируется долгосрочный рост объема воздушных перевозок, стремительно развивается техника, производство полетов усложняются, вследствие чего в эксплуатационной среде приходится сталкиваться с новыми проблемами. Высокие темпы технического прогресса меняют характер деятельности гражданской авиации и делают систему гражданской авиации более уязвимой к угрозам для кибербезопасности. Злонамеренная кибердеятельность может по-разному затронуть гражданскую авиацию – от незначительных нарушений производственных процессов до катастрофических исходов. Риски стремительно растут и налицо острая необходимость в устойчивом механизме обеспечения кибербезопасности на международном, региональном и национальном уровнях.

1.1.2 Создание надежной инфраструктуры кибербезопасности, которая основана на тесном сотрудничестве между государствами, отраслью и ИКАО, позволяет обеспечить повышение общей осведомленности о кибербезопасности, что в конечном счете приведет к более безопасной и устойчивой системе гражданской авиации.

1.1.3 ИКАО неуклонно адаптирует свою деятельность применительно к постоянно меняющейся глобальной картине угроз, что соответствует резолюциям Совета Безопасности Организации Объединенных Наций, в которых подтверждается ответственность государств за обеспечение безопасности воздушных сообщений, осуществляемых в пределах их территории, и содержится призыв ко всем государствам сотрудничать с ИКАО в деле обеспечения того, чтобы согласно Чикагской конвенции международные стандарты по безопасности анализировались, обновлялись и вводились в действие на основе текущих рисков. Поскольку угрозы для кибербезопасности гражданской авиации эволюционируют и их масштабы, вероятно, будут возрастать, ИКАО в соответствии с положениями резолюции 2341 (2017) СБ ООН принимает меры по созданию надлежащих механизмов смягчения и уменьшения рисков для критической авиационной инфраструктуры, связанных с незаконным вмешательством посредством кибервекторов и любыми событиями, которые могут повлиять на безопасность полетов.

1.1.4 В этой связи и в целях надлежащего достижения целей семи основополагающих элементов авиационной стратегии кибербезопасности, а также для формирования концептуальных рамок кибербезопасности и был разработан настоящий план действий.

1.2 ЦЕЛЬ

1.2.1 Настоящий план – это "живой документ", который будет меняться по мере развития ситуации в области кибербезопасности и будет регулярно обновляться с целью отразить требуемые изменения, вытекающие, помимо прочего, из анализа пробелов и мероприятий, изложенных в главах 3 и 4. ПДоК содержит цели и будущие действия для реализации стратегии авиационной кибербезопасности ИКАО. Представленные в настоящем документе элементы отражают проделанную или выполняемую в настоящее время работу в различных регионах/государствах или отрасли. Он включает результаты анализа нынешней "как есть" ситуации в авиационной системе в плане кибербезопасности в сравнении с ситуацией "как будет", предложенной в указанной

стратегии, и содержит подробный план действий, который может стимулировать такую эволюцию в направлении реализации стратегического видения.

1.2.2 Учитывая значительный объем работы, который требуется выполнить для достижения целей и принятия мер, указанных в настоящем документе, в добавлении А предлагается поэтапный подход с определением краткосрочных, среднесрочных и долгосрочных задач.

1.3 КОНТЕКСТ РИСКА

1.3.1 Кибербезопасность – это не новая концепция в гражданской авиации. Однако поскольку угрозы для кибербезопасности приобретают все более распространенный характер, этот вопрос занимает одно из центральных мест при обсуждении и анализе рисков и уязвимости в рамках системы гражданской авиации. Сектор гражданской авиации в особенности подвержен риску, поскольку кибератаки с большей вероятностью будут успешными в таком секторе, компоненты которого функционально и в цифровом отношении все более взаимозависимы, а также потому, что используемые в настоящее время в секторе гражданской авиации механизмы киберзащиты еще не могут справиться с этой непрекращающейся и адаптирующейся угрозой.

1.3.2 Совсем недавно Группа экспертов ИКАО по авиационной безопасности оценила уровень риска, связанного с использованием уязвимости в террористических целях, как средний. Эта оценка основана на остаточной уязвимости в области кибербезопасности и исходит из того, что государства эффективно внедрили положения Приложения 17 *"Безопасность"*. Однако киберриски стремительно эволюционируют, и их следует оценивать в отношении всех типов кибернарушений, которые могут затронуть не только авиационную безопасность, но и безопасность полетов гражданской авиации. Более того, источник кибератак обычно трудно отследить и поэтому установление источника кибератак и судебное преследование за их совершение зачастую является сложным и трудным в осуществлении процессом, а жертвам атаки или их страховщикам приходится нести расходы, связанные с возмещением ущерба. В силу этих причин чрезвычайно важно, чтобы ИКАО, государства и отрасль сотрудничали в деле систематической реализации стратегии кибербезопасности.

1.4 ПРЕИМУЩЕСТВА ПЛАНА ДЕЙСТВИЙ

1.4.1 ПДоК призван гарантировать принятие ИКАО, государствами-членами и отраслью обязательств по реализации стратегии авиационной кибербезопасности и достижению целей, изложенных в ее семи основополагающих элементах. Надежный механизм кибербезопасности укрепит систему гражданской авиации и принесет пользу всему мировому авиационному сообществу.

Глава 2

ЦЕЛЬ

2.1 ЦЕЛЬ ПЛАНА ДЕЙСТВИЙ ПО ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ

2.1.1 Цель Плана действий по обеспечению кибербезопасности заключается в достижении целей, поставленных в каждом из семи основополагающих элементов стратегии кибербезопасности, а также в разработке надежного механизма кибербезопасности гражданской авиации.

2.1.2 Принципы, лежащие в основе настоящего плана действий, включают:

a) осознание государствами-членами своих обязательств в отношении кибербезопасности, вытекающих из *Конвенции о международной гражданской авиации* (Чикагская конвенция), по обеспечению безопасности полетов, авиационной безопасности и непрерывности деятельности гражданской авиации;

b) координацию мер по авиационной кибербезопасности, принимаемых полномочными органами государств-членов, с целью обеспечить эффективное и действенное глобальное управление авиационной кибербезопасностью;

c) обязательства всех заинтересованных сторон системы гражданской авиации продолжать развивать киберустойчивость в целях защиты авиации от кибератак, связанных с любыми исполнителями угроз, которые могут негативно повлиять на безопасность полетов, авиационную безопасность и непрерывность функционирования авиатранспортной системы.

2.2 ПРИМЕНЕНИЕ

2.2.1 Настоящий документ главным образом предназначен для государств – членов ИКАО и отрасли в качестве средства оказания им помощи в управлении рисками для кибербезопасности в гражданской авиации за счет применения комплексного, координированного и целостного подхода.

2.2.2 Государствам, отрасли и другим соответствующим заинтересованным сторонам следует предпринимать действия, вытекающие из настоящего плана действий.

Глава 3

СТРАТЕГИЧЕСКИЙ ПЛАН ДЕЙСТВИЙ

3.1 СЕМЬ ОСНОВОПОЛАГАЮЩИХ ЭЛЕМЕНТОВ СТРАТЕГИИ КИБЕРБЕЗОПАСНОСТИ

3.1.1 Приведенные в настоящей главе компоненты разработаны с целью предложить серию принципов, мер и действий, направленных на достижение целей семи основополагающих элементов стратегии авиационной кибербезопасности, а именно:

1. Международное сотрудничество
2. Управление
3. Действенное законодательство и нормативные положения
4. Политика в области кибербезопасности
5. Обмен информацией
6. Управление инцидентами и планирование мероприятий на случай аварийной обстановки
7. Наращивание потенциала, подготовка персонала и культура кибербезопасности

ОСНОВОПОЛАГАЮЩИЙ ЭЛЕМЕНТ 1. МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО
• Развивать сотрудничество на национальном и международном уровне между всеми заинтересованными сторонами. • Признавать на взаимной основе усилия (разработка мер, поддержание и совершенствование кибербезопасности), направленные на защиту гражданской авиации. • Добиваться регуляторной гармонизации на глобальном, региональном и национальном уровне с целью способствовать глобальной согласованности и обеспечить интероперабельность мер защиты. • Привлекать государства к решению проблем кибербезопасности международной гражданской авиации. • Содействовать и способствовать проведению международных мероприятий в области кибербезопасности. • Признать, что кибербезопасность является общей ответственностью во всех сегментах глобальной системы гражданской авиации.

ОСНОВОПОЛАГАЮЩИЙ ЭЛЕМЕНТ 2. УПРАВЛЕНИЕ
• Рекомендовать к реализации, поддерживать и развивать стратегию кибербезопасности ИКАО. • Разработать четкие национальные процессы управления и подотчетности в отношении кибербезопасности гражданской авиации. • Обеспечить координацию на уровне государств между ведомствами гражданской авиации и компетентными национальными органами по кибербезопасности. • Установить надлежащие каналы координации между различными государственными органами и отраслью. • Включить вопросы кибербезопасности в национальные программы обеспечения безопасности полетов и авиационной безопасности в гражданской авиации.

- Включить вопросы кибербезопасности в глобальные и региональные планы.
- Разработать общий базовый уровень для Стандартов и Рекомендуемой практики в области кибербезопасности.

ОСНОВОПОЛАГАЮЩИЙ ЭЛЕМЕНТ 3. ДЕЙСТВЕННОЕ ЗАКОНОДАТЕЛЬСТВО И НОРМАТИВНЫЕ ПОЛОЖЕНИЯ
• Обеспечить наличие в международных правовых документах надлежащего механизма предотвращения киберинцидентов, а также судебного преследования их виновников. • Проанализировать существующее национальное законодательство и, при необходимости, обновить или принять национальное законодательство, обеспечивающее предотвращение и расследование кибератак и судебное преследование за совершение кибератак, которые влияют на безопасность полетов, авиационную безопасность, эффективность или непрерывность деятельности гражданской авиации. • Обеспечить введение в действие надлежащих национальных нормативных положений и законодательства в области кибербезопасности гражданской авиации. • Разработать надлежащие рекомендации для государств и отрасли по вопросу внедрения положений о кибербезопасности.

