International Civil Aviation Organization
Organisation de l'aviation civile internationale
Organización de Aviación Civil Internacional
Международная организация гражданской авиации
منظمة الطيران المدني الدولي
国际民用航空组织

Тел.: +1 514-954-8219, доб. 6760

Ref.: AS8/1.9.1-20/114

5 ноября 2020 года

Содержание: План действий по обеспечению кибербезопасности

Требуемые действия: a) распространить План действий по обеспечению кибербезопасности и координировать его осуществление со всеми соответствующими национальными учреждениями, отраслью и заинтересованными сторонами; и b) разработать и внедрить национальные планы и приоритеты, обеспечивающие основу для действий

ИСПРАВЛЕНИЕ от 10 ноября 2020 года

(только на русском языке)

Просьба заменить План действий по обеспечению кибербезопасности прилагаемыми новыми страницами.

999 Robert-Bourassa Boulevard
Montréal, Quebec
Canada H3C 5H7
Tel.: +1 514-954-8219
Fax: +1 514-954-6077
Email: icaohq@icao.int
www.icao.int

План действий по обеспечению кибербезопасности

Опубликовано с санкции Генерального секретаря

Ноябрь 2020 г.

Международная организация гражданской авиации

Термины и определения[1]

ЗКР: заявление о контексте риска

Годовой доклад о глобальных рисках, подготовленный Рабочей группой ИКАО по угрозам и рискам на основе ее анализа.

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 (информационная безопасность)

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].

Источник угрозы (или исполнитель)

Субъект, который частично или полностью несет ответственность за инцидент, который воздействует (или может воздействовать) на безопасность организации, например террорист, преступник, хакер, хактивист и т. д.

Кибербезопасность

Термин "кибербезопасность" используется в настоящем документе взаимозаменяемо с термином "информационная безопасность".

Матрица риска

Инструмент для ранжирования и отображения компонентов рисков (угроза, последствия и уязвимость) и в конечном счете остаточных рисков.

Обмен информацией

Обмен различной информацией о сетевой и информационной безопасности, например о рисках, уязвимостях, угрозах и проблемах внутренней безопасности, а также о передовой практике.

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 в ситуациях, когда они действительно имеют место. Политика в области кибербезопасности должна определять все активы организации, а также потенциальные угрозы этим активам. Сотрудники должны получать обновленную информацию о политике организации в области обеспечения безопасности. Сама политика также должна обновляться на регулярной основе.

[1] Находятся на стадии рассмотрения SSGC/RSGLEG.

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 (информационная безопасность)

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

Свойство чего-то, что потенциально может подвергаться угрозе, которое может быть использовано нарушителем, например в аэропорту или на борту воздушного судна, или которое означает, что актив может быть непреднамеренно затронут умышленным актом вмешательства против неавиационной цели, что усугубляется любым слабым звеном в существующих мерах по обеспечению безопасности.

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.

Приоритетный результат	**1. РАЗРАБОТКА ГЛОБАЛЬНОГО И СОГЛАСОВАННОГО КОНЦЕПТУАЛЬНОГО ВИДЕНИЯ**	**КТО**	**