ОСНОВОПОЛАГАЮЩИЙ ЭЛЕМЕНТ 4. ПОЛИТИКА В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ
• Обеспечить включение кибербезопасности в качестве компонента систем безопасности полетов и авиационной безопасности гражданской авиации и комплексных механизмов управления риском. • Обеспечить сопоставимость различных методик оценки риска для кибербезопасности гражданской авиации. • Разработать политику в области кибербезопасности с учетом полного жизненного цикла авиационных систем.

ОСНОВОПОЛАГАЮЩИЙ ЭЛЕМЕНТ 5. ОБМЕН ИНФОРМАЦИЕЙ
• Разработать или использовать существующие платформы и механизмы обмена информацией, которые соответствуют существующим положениям ИКАО, для обеспечения осведомленности о киберситуации и, следовательно, предотвращения, раннего обнаружения и смягчения последствий соответствующих киберсобытий. • Обеспечить информирование компетентного органа о любых киберинцидентах или уязвимостях, которые могут представлять значительный риск для безопасности полетов и/или авиационной безопасности.

ОСНОВОПОЛАГАЮЩИЙ ЭЛЕМЕНТ 6. УПРАВЛЕНИЕ ИНЦИДЕНТАМИ И ПЛАНИРОВАНИЕ МЕРОПРИЯТИЙ НА СЛУЧАЙ АВАРИЙНОЙ ОБСТАНОВКИ
• Обеспечить составление надлежащих и масштабируемых планов, предусматривающих непрерывность безопасного и надежного функционирования гражданской авиации в случае киберинцидентов. • Поощрять использование существующих планов на случай непредвиденных обстоятельств, включающих положения о реагировании на киберинциденты и восстановлении после них, а также о регулярном/периодическом проведении учений для проверки возможностей по обнаружению киберинцидентов, реагированию на киберинциденты и восстановлению после них.

ОСНОВОПОЛАГАЮЩИЙ ЭЛЕМЕНТ 7. НАРАЩИВАНИЕ ПОТЕНЦИАЛА, ПОДГОТОВКА ПЕРСОНАЛА И КУЛЬТУРА КИБЕРБЕЗОПАСНОСТИ
• Обеспечить надлежащую квалификацию персонала на основе ролевых моделей как в области авиационной безопасности, так и в области кибербезопасности. • Повысить осведомленность о кибербезопасности, включая деятельность по надлежащей киберпрофилактике. • Обеспечить включение в национальную образовательную структуру надлежащих учебных программ по авиационной кибербезопасности с целью обеспечения наличия багажа знаний по всем аспектам безопасности полетов и авиационной безопасности на всех уровнях организации, включая руководство высшего звена. • Способствовать инновациям и надлежащим научным исследованиям и разработкам в области кибербезопасности. • Включить кибербезопасность в стратегию ИКАО по следующему поколению авиационных специалистов.

Глава 4

РЕАЛИЗАЦИЯ, МОНИТОРИНГ И ПЕРЕСМОТР

4.1 РЕАЛИЗАЦИЯ

ПДоК предназначен для ИКАО, ее государств-членов, отрасли и других заинтересованных сторон. Каждой организации рекомендуется соблюдать контрольные сроки, установленные в дорожной карте (см. добавление A), в которой указываются приоритетные конечные результаты, действия и смежные задачи. Это поможет ИКАО, государствам и заинтересованным сторонам сосредоточить свои усилия и деятельность на принятии эффективных мер в целях создания надежного глобального механизма обеспечения авиационной кибербезопасности.

4.2 МОНИТОРИНГ И ПЕРЕСМОТР

ИКАО по мере необходимости будет пересматривать ПДоК. ИКАО также будет предоставлять обновленные сведения о состоянии выполнения задач и соблюдении планируемых сроков, указанных в ПДоК. Это будет включать области, в которых государства нуждаются в помощи в реализации ПДоК и/или в которых требуется помощь в развитии потенциала и другие соответствующие усилия.

4.3 РАБОТА В РАМКАХ ПАРТНЕРСКИХ ОТНОШЕНИЙ

В мероприятиях, направленных на неуклонное повышение кибербезопасности гражданской авиации, должны участвовать все авиационные заинтересованные стороны. ПДоК содержит общие рамки участия всех заинтересованных сторон и определяет действия, которые ИКАО, государствам-членам и отрасли необходимо предпринять для разработки общего механизма обеспечения кибербезопасности.

4.4 РОЛЬ ИКАО, ГОСУДАРСТВ И ЗАИНТЕРЕСОВАННЫХ СТОРОН

4.4.1 ИКАО будет играть важную глобальную руководящую роль и выполнять функцию контроля в реализации и координации ПДоК, включая:

- обновление ПДоК по мере необходимости;
- разработку и обновление Стандартов и Рекомендуемой практики (SARPS) и Правил аэронавигационного обслуживания (PANS), а также руководств и другого инструктивного материала;
- мониторинг и анализ ландшафта киберугроз и рисков;
- оказание целенаправленной помощи для устранения недостатков в области кибербезопасности гражданской.

4.4.2 Государствам и отрасли также предстоит сыграть важную роль в деле реализации и обеспечения эффективности ПДоК. Государствам и заинтересованным сторонам рекомендуется демонстрировать из года в год достигнутые успехи в реализации плана.

Глава 5

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО

5.1 СОСТАВЛЕНИЕ ПЕРЕЧНЯ ИНИЦИАТИВ В ОБЛАСТИ АВИАЦИОННОЙ КИБЕРБЕЗОПАСНОСТИ

5.1.1 Будет составлен перечень инициатив в области кибербезопасности, который будет обновляться и размещаться на портале ИКАО для использования соответствующими аудиториями. Этот перечень будет содержать уже существующие инициативы, а также включать существующие инициативы в авиационной области, касающиеся кибербезопасности, на глобальном, региональном или национальном уровне. В этом перечне будут учитываться не только инициативы в области авиационной кибербезопасности, но также инициативы, которые в конечном счете имеют отношение к гражданской авиации (например, кибербезопасность в других сферах транспорта или секторах, таких как энергетический, финансовый).

5.2 СОЗДАНИЕ ОБЩЕЙ ОСНОВЫ ДЛЯ ИНТЕРОПЕРАБЕЛЬНОСТИ МЕР КИБЕРБЕЗОПАСНОСТИ И СИСТЕМ УПРАВЛЕНИЯ [2]

5.2.1 Для того чтобы обеспечить единообразное, безопасное и интероперабельное управление информационными технологиями/системами связи, государствам и отрасли следует руководствоваться соответствующими принципами и ввести в действие надлежащие инструменты/системы.

5.2.2 Поскольку доверие лежит в основе эффективного, единообразного и интероперабельного управления обменом информацией, следует поддержать разработку международного авиационного механизма доверия, способствующего управлению информацией и обеспечению интероперабельности; кроме того, политика и процедуры должны в максимально возможной степени применяться всеми соответствующими заинтересованными сторонами.

5.2.3 Интероперабельности мер кибербезопасности и управления можно также достичь за счет участия в различных типах международных соглашений о сотрудничестве. Для обеспечения возможности сотрудничества при соблюдении применимой политики в области конфиденциальности, информационной безопасности и национальной безопасности следует разработать типовые формы для таких соглашений. В этой связи в качестве базовых принципов типовых соглашений необходимо определить следующие аспекты:

- предмет и цель соглашения;
- субъекты, которые могли бы заключить такие соглашения;
- роли и обязанности таких субъектов;
- меры, которые могут быть использованы для повышения кибербезопасности в гражданской авиации и которые подлежат координации.

[2] Системы управления в данном контексте включают системы управления риском, но не ограничиваются ими.

5.2.4 Международные соглашения должны иметь целью:

- установление диалога между заинтересованными сторонами для обсуждения средств снижения коллективного риска и защиты национальной и международной инфраструктуры гражданской авиации;
- введение мер снижения и смягчения риска для противодействия угрозам кибербезопасности гражданской авиации;
- обмен информацией о национальном законодательстве, национальных стратегиях, политике и передовой практике в сфере гражданской авиации, связанных с кибербезопасностью;
- принятие мер в поддержку наращивания потенциала в области кибербезопасности там, где это требуется.

5.2.5 В контексте, при котором различные авиационные заинтересованные стороны могут использовать множество методических принципов и моделей, а также различную терминологию, крайне важно создать общий лексикон и основу для взаимопонимания, в частности, в отношении кибербезопасности гражданской авиации. В этой связи на уровне ИКАО необходимо разработать в тесном сотрудничестве с государствами-членами и отраслью общий набор принципов для надлежащего, глобального и координированного управления кибербезопасностью. Будет проведен анализ существующего механизма, с тем чтобы определить наилучший способ достижения "бесшовного" и эффективного согласования этих принципов и моделей.

5.3 РАЗРАБОТКА ОБЩЕЙ ТЕРМИНОЛОГИИ

5.3.1 Под эгидой ИКАО будет разработана общая терминология, относящаяся к кибербезопасности гражданской авиации, с учетом существующей терминологии в области кибербезопасности и терминологии и концептуальных основ в области авиации, с тем чтобы все авиационные заинтересованные стороны, независимо от характера и уровня их деятельности, могли понимать друг друга.

5.3.2 Цель заключается в содействии проведению мероприятий в области кибербезопасности. Это не означает, что для всех терминов будет выработано и/или согласовано единое определение. Вполне приемлемо, если будут существовать различные определения одного и того же термина (например, вероятность, серьезность, событие и т. д.) при условии, что они относятся к конкретному контексту и такое повторение терминов не создает путаницу, которая может привести к неэффективности управления рисками для кибербезопасности гражданской авиации. Говоря конкретно, с учетом того, что на комплексном управлении рисками для безопасности полетов и авиационной безопасности делается все больший акцент, ИКАО необходимо уделить очень пристальное внимание обеспечению надлежащего согласования терминологии. Ссылаясь на первоначальное заявление о контексте, упомянутое выше, и с учетом уточнения различий между авиационной безопасностью, касающейся управления незаконными и умышленными актами, и безопасностью полетов, имеющей дело с умышленными, неумышленными и случайными факторами угрозы, вопросы комплексного управления риском требуют дополнительного уточнения, поскольку они могут охватывать проблемы как авиационной безопасности, так и безопасности полетов (за основу можно взять определения из Приложения 17 и Приложения 19 ИКАО). Говоря точнее, с учетом различия объектов внимания дисциплин безопасности полетов и авиационной безопасности (безопасность полетов направлена на противодействие умышленным, неумышленным и случайным факторам угрозы, а авиационная безопасность нацелена на предотвращение незаконных и умышленных актов) внедрение комплексного управления рисками, охватывающего обе дисциплины, требует уточнения сферы охвата и назначения используемых терминов.

5.4 РАЗРАБОТКА ТИПОВОЙ СХЕМЫ ОБМЕНА ИНФОРМАЦИЕЙ/ ВЗАИМОДЕЙСТВИЯ В АВИАЦИИ

5.4.1 Необходимой предпосылкой обеспечения правильного понимания ландшафта киберрисков является общая структура для определения высокоуровневых функциональных схем с описанием обмена информацией между всеми авиационными субъектами деятельности. Для достижения понимания ландшафта киберрисков необходима общая структура для определения высокоуровневых схем обмена информацией между всеми авиационными заинтересованными сторонами.

5.4.2 Эта высокоуровневая схема обмена информацией/взаимодействия должна носить достаточно общий характер, чтобы охватить все типы авиационных операций, и должна, насколько это возможно, не зависеть от реализованных физических и/или технических архитектур (функциональный/ сервисный подход). Высокоуровневая схема должна, к примеру, включать потоки цифровых данных для организации воздушного движения и деятельности аэропортов, а также потоки цифровых данных для воздушных судов, выполняющих полет/проходящих техническое обслуживание. В этой высокоуровневой схеме должны быть отражены любые усилия, уже осуществляемые другими группами. Цель заключается в том, чтобы каждая заинтересованная сторона могла составить/адаптировать/модифицировать свою собственную схему в части способов взаимодействия с другими заинтересованными сторонами. В конечном счете каждая заинтересованная сторона должна иметь возможность разработать или адаптировать такую схему к своим индивидуальным условиям. Таким образом, результаты оценок риска для авиационной безопасности, проводимых каждым партнером по своей собственной методике и критериям (которые стали сопоставимы на основе общего механизма оценки риска – см. раздел 5.6), могут быть предоставлены другим заинтересованным сторонам и использоваться ими по мере возможности. В рамках сотрудничества с использованием сопоставимых методик оценки риска для авиационной безопасности и схемы обмена информацией/взаимодействия заинтересованные стороны смогут уяснить, каким образом риски могут далее распространиться на других партнеров по риску или быть ими устранены, и таким образом они будут способствовать обмену информацией о рисках, с которыми сталкивается или которые вызывает каждая сторона.

5.5 СОЗДАНИЕ СИСТЕМЫ МЕЖОРГАНИЗАЦИОННОГО ОБМЕНА ИНФОРМАЦИЕЙ О РИСКАХ

5.5.1 Существует множество содержащих стандарты и инструктивный материал документов, в которых говорится об ответственности каждой организации за управление своей собственной кибербезопасностью в части внутренних систем, процессов, продуктов и данных. Однако, учитывая тот факт, что с одинаковыми рисками для кибербезопасности гражданской авиации сталкиваются многие заинтересованные стороны, необходимо рассматривать этот вопрос шире, а не только в рамках отдельных организаций. Для эффективного и действенного управления общим риском необходимо уделять особое значение обмену информацией о рисках, что неизбежно в условиях, в которых системы, процессы, продукты или данные используются совместно или передаются из одной организации в другую.

5.5.2 Следует рассмотреть возможность заключения внешних соглашений со сторонними поставщиками, чтобы обеспечить обмен конфиденциальной информацией о кибербезопасности между организацией и соответствующими полномочными/регулирующими органами в целях содействия управлению рисками и угрозами во всей цепи поставок.

5.6 ОПРЕДЕЛЕНИЕ КРИТЕРИЕВ СОПОСТАВИМОСТИ ПОЗИЦИЙ В ОТНОШЕНИИ ОЦЕНКИ РИСКОВ

5.6.1 В контексте, при котором риски распространяются на несколько организаций, крайне важно, чтобы заинтересованные стороны могли осознать весь масштаб рисков и понять соответствующую потребность других заинтересованных сторон в управлении этими рисками. В этом контексте следует разработать критерии, которые будут способствовать легкому пониманию и сопоставимости оценок рисков для кибербезопасности.

5.7 ОБЕСПЕЧЕНИЕ НАДЛЕЖАЩЕЙ КООРДИНАЦИИ ГРАЖДАНСКИХ И ВОЕННЫХ ОРГАНОВ

5.7.1 По возможности и в соответствии с национальным законодательством, включая требования национальной безопасности и национальной обороны, но не ограничиваясь ими, компетентным органам гражданской авиации и военным органам следует создать возможности и процессы для сотрудничества по вопросам, связанным с авиационной кибербезопасностью.

5.7.2 Большую пользу в деле выявления потенциальных киберугроз и рисков может принести заблаговременный обмен информацией о кибербезопасности и координация между гражданскими и военными авиационными органами, способствуя тем самым успешному устранению киберрисков для авиационной системы.

5.7.3 Обмен информацией между гражданскими и военными авиационными органами также важен при управлении кризисными ситуациями, связанными с кибербезопасностью. Государства могут оказывать поддержку своим национальным органам гражданской авиации и военным органам в создании договоренности, способствующей по мере возможности обмену информацией посредством соответствующих механизмов.

5.8 СОДЕЙСТВИЕ ПРОВЕДЕНИЮ ГЛОБАЛЬНЫХ И РЕГИОНАЛЬНЫХ МЕРОПРИЯТИЙ ПО КИБЕРБЕЗОПАСНОСТИ В ГРАЖДАНСКОЙ АВИАЦИИ

5.8.1 ИКАО по мере необходимости будет поддерживать и планировать организацию глобальных и региональных мероприятий с целью содействия обеспечению кибербезопасности в гражданской авиации.

Глава 6

УПРАВЛЕНИЕ

6.1 СОЗДАНИЕ СТРУКТУРЫ УПРАВЛЕНИЯ

6.1.1 ИКАО следует создать внутреннюю структуру управления авиационной кибербезопасностью, которая обеспечивает целостный, междисциплинарный и основанный на оценке риска подход к кибербезопасности и киберустойчивости во всех соответствующих авиационных сферах и областях экспертных знаний.

6.1.2 Кроме того, государствам следует определить и внедрить национальные структуры управления и подотчетности в области кибербезопасности гражданской авиации, обеспечив разработку и внедрение национальных и международных требований в области кибербезопасности и киберустойчивости, а также определив роли и обязанности каждой заинтересованной стороны на национальном уровне. В ходе такой разработки следует также учитывать необходимую координацию между национальными полномочными органами гражданской авиации и компетентными органами в области кибербезопасности.

6.2 РАЗРАБОТКА ДОЛГОСРОЧНОГО(ЫХ) ПЛАНА(ОВ) ПО КИБЕРБЕЗОПАСНОСТИ

6.2.1 Рекомендуется надлежащим образом согласовать План действий по обеспечению кибербезопасности (ПДоК) с существующими Глобальным планом обеспечения авиационной безопасности (ГПАБ), Глобальным аэронавигационным планом (ГАНП) и Глобальным планом обеспечения безопасности полетов (ГПБП), и следует включить в эти планы и акцентировать аспекты кибербезопасности, где это уместно.

6.2.2 В целях обеспечения надлежащего осуществления и применения глобальных планов на национальном уровне государствам настоятельно рекомендуется включать согласованные в национальном масштабе соответствующие действия, связанные с кибербезопасностью, в свои национальные программы по безопасности полетов и авиационной безопасности и аэронавигационные планы.

6.3 РАЗРАБОТКА СИСТЕМЫ УПРАВЛЕНИЯ И ПОДОТЧЕТНОСТИ

6.3.1 ИКАО следует разработать инструктивный материал по политике в области кибербезопасности в целях обеспечения гармонизации и согласованности глобальной, региональной и национальной политики в этой области.

6.3.2 Меры по управлению кибербезопасностью должны быть обусловлены проводимой политикой и должно быть обеспечено их введение; также необходимо определить принципы подотчетности для контроля соблюдения.

6.3.3 Государствам следует предпринимать значимые действия по непрерывному повышению эффективности, качества и согласованности процессов управления кибербезопасностью на национальном уровне.

6.3.4 При необходимости системы менеджмента информационной безопасности (СМИБ) могут быть эффективными инструментами управления кибербезопасностью и могут быть внедрены на государственном или организационном уровне[3].

[3] При разработке программы по кибербезопасности на национальном уровне государства могут обратиться к стандарту ИСО 27001 для определения принципов руководства, например: обеспечение включения в процессы организации требований системы менеджмента информационной безопасности; обеспечение наличия требуемых ресурсов и обеспечение достижения целей, заложенных в системе менеджмента информационной безопасности.

Глава 7

ДЕЙСТВЕННОЕ ЗАКОНОДАТЕЛЬСТВО И НОРМАТИВНО-ПРАВОВАЯ БАЗА

7.1 РАССМОТРЕНИЕ СУЩЕСТВУЮЩИХ ДОКУМЕНТОВ МЕЖДУНАРОДНОГО ВОЗДУШНОГО ПРАВА В ЧАСТИ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ

7.1.1 ИКАО проведет анализ существующих документов международного воздушного права, с тем чтобы выявить действительные и потенциальные пробелы в отношении киберрисков и предложить возможные решения для устранения выявленных пробелов, если таковые имеются, в целях дальнейшей защиты гражданской авиации.

7.2 ПРИВЕДЕНИЕ ПОЛОЖЕНИЙ ИКАО В СООТВЕТСТВИЕ С ПОТРЕБНОСТЯМИ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

7.2.1 По мере развития кибербезопасности в авиации может возникнуть потребность в разработке положений в дополнение к существующим SARPS и PANS. Это должно осуществляться на индивидуальной основе, имея в виду, что добавления новых положений SARPS или PANS следует избегать, насколько это возможно, и при необходимости такое добавление должно координироваться между всеми соответствующими заинтересованными сторонами.

7.3 РАТИФИКАЦИЯ ПЕКИНСКИХ КОНВЕНЦИИ И ПРОТОКОЛА

7.3.1 Государствам рекомендуется ратифицировать *Конвенцию о борьбе с незаконными актами в отношении международной гражданской авиации* (Пекинская конвекция 2010 года) и *Протокол, дополняющий Конвенцию о борьбе с незаконным захватом воздушных судов* (Пекинский протокол 2010 года).

7.4 ГОСУДАРСТВА ДОЛЖНЫ ОБЕСПЕЧИТЬ РАЗРАБОТКУ И ПРИМЕНЕНИЕ НА НАЦИОНАЛЬНОМ УРОВНЕ НАДЛЕЖАЩЕГО ЗАКОНОДАТЕЛЬСТВА И НОРМАТИВНЫХ ПОЛОЖЕНИЙ

7.4.1 Государствам рекомендуется проанализировать свои существующие национальные нормативно-правовые системы в области кибербезопасности и гражданской авиации с целью определения существующих пробелов, а также обеспечить принятие надлежащего законодательства и правил в отношении конкретных элементов кибербезопасности гражданской авиации. Другим ключевым компонентом является механизм правоприменения, который государствам рекомендуется внедрить (если он еще не существует в их национальных правовых рамках) для криминализации и судебного преследования в случае совершения незаконных актов, направленных против гражданской авиации, с использованием киберсредств.

Глава 8

ПОЛИТИКА В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

8.1 РАЗРАБОТКА И ВНЕДРЕНИЕ ПОЛИТИКИ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

8.1.1 Необходимо разработать политику в области кибербезопасности на национальном и организационном уровнях. Государства должны иметь четкую и действенную политику в области кибербезопасности, включающую:

- цели, вытекающие из результатов оценок рисков для кибербезопасности гражданской авиации;
- обязательство соблюдать соответствующие требования и метод оценки соблюдения требований;
- положения, касающиеся управления и координации с внешними зависимыми сторонами (см. главу о международном сотрудничестве);
- обязательство постоянно совершенствовать механизм обеспечения кибербезопасности;
- положения, обеспечивающие, что политика полностью документирована и доступна в виде официального документа;
- положения, обеспечивающие, что политика должным образом распространяется.

8.2 ВЫЯВЛЕНИЕ И ОЦЕНКА КИБЕРРИСКОВ ДЛЯ ГРАЖДАНСКОЙ АВИАЦИИ

8.2.1 Одна из проблем выявления риска и его оценки заключается в способности предвидеть весьма быстрые изменения в происхождении и характеристиках угроз. Предвидение меняющихся угроз чрезвычайно важно для того, чтобы авиатранспортная система могла упреждающе адаптировать свою стратегию защиты не только исходя из текущих угроз, но также с учетом и потенциальных будущих угроз. Благодаря такому предвидению сектор гражданской авиации должен быть способен проявить бóльшую степень проактивности в контексте, когда существует асимметрия между нарушителями, которые весьма быстро ориентируются и адаптируются, и защищающимися сторонами, которые, учитывая сложность подлежащей защите системы, реагируют достаточно медленно. При этом сценарии такой упреждающий подход приобретает еще большее значение. Таким образом, для содействия смягчению рисков для кибербезопасности следует разработать механизм идентификации и оценки таких рисков, поддерживающий эту необходимость.

8.2.2 Рекомендуется выявлять и оценивать риски для кибербезопасности, принимая во внимание все потенциальные последствия атаки на систему гражданской авиации (авиационная безопасность, безопасность полетов, эффективность, устойчивость, бесперебойность обслуживания и т. д.), а также все потенциальные источники угрозы и существующие уязвимости перед такими угрозами. Эта деятельность должна базироваться на матрицах киберриска, ранее разработанных под эгидой Рабочей группы по угрозам и рискам (WGTR) Группы экспертов по авиационной безопасности.

8.2.3 Поскольку со значительной частью рисков для кибербезопасности гражданской авиации сталкиваются многие заинтересованные стороны, рекомендуется рассмотреть схему обмена

информацией/взаимодействия в авиации (см. главу 5.1). Эту схему следует использовать как средство, гарантирующее исчерпывающий охват рассматриваемых сценариев и способствующее пониманию всеми заинтересованными сторонами того, как они взаимодействуют друг с другом, и своей зависимости от рисков.

8.2.4 Поскольку уровень серьезности рисков для кибербезопасности будет со временем меняться (и эти риски могут видоизменяться быстрее по сравнению с другими видами рисков), рекомендуется изучить способы адаптации любых мер реагирования мировой авиации на эти риски, которые могут быть применены на оперативной и согласованной основе (например, балансирование потребности в авиационных стандартах, инструктивных материалах, неавиационной передовой практике и использование/опора на ответные меры в других сферах деятельности).

8.2.5 Рекомендуется, чтобы деятельность по выявлению и оценке рисков для кибербезопасности в полной мере осуществлялась и координировалась группой экспертов, состоящей из экспертов в области кибербезопасности гражданской авиации, или, если это невозможно, группой экспертов в области киберпространства и гражданской авиации, желательно с обширным опытом в области кибербезопасности.

8.2.6 Эта группа экспертов должна отвечать за разработку заявления о глобальном контексте риска в области кибербезопасности.

Глава 9

ОБМЕН ИНФОРМАЦИЕЙ

Обмен информацией, связанной с кибербезопасностью, необходим для управления рисками для кибербезопасности системы гражданской авиации. Исходя из понимания того, что содействие обмену информацией является ключевым элементом создания культуры кибербезопасности, заинтересованным сторонам гражданской авиации следует разработать или использовать существующие программы, позволяющие осуществлять в максимально возможной степени обмен информацией внутри их организаций и с внешними партнерами. Посредством этих программ им следует создать партнерские связи и обмениваться существенной информацией с другими заинтересованными сторонами, владеющими и управляющими инфраструктурой гражданской авиации, и разработать процедуры и практику обмена информацией внутри их организаций.

Эти программы обмена информацией должны обеспечивать возможность разработки, эксплуатации и регулировки киберзащиты гражданской авиации в соответствии с известными и возникающими киберугрозами. Они должны способствовать развитию:

- ситуационной осведомленности как в обычных повседневных операциях, так и в кризисной ситуации или при возникновении инцидента или происшествия;
- оперативного и тактического управления рисками в предвидении угроз и в ответ на них;
- стратегического планирования в целях создания потенциала для укрепления кибербезопасности и устойчивости на будущее.

9.1 РАЗРАБОТКА СИСТЕМЫ ОБМЕНА ИНФОРМАЦИЕЙ О РИСКАХ

9.1.1 Обмен киберинформацией носит двусторонний и многосторонний характер – любая комбинация обмена по горизонтали и вертикали (на национальном, региональном, глобальном уровне) между следующими сторонами:

- национальные органы по обеспечению кибербезопасности;
- национальные ведомства гражданской авиации;
- национальные военные авиационные органы;
- другие авиационные заинтересованные стороны (эксплуатанты, поставщики обслуживания и изготовители);
- неавиационные заинтересованные стороны (поставщики ИТ-решений и услуг связи и участники цепи поставок).

9.1.2 Установлено, что существует много типов информации, касающейся кибербезопасности, например:

- *Киберразведданные*, такие как ландшафт угроз, разведданные о возможностях и намерениях киберзлоумышленников.
- *Показатели компрометации (IoCs)*.
- *Тактика, методы и процедуры (TTPs)*, например сценарии атак и предпочтительные методы, используемые хакерами.

- *Уязвимости,* например в аппаратном оборудовании, программном обеспечении, обслуживании, протоколе, стандарте и т. д., включая возможные сценарии эксплуатации.
- *Донесения об инцидентах.*

9.1.3 В зависимости от национального законодательства и характера киберинформации могут существовать различные методы и ограничения в плане обмена информацией с разными получателями (например, национальным органом по кибербезопасности, национальным ведомством гражданской авиации, национальными военными авиационными органами и другими авиационными заинтересованными сторонами).

9.1.4 На глобальном, региональном и национальном уровнях необходимо определить потребности (в частности, в кризисные периоды) и политику в области обмена информацией и сотрудничества.

9.1.5 При распространении и более широком обмене киберинформацией рекомендуется использовать протокол "Светофор" (TLP)[4], чтобы указать уровень распространения/ограничений.

9.1.6 Из киберинформации, которая может содержать закрытую информацию, следует в максимально возможной степени удалить идентификационные или конфиденциальные данные, прежде чем она будет предоставлена, что гораздо лучше, чем вообще не обмениваться такой информацией.

9.2 РАЗРАБОТКА ПРИНЦИПОВ И РЕКОМЕНДАЦИЙ ОТНОСИТЕЛЬНО ОТВЕТСТВЕННОГО РАСКРЫТИЯ ИНФОРМАЦИИ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИМИ ОРГАНИЗАЦИЯМИ, ЗАНИМАЮЩИМИСЯ ВОПРОСАМИ БЕЗОПАСНОСТИ

9.2.1 Принимая во внимание все больший интерес, который проявляет научно-исследовательское сообщество к вопросам кибербезопасности гражданской авиации, и во избежание безответственного раскрытия результатов исследований, которое может причинить ущерб безопасности полетов, авиационной безопасности, эффективности или непрерывности деятельности гражданской авиации, необходимо определить принципы ответственного раскрытия информации об уязвимостях, которые могут быть обнаружены научно-исследовательскими организациями, занимающимися вопросами безопасности, или третьими сторонами. При этом следует принимать во внимание рекомендацию 4.4 стратегии кибербезопасности.

9.2.2 Инструктивные указания относительно этих принципов (касающиеся, помимо других вопросов, например, обнаружения, уведомления изготовителей, расследования, уведомления отрасли, разрешения, и, наконец, публичного выпуска) должны быть выработаны с участием, с одной стороны, научно-исследовательских организаций и третьих сторон, а с другой стороны, авиационных ведомств и авиационных заинтересованных сторон для гарантии в максимально возможной степени того, что такая деятельность по исследованию, обнаружению и раскрытию уязвимых мест не окажет негативного воздействия на безопасность полетов и предоставление обслуживания. В идеальном случае инструктивные указания должны затрагивать не только процессы ответственного раскрытия информации, но также вопросы осведомленности и образовательные компоненты.

[4] См. инструктивный материал ИКАО: Руководство по протоколу "Светофор".

9.3 СОЗДАНИЕ ГЛОБАЛЬНОЙ СЕТИ РЕГИОНАЛЬНЫХ/НАЦИОНАЛЬНЫХ ОРГАНОВ ПО КИБЕРБЕЗОПАСНОСТИ ДЛЯ ЦЕЛЕЙ ГРАЖДАНСКОЙ АВИАЦИИ

9.3.1 В государствах и отрасли отсутствует единообразие в части распределения ответственности за кибербезопасность, а специалисты, обладающие надлежащими знаниями в этой области, рассредоточены по самым разным авиационным и неавиационным организациям и функциональным областям. Главная проблема, присущая такому разнообразию, связана с трудностью определения надлежащего координатора в рамках организации и создания и использования официальных каналов связи между заинтересованными сторонами. Рекомендации по назначению и использованию единого координатора по вопросам кибербезопасности гражданской авиации в государствах и организациях могут облегчить создание глобальных, региональных и национальных каналов связи, формирование надлежащих сообществ в области кибербезопасности и развитие культуры кибербезопасности.

9.4 ГЛОБАЛЬНАЯ СИСТЕМА ОБМЕНА ИНФОРМАЦИЕЙ О КИБЕРБЕЗОПАСНОСТИ ДЛЯ АВИАЦИИ

9.4.1 Системы обмена информацией для гражданской авиации могут быть созданы на глобальном, региональном и/или национальном уровне и взаимосвязаны в целях содействия обмену информацией о кибербезопасности.

9.4.2 Форумы по обмену информацией могут предусматривать обмен между государственными структурами, между государственными и частными структурами и между частными структурами. Заинтересованные стороны должны участвовать в сообществах, пользующихся доверием, для содействия обмену как передовым опытом, так и информацией об угрозах.

Глава 10

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ И ПЛАНИРОВАНИЕ МЕРОПРИЯТИЙ НА СЛУЧАЙ АВАРИЙНОЙ ОБСТАНОВКИ

10.1 РАЗРАБОТКА СРЕДСТВ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ И ПЛАНИРОВАНИЕ МЕРОПРИЯТИЙ НА СЛУЧАЙ АВАРИЙНОЙ ОБСТАНОВКИ

10.1.1 Всем заинтересованным сторонам настоятельно рекомендуется разработать и испытать планы реагирования на инциденты и планы мероприятий на случай аварийной обстановки в координации с их оперативными партнерами, что включает в себя:

- использование уже разработанных и существующих планов мероприятий на случай непредвиденных обстоятельств и/или внесение в них изменений в целях включения положений о кибербезопасности;
- обеспечение и поддержание заинтересованными сторонами гражданской авиации надлежащей масштабируемости, обеспечивающей безопасность полетов, авиационную безопасность и непрерывность деятельности воздушного транспорта во время возможных киберинцидентов;
- разработку положений о механизмах реагирования на инциденты в области кибербезопасности и восстановления после них, в том числе планов мероприятий на случай непредвиденных обстоятельств и аварийной обстановки;
- привлечение военных авиационных органов к участию в процессе планирования, с тем чтобы проактивно установить линии связи;
- достижение приемлемых уровней эффективности и соблюдение требований в отношении поддержания минимальных уровней обслуживания ключевых служб;
- разработку согласованной классификации донесений о киберинцидентах и координацию систем представления данных об инцидентах в области гражданской авиации и в области кибербезопасности на национальном, региональном и, по возможности, международном уровнях;
- периодическое проведение авиационными заинтересованными сторонами практических учений для проверки обоснованности предположений, сделанных при планировании и на теоретических учениях.

10.2 ОБНАРУЖЕНИЕ И АНАЛИЗ ИНЦИДЕНТОВ И СРЕДСТВА РЕАГИРОВАНИЯ НА НИХ НА УРОВНЕ ЗАИНТЕРЕСОВАННЫХ СТОРОН

10.2.1 По мере возможности необходимо внедрить планы реагирования на инциденты, а заинтересованным сторонам следует разработать механизмы для обнаружения и анализа инцидентов в области кибербезопасности и реагирования на них на всех уровнях. Важно следить за состоянием кибербезопасности таких систем/служб, которые считаются важными для обеспечения деятельности гражданской авиации, с тем чтобы обнаруживать потенциальные проблемы и постоянно отслеживать эффективность защитных мер безопасности. В случае обнаружения инцидентов в области кибербезопасности их следует проанализировать и ввести в действие соответствующие планы реагирования; эти планы должны включать меры по смягчению и ограничению последствий инцидентов в области кибербезопасности.

10.3 СОЗДАНИЕ ПОДРАЗДЕЛЕНИЯ ПО КООРДИНАЦИИ ДЕЙСТВИЙ В КРИЗИСНОЙ СИТУАЦИИ ДЛЯ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ ГРАЖДАНСКОЙ АВИАЦИИ

10.3.1 По возможности следует создать (на основе уже существующих механизмов) подразделение по координированию кризисных ситуаций в гражданской авиации, в которое войдут эксперты в области кибербезопасности гражданской авиации, с привлечением, по мере необходимости, представителей военных авиационных органов.

10.3.2 Следует на регулярной основе проводить периодические учения, в частности теоретические учения (ТТХ) с привлечением, по мере необходимости, представителей всех соответствующих заинтересованных сторон отрасли.

Глава 11

НАРАЩИВАНИЕ ПОТЕНЦИАЛА, ПОДГОТОВКА ПЕРСОНАЛА, КУЛЬТУРА КИБЕРБЕЗОПАСНОСТИ И ОБРАЗОВАНИЕ

11.1 НАРАЩИВАНИЕ ТЕХНИЧЕСКОГО ПОТЕНЦИАЛА, ПОДГОТОВКА ПЕРСОНАЛА, КУЛЬТУРА КИБЕРБЕЗОПАСНОСТИ И ОБРАЗОВАТЕЛЬНЫЕ МАТЕРИАЛЫ

11.1.1 Образование, подготовка персонала и повышение осведомленности в области кибербезопасности гражданской авиации должны быть определены и популяризированы на глобальном, региональном и национальном уровнях.

11.1.2 Культуру кибербезопасности и образовательные мероприятия в этой области следует популяризировать во всех организациях гражданской авиации; эта инициатива должна исходить от старшего руководства и призвана подчеркнуть ключевые роли представителей различных сторон и ожидаемые результаты. Такие мероприятия должны обеспечить формирование багажа знаний в области кибербезопасности, связанного со всеми аспектами безопасности полетов и авиационной безопасности, и должны включать:

- понятия принципов обеспечения безопасности на этапе разработки для смягчения киберугроз в координации с отвечающим за безопасность полетов сообществом. Эти понятия должны помочь отвечающему за безопасность полетов сообществу принимать более обоснованные решения для противодействия киберугрозам;
- координированный подход между заинтересованными сторонами, имеющими отношение к обеспечению авиационной безопасности и безопасности полетов, признающий, что меры контроля авиационной безопасности не должны негативно влиять на безопасность полетов, создающий возможность для передачи технических знаний и обеспечивающий принятие обоснованных решений на базе одинаково понимаемого ландшафта рисков;
- понятия практики киберпрофилактики для эксплуатационного и вспомогательного персонала, которая должна способствовать предотвращению потенциальных негативных последствий для системы гражданской авиации, вызываемых применением возрастающего числа готовых коммерческих готовых (COTS) продуктов и неспецифических вредоносных программных средств;
- понятия "справедливой культуры" от отвечающего за безопасность полетов сообщества для обеспечения возможности и стимулирования самостоятельных донесений о событиях, вызванных непреднамеренным поведением персонала (например, непреднамеренное неправильное обращение с USB-носителем).

11.1.3 При проведении этих мероприятий следует делать акцент на последствиях или потенциальных последствиях.

11.1.4 Формирование такой культуры кибербезопасности и популяризация культуры кибербезопасности и образовательных материалов в этой области должны способствовать взаимному/общему пониманию в сообществах, отвечающих за безопасность полетов и авиационную

безопасность, ландшафта рисков в области кибербезопасности, а также укреплению взаимной уверенности в принимаемых контрмерах.

11.1.5 ИКАО следует поощрять осуществление транснациональных/трансрегиональных программ обмена в области образования и подготовки по кибербезопасности.[5]

11.1.6 Культура кибербезопасности и образовательные мероприятия в этой области должны делать акцент не только на функционировании систем, но скорее на их полном жизненном цикле, включая:

- требование (безопасность – неотъемлемая часть уже на этапе определения требования);
- проектирование (следуя стратегии обеспечения безопасности на этапе проектирования, безопасность аппаратных средств, программного обеспечения и данных, управление изменениями, управление уязвимостью);
- разработка (безопасная среда, непрерывное и комплексное тестирование системы безопасности);
- изготовление/приобретение (включая информационные и операционные технологии цепи поставок аппаратных средств и программного обеспечения);
- эксплуатацию (включая управление доступом, целостность данных, безопасное функционирование систем);
- техническое обслуживание (включая стратегию внесения исправлений и обновлений);
- ликвидацию (включая управление идентификаторами и остаточными данными на запоминающих устройствах).

[5] Например, инициативы по межнациональному кампусу или сеть и центры ЕС по компетенции в области кибербезопасности.

Глава 12

ВЫВОД

План действий по обеспечению кибербезопасности объединяет усилия ИКАО, государств, отрасли и других заинтересованных сторон в применении целостного и координированного подхода к решению текущих и возникающих проблем в области кибербезопасности. Он также подчеркивает, что кибербезопасность является комплексной проблемой и затрагивает все сферы авиационного сектора. Этот план способствует осуществлению стратегии авиационной кибербезопасности ИКАО и продвижению к созданию надежного глобального механизма обеспечения кибербезопасности.

— — — — — — — —

ДОБАВЛЕНИЕ A

Дорожная карта реализации Пана действий по обеспечению кибербезопасности

ОБЩИЕ НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ ПО ОСУЩЕСТВЛЕНИЮ СТРАТЕГИИ КИБЕРБЕЗОПАСНОСТИ

Приоритетный результат	**РАЗРАБОТКА ГЛОБАЛЬНОГО И СОГЛАСОВАННОГО КОНЦЕПТУАЛЬНОГО ВИДЕНИЯ**
Приоритетные действия	• Признать, что крайне важно разработать всеобъемлющее и согласованное концептуальное видение в области кибербезопасности в качестве основы для надежного и координированного управления на глобальном уровне риском для кибербезопасности авиации. • Признать, что сектор гражданской авиации должен быть устойчив к кибератакам и должен обеспечивать безопасность своих операций, и пользуется доверием в глобальном масштабе, и в то же время продолжает использовать инновации и развиваться. • Признать, что проблемы рисков для кибербезопасности гражданской авиации следует решать в рамках Конвенции о международной гражданской авиации.

Действия

Действие #	**Исполнитель**	**Конкретные меры/задачи**	**Показатели**	**Приоритет**	**Дата начала реализации**
ПДоК 0.1	ICAO, государства-члены и отрасль	ИКАО должна разработать типовую политику в области кибербезопасности для использования государствами-членами при разработке собственной национальной/организационной политики.	Типовой образец имеется для предоставления государствам-членам и отрасли	Высокий	2021 г.
ПДоК 0.2	ИКАО и государства-члены	Начать работу по реализации стратегии авиационной кибербезопасности ИКАО на национальном уровне (в соответствии с поручением в резолюции A40-10) (для проверки уровня реализации стратегии государствами необходимо разработать набор параметров для оценки степени реализации определенных действий).	Подтверждение начала работы по реализации на национальном уровне	Высокий	2023 г.
ПДоК 0.3	ИКАО	Провести исследование для составления перечня инициатив/ методик в области кибербезопасности, чтобы установить, как государства и отрасль управляют кибербезопасностью гражданской авиации (вопросник относительно того, разработали ли государства план действий по реализации стратегии).	Исследование/вопросник ИКАО, направленный государствам-членам	Высокий	2021-2022 гг.

ОСНОВОПОЛАГАЮЩИЕ ЭЛЕМЕНТЫ СТРАТЕГИИ КИБЕРБЕЗОПАСНОСТИ

Приоритетный результат	**1. ОБЕСПЕЧЕНИЕ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА**
Приоритетные действия	• Развивать сотрудничество между всеми заинтересованными сторонами на национальном, региональном и международном уровнях. • Признать на взаимной основе необходимость мер (обеспечение, поддержание и повышение кибербезопасности) по защите гражданской авиации. • Добиться регуляторной гармонизации на международном, региональном и национальном уровнях, с тем чтобы содействовать глобальной согласованности и интероперабельности мер защиты. • Привлекать государства к решению проблем кибербезопасности в международной гражданской авиации. • Способствовать проведению международных мероприятий в области кибербезопасности. • Признать, что кибербезопасность является общей ответственностью во всех сегментах глобальной системы гражданской авиации.

Действия

Действие #	**Исполнитель**	**Прослежи-ваемость связи со стратегией авиацион-ной кибер-безопасности**	**Прослежи-ваемость связи с главой 5**	**Конкретные меры/задачи**	**Показатели**	**Приоритет**	**Дата начала реализации**
ПДоК 1.1	ИКАО и государства-члены	1.1	5.2	Включить аспекты кибербезопасности в программы контроля за обеспечением безопасности полетов и авиационной безопасности ИКАО; включить соответствующие Стандарты в программы проверки ИКАО (такие как УППКБП и УППАБ).	Включение имеющих отношение к кибербезопасности Стандартов в программы проверки ИКАО, связанные как с безопасностью полетов, так и с авиационной безопасностью	Высокий	На постоянной основе
ПДоК 1.2	ИКАО	1.1	5.1 См. также ПДоК 4.6 (п.8.2 плана действий)	Провести исследование для составления перечня инициатив/методик в области кибербезопасности, чтобы установить, как государства и отрасль управляют кибербезопасностью гражданской авиации.	Результаты вопросников, число инициатив и регионов	Высокий	На постоянной основе

ПДоК 1.3	ИКАО	1.1	5.1	Составить перечень всех инициатив в области кибербезопасности, связанных с различными группами экспертов ИКАО.	Разработка и обновление программы работы ИКАО в области авиационной кибербезопасности Специальным координационным комитетом по кибербезопасности	Высокий	2024 г.
ПДоК 1.4	ИКАО и государства-члены	1.2	5.2.3 и 5.5 См. также ПДоК 5.1 (п. 9.2 плана действий)	A) Разработать образцы типовых меморандумов о взаимопонимании/сотрудничестве и внешних соглашений; B) дать рекомендации относительно методики разработки этих соглашений.	Наличие шаблона и рекомендаций	Низкий	2023-2024 гг.
ПДоК 1.5	ИКАО, государства-члены и отрасль	1.2	5.3	Разработать последовательную и согласованную терминологию в области кибербезопасности гражданской авиации, с тем чтобы все авиационные заинтересованные стороны, независимо от характера и уровня их деятельности, могли понимать друг друга в части кибербезопасности.	Публикация всеобъемлющего глоссария по кибербезопасности	Средний	2023 г.
ПДоК 1.6	ИКАО, государства-члены и отрасль	1.2	5.4	ИКАО должна разработать общие рамки определения высокоуровневой функциональной схемы обмена информацией между авиационными партнерами (например, ПАНО, АОС, В/С, аэропорты, МЕТ, MRO, CNS) в качестве необходимого условия понимания ландшафта киберрисков. Государствам-членам и отрасли следует разработать такие рамки на национальном и организационном уровнях.	Наличие общих рамок и определенной типовой схемы обмена информацией/ взаимодействия в авиации Осведомленность и понимание функциональной схемы	Высокий	2024 г.

ПДоК 1.7	ИКАО и государства-члены	1.2	5.7 См. также ПДоК 6.2 (п. 10.2 плана действий)	ИКАО должна определить модели сотрудничества между гражданской и военной авиацией в целях разработки, в соответствующих случаях, моделей/руководящих указаний для интероперабельных гражданских и военных авиационных интерфейсов. Определить критерии и уровень соответствующего взаимодействия.	Наличие таких моделей/руководящих указаний для сотрудничества и интероперабельности гражданских и военных органов в сфере кибербезопасности Опубликованный перечень критериев и минимального количества требуемых мер взаимодействия	Высокий	2023 г.
ПДоК 1.8	ИКАО, государства-члены и отрасль	1.3	5.8	Планировать, организовывать и поддерживать международные и региональные мероприятия по содействию повышению кибербезопасности в гражданской авиации.	Международное сотрудничество в проведении мероприятий, повышении осведомленности	н. д.	На постоянной основе
ПДоК 1.9	ИКАО, государства-члены и отрасль	1.3	5.4	Обеспечить участие всех соответствующих заинтересованных сторон в дискуссиях и мероприятиях, касающихся кибербезопасности гражданской авиации. Постоянное участие соответствующих заинтересованных сторон и проведение с ними информационно-разъяснительной работы	Публикация результатов совместной работы Публикация доказательства участия, например подтверждения партнерских отношений, группового членства и т.д.	Высокий	На постоянной основе
ПДоК 1.10	ИКАО, государства-члены и отрасль	1.2	5.2.2	Разработать механизм доверия в рамках международной авиации, позволяющий организациям взаимодействовать исходя из их доверия к другим заинтересованным сторонам.	Разработка механизма доверия, используемого многими организациями	Высокий	2024-2025 гг.

Приоритетный результат	**2. РАЗРАБОТКА ПРИНЦИПОВ УПРАВЛЕНИЯ И ПОДОТЧЕТНОСТИ**
Приоритетные действия	• Рекомендовать к реализации, поддерживать и развивать стратегию кибербезопасности ИКАО. • Разработать четкие национальные принципы управления и подотчетности в отношении кибербезопасности гражданской авиации. • Обеспечить координацию на уровне государств между ведомствами гражданской авиации и компетентными национальными органами по кибербезопасности. • Установить надлежащие каналы координации между различными государственными органами и отраслью. • Включить вопросы кибербезопасности в национальные программы обеспечения безопасности полетов и авиационной безопасности в гражданской авиации. • Включить вопросы кибербезопасности в глобальные региональные планы. • Разработать общий базовый уровень для Стандартов и Рекомендуемой практики в области кибербезопасности.

Действия

Действие #	**Исполнитель**	**Прослежи-ваемость связи со стратегией кибербезо-пасности**	**Прослежи-ваемость связи с главой 6**	**Конкретные меры/задачи**	**Показатели**	**Приоритет**	**Дата начала реализации**
ПДоК 2.1	ИКАО и государства-члены		6.1	Создать структуру управления в области кибербезопасности гражданской авиации.	Определение адекватной структуры (структур) управления кибербезопасностью гражданской авиации	н. д.	2021-2023 гг.
ПДоК 2.2	ИКАО и государства-члены	2.2	6.3	ИКАО должна разработать общий набор принципов адекватной системы (систем) управления кибербезопас-ностью гражданской авиации. Государствам-членам следует разработать такие принципы на национальном уровне в соответствии с моделью ИКАО.	Публикация общих принципов	Высокий	2023-2024 гг.
ПДоК 2.3	ИКАО, государства-члены и отрасль	2.2	6.3.2 См. также п. 8.1.	Разработать инструктивный материал для оказания помощи организациям в реализации скоординированных механизмов управления кибербезо-пасностью в целях поддержки создания системного подхода к	Публикация инструктивных указаний	Высокий	2023 г.

			плана действий	управлению рисками для авиационной кибербезопасности и оценки зрелости и эффективности этих механизмов.			
ПДоК 2.4	ИКАО и государства-члены	2.2	6.3	Содействовать созданию механизмов координации между ведомствами гражданской авиации и органами по кибербезопасности.	Обзор ИКАО: число выявленных существующих действующих координационных механизмов	Средний	2022 г.
ПДоК 2.5	ИКАО	2.3	6.2.1 См. также ПДоК 1.9 (п. 5.2 плана действий)	ИКАО должна включить вопросы кибербезопасности в региональные и глобальные планы в целях обеспечения безопасности полетов, авиационной безопасности и устойчивости авиации.	Публикация обновленных планов	н. д.	2022-2023 гг.
ПДоК 2.6	ИКАО		6.2	ИКАО должна создать в хранилище данных раздел, содержащий реестр передовых методов/инструктивных указаний.	Хранилище данных ИКАО о передовых методах	н. д.	2020-2021 гг.
ПДоК 2.7	ИКАО, государства-члены и отрасль	3.2	6.3	ИКАО должна разработать типовые процедуры представления данных о киберинцидентах, включая инструктивный материал по классификации инцидентов. Государства-члены и отрасль должны разработать национальные и организационные процедуры своевременного и эффективного представления данных о киберинцидентах.	Процедуры представления данных о киберинцидентах/число инцидентов, о которых представлены дынные в соответствии с процедурами	Высокий	2022-2023 гг.
ПДоК 2.8	ИКАО и государства-члены	2.2	6.2	ИКАО должна определить, в какой степени государства-члены включают вопросы кибербезопасности в свои национальные программы по безопасности полетов и авиационной безопасности гражданской авиации и аэронавигационные планы.	Обзор ИКАО: число государств, включающих вопросы кибербезопасности в свои национальные программы по безопасности полетов и авиационной безопасности	Высокий	Обзор 2022 г. Ведется дальнейшая работа

Приоритетный результат	**3. РАЗРАБОТКА ДЕЙСТВЕННОГО ЗАКОНОДАТЕЛЬСТВА И НОРМАТИВНЫХ ПОЛОЖЕНИЙ**
Приоритетные действия	• Обеспечить наличие в международных правовых документах надлежащего механизма предотвращения киберинцидентов, а также судебного преследования их виновников. • Проанализировать существующее национальное законодательство и, при необходимости, обновить или принять национальное законодательство, обеспечивающее предотвращение и расследование кибератак и судебное преследование за совершение кибератак, которые влияют на безопасность полетов, авиационную безопасность, эффективность или непрерывность деятельности гражданской авиации. • Обеспечить наличие надлежащих национальных нормативных положений и законодательства в области кибербезопасности гражданской авиации. • Разработать для государств и отрасли надлежащие инструктивные указания относительно внедрения положений о кибербезопасности.

Действия

Действие #	**Исполнитель**	**Прослежи-ваемость связи со стратегией кибербезо-пасности**	**Прослежи-ваемость связи с главой 7**	**Конкретные меры/задачи**	**Показатели**	**Приоритет**	**Дата начала реализации**
ПДоК 3.1	Государства-члены	3.3	7.4	Государства-члены должны ратифицировать пекинские документы.	Число государств, ратифицировавших пекинские документы	Высокий	На постоянной основе
ПДоК 3.2	ИКАО	3.3	7.3	Анализ документов по международному воздушному праву	Обзор и анализ пробелов в соответствующих документах по международному воздушному праву	Высокий	2022 г.
ПДоК 3.3	ИКАО и государства-члены	3.3 и 3.4	7.2	Анализ существующего национального законодательства в области кибербезопасности гражданской авиации и выявление пробелов, в том числе в уголовном праве	Обзор состояния национального законодательства в отношении незаконных актов против гражданской авиации, совершаемых с помощью киберсредств	Средний	2023-2024 гг.
ПДоК 3.4	ИКАО	3.3	7.1	Рассмотреть существующие Стандарты и Рекомендуемую практику ИКАО по авиационной безопасности для определения необходимости их обновления на предмет кибербезопасности.	Рассмотрение и анализ пробелов в SARPS ИКАО	Высокий	2022 г.

ПДоК 3.5	ИКАО	3.2		Создать, пересматривать и изменять инструктивный материал, касающийся внедрения требований по обеспечению кибербезопасности гражданской авиации.	Публикация инструктивного материала по кибербезопасности гражданской авиации	Высокий	2021 г. и на постоянной основе

Приоритетный результат	**4. РАЗРАБОТКА ПОЛИТИКИ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ**
Приоритетные действия	• Обеспечить включение кибербезопасности в качестве компонента систем безопасности полетов и авиационной безопасности и комплексного механизма управления риском. • Обеспечить сопоставимость различных методик оценки риска для кибербезопасности гражданской авиации. • Разработать политику в области кибербезопасности с учетом полного жизненного цикла авиационных систем.

Действия

Действие #	**Исполнитель**	**Прослежи-ваемость связи со стратегией кибербезо-пасности**	**Прослежи-ваемость связи с главой 8**	**Конкретные меры/задачи**	**Показатели**	**Приоритет**	**Дата начала реализации**
ПДоК 4.1	Государства-члены и отрасль	4.1	8.1	Государства-члены и отрасль должны обеспечить взятие их руководством обязательств по решению вопросов кибербезопасности и киберустойчивости гражданской авиации.	Кампания по повышению осведомленности/доказательства взятия обязательств, такие как декларации об обязательствах, обязанности в области кибербезопасности, определенные в руководствах по управлению органов власти и организаций	Средний	2022-2023 гг.
ПДоК 4.2	ИКАО, государства-члены и отрасль	4.3	8.2 См. также п. 5.11 плана действий	Поощрять проведение научно-исследовательской работы в гражданской авиации в области кибербезопасности путем установления контактов с университетами, институтами, исследовательскими сообществами и т. д.	Число контактов и проектов	Высокий	2022-2023 гг.

ПДоК 4.3	Государства-члены и отрасль	4.2	5.6 и 8.2	Установить критерии проведения совместной трансорганизационной оценки риска наряду с определением подлежащей обмену информации, а также необходимые критерии сопоставимости рисков. Государствам-членам следует установить такие критерии на национальном уровне, а отрасли – на организационном уровне.	Публикация целей и критериев совместной трансорганизационной оценки риска.	Высокий	2023 г.
ПДоК 4.4	ИКАО, государства-члены и отрасль	4.3	8.1	Разработать политику обеспечения безопасности на этапе разработки в качестве основы для безопасного жизненного цикла систем гражданской авиации.	Разработанная политика безопасного жизненного цикла систем гражданской авиации	Средний	2022-2023 гг.
ПДоК 4.5	ИКАО, государства-члены и отрасль	4.2	8.2	ИКАО должна организовать международные форумы для обсуждения задач трансорганизационной/трансфункциональной кибербезопасности и киберустойчивости, а также минимального уровня функциональных возможностей, критически необходимых для сектора гражданской авиации. Государствам-членам следует организовывать такие форумы на национальном и региональном уровнях, а отрасли следует организовывать специальные форумы и активно участвовать в форумах, организуемых ИКАО и государствами-членами.	Количество форумов для обсуждения задач	Высокий	2022-2023 гг.
ПДоК 4.6	ИКАО, государства-члены и отрасль	4.3	8.2	Составить перечень существующих инициатив по управлению риском для кибербезопасности гражданской авиации (профили риска, сценарии, управление уязвимостью, оценки риска).	Наличие хранилища данных об инициативах по управлению рисками в области кибербезопасности	Средний	2023-2024 гг.

ПДоК 4.7	ИКАО, государства-члены и отрасль	4.3	8.3	ИКАО должна составить перечень стратегических сценариев киберриска на международном уровне. Государствам-членам и отрасли следует вносить вклад и разработать подобные перечни на национальном и организационном уровнях.	Наличие 10 сценариев киберриска	Высокий	2023-2024 гг.
ПДоК 4.8	ИКАО, государства-члены и отрасль		8.2	ИКАО должна определить профили риска для каждой эксплуатационной сферы. Государствам-членам и отрасли следует вносить вклад путем определения подобных профилей риска на национальном и организационном уровнях.	Наличие профилей риска	Высокий	2023 г.
ПДоК 4.9	ИКАО		8.2	Разработать заявление о глобальном контексте риска в области кибербезопасности.	Публикация заявления о глобальном контексте риска в области кибербезопасности	Высокий	2023 г.

Приоритетный результат	**5. РАЗВИТИЕ ПОТЕНЦИАЛА ДЛЯ ОБМЕНА ИНФОРМАЦИЕЙ**
Приоритетные действия	• Разработать или использовать существующие платформы и механизмы обмена информацией, которые признаны и соответствуют действующим положениям ИКАО, в целях повышения осведомленности о киберситуации и обеспечения таким образом предотвращения, раннего обнаружения и смягчения последствий соответствующих киберсобытий. • Обеспечить информирование компетентных органов о любых киберинцидентах или уязвимостях, которые могут представлять значительный риск для безопасности полетов и/или авиационной безопасности.

Действия

Действие #	**Исполнитель**	**Прослежи-ваемость связи со стратегией кибербезо-пасности**	**Прослежи-ваемость связи с главой 9**	**Конкретные меры/задачи**	**Показатели**	**Приоритет**	**Дата начала реализации**
ПДоК 5.1	ИКАО	5.1	9.1 и 9.2	ИКАО должна разработать инструктивный материал по обмену информацией.	Инструктивный материал по обмену информацией, доступный сообществу	Высокий	2022-2023 гг.

ПДоК 5.2	ИКАО	5.1	9.1	ИКАО при поддержке государств-членов и отрасли должна определить потребности в обмене информацией о кибербезопасности и сотрудничестве (включая, в частности, во время кризисных ситуаций), а также политику.	Разработать перечень потенциальной подлежащей обмену информации	Средний	2022-2024 гг.
ПДоК 5.3	ИКАО	5.1	9.1	Разработать инструктивный материал по использованию TLP (протокол "Светофор") для определения уровня распространения/ограничений при распространении киберинформации и дальнейшем обмене такой информацией.	Публикация инструктивного материала по использованию TLP при распространении киберинформации и обмене ею	Высокий	2021 г.
ПДоК 5.4	ИКАО, государства-члены и отрасль	5.2	9.2	Рассмотреть возможность определения принципов ответственного раскрытия уязвимостей в области кибербезопасности.	Наличие и публикация принципов ответственного раскрытия уязвимостей, если это будет сочтено возможным	Высокий	2023 г.
ПДоК 5.5	ИКАО и государства-члены	5.2	9.4	ИКАО должна разработать и поддерживать сеть координаторов по вопросам кибербезопасности гражданской авиации на международном уровне для государств-членов и отрасли. Государствам-членам следует в сотрудничестве с ИКАО разработать сеть координаторов на национальном уровне.	Создание сети координаторов по вопросам кибербезопасности гражданской авиации Публикация сети координаторов каждого государства-члена	Средний	2024-2025 гг.

Приоритетный результат	**6. РАЗРАБОТКА МЕХАНИЗМА УПРАВЛЕНИЯ ИНЦИДЕНТАМИ И ПЛАНИРОВАНИЕ МЕРОПРИЯТИЙ НА СЛУЧАЙ АВАРИЙНОЙ ОБСТАНОВКИ**
Приоритетные действия	• Обеспечить составление надлежащих и масштабируемых планов, предусматривающих непрерывность безопасного и надежного производства полетов гражданской авиации в случае возникновения киберинцидентов. • Обеспечить использование существующих планов на случай непредвиденных обстоятельств, включать в них положения о реагировании на инциденты в области кибербезопасности и восстановлении после них и регулярно/периодически проводить учения для проверки возможностей по обнаружению киберинцидентов, реагированию на киберинциденты и восстановлению после них.

Действия

Действие #	**Исполнитель**	**Прослежи-ваемость связи со стратегией кибербезо-пасности**	**Прослежи-ваемость связи с главой 10**	**Конкретные меры/задачи**	**Показатели**	**Приоритет**	**Дата начала реализации**
ПДоК 6.1	Государства-члены и отрасль	6.1	10.1	Государства-члены должны установить задачи и минимальные уровни функциональных возможностей, имеющих важное значение для сектора гражданской авиации. Отрасль должна выполнить установленные задачи.	Публикация перечня задач и минимальных приемлемых уровней функциональных возможностей для непрерывной деятельности авиации	Высокий	2022-2023 гг.
ПДоК 6.2	ИКАО и государства-члены	6.1	10.2	ИКАО должна разработать инструктивный материал и порядок участия военных органов в процессах планирования мероприятий на случай киберинцидентов в гражданской авиации. Государствам-членам следует разработать процедуры и соглашения о сотрудничестве между гражданскими и военными авиационными органами.	Разработка и публикация инструктивного материала, касающегося процессов и процедур сотрудничества гражданских/ военных органов в сфере реагирования на киберинциденты в гражданской авиации	Высокий	2022-2023 гг
ПДоК 6.3	ИКАО, государства-члены и отрасль	6.1.	10.1	ИКАО должна разработать инструктивный материал по реагированию на киберинциденты в гражданской авиации и восстановлению после них, включая планы мероприятий на случай	Публикация инструктивного материала по реагированию на киберинциденты в гражданской авиации и восстановлению после них, включая планы мероприятий	Высокий	2022-2023 гг

				непредвиденной и аварийной обстановки. Государствам-членам и отрасли в соответствии с рекомендациями ИКАО следует разработать такие инструктивные указания на национальном и организационном уровнях.	на случай непредвиденной и аварийной обстановки		
ПДоК 6.4	Государства-члены	6.1.	10.2 и 10.3	Государства-члены должны разработать и внедрить механизмы и планы для обнаружения и анализа киберинцидентов в гражданской авиации и реагирования на них на оперативном уровне.	Обзор с целью отслеживания уровня внедрения	Высокий	2023-2024 гг
ПДоК 6.5	ИКАО и государства-члены	6.1.	10.1	Разработать порядок координации действий в кризисных ситуациях, связанных с кибербезопасностью гражданской авиации, в том числе на национальном и международном уровнях.	Определение установленного порядка координации действий в кризисных ситуациях, связанных с кибербезопасностью Публикация инструктивного материала	Средний	2024-2025 гг
ПДоК 6.6	Государства-члены и отрасль	6.1	10.3	Периодически проводить теоретические и практические учения.	Обмен накопленным опытом, по мере необходимости	Высокий	2022-2023 гг

Приоритетный результат	**7. НАРАЩИВАНИЕ ПОТЕНЦИАЛА, ПОДГОТОВКА ПЕРСОНАЛА И ФОРМИРОВАНИЕ КУЛЬТУРЫ КИБЕРБЕЗОПАСНОСТИ**
Приоритетные действия	• Обеспечить надлежащую квалификацию персонала на основе ролевых моделей как в области авиационной безопасности, так и в области кибербезопасности. • Повысить осведомленность о кибербезопасности, включая деятельность по надлежащей киберпрофилактике. • Обеспечить включение в национальную образовательную структуру надлежащей учебной программы по авиационной кибербезопасности с целью обеспечения наличия багажа знаний по всем аспектам безопасности полетов и авиационной безопасности на всех уровнях организации, включая руководство высшего звена. • Способствовать инновациям и надлежащим научным исследованиям и разработкам в области кибербезопасности. • Включить кибербезопасность в стратегию ИКАО по следующему поколению авиационных специалистов.

Действия

Действие #	**Исполнитель**	**Прослежи-ваемость связи со стратегией кибербезо-пасности**	**Прослежи-ваемость связи с главой 11**	**Конкретные меры/задачи**	**Показатели**	**Приоритет**	**Дата начала реализации**
ПДоК 7.1	ИКАО, государства-члены и отрасль	7.1.	11.1	Определить и популяризировать культуру и образование в области кибербезопасности гражданской авиации.	Наличие курсов и инструктивного материала, касающихся культуры кибербезопасности гражданской авиации	Средний	2022-2023 гг.
ПДоК 7.2	Государства-члены и отрасль	7.2.	11.1	Государствам-членам и отрасли следует разработать соответствующие требования к ролевой подготовке персонала в области авиационной кибербезопасности на всех уровнях в рамках своих организаций	Разработка соответствующей методики ролевой подготовки персонала в области авиационной безопасности и кибербезопасности	Высокий	2022-2023 гг.
ПДоК 7.3	ИКАО и государства-члены	7.3.	11.1	ИКАО должна включить кибербезопасность в стратегию по следующему поколению авиационных специалистов. Государствам-членам следует включить кибербезопасность в свои национальные стратегии, связанные со стратегий NGAP.	Включение кибербезопасности в стратегию NGAP	Средний	2022-2023 гг.

ПДоК 7.4	ИКАО	7.3.	11.1	ИКАО должна проанализировать способы и средства разработки квалификационных требований на основе ролевых моделей в области кибербезопасности.	Включение вопросов ролевой подготовки персонала в области кибербезопасности в документы Doc 7192 и 9868 ИКАО, если это будет сочтено целесообразным	Высокий	2023-2025 гг
ПДоК 7.5	ИКАО, государства-члены и отрасль	7.3.	11.1	Развитие деятельности по наращиванию потенциала	Организация учебных курсов по авиационной кибербезопасности	Высокий	На постоянной основе

— КОНЕЦ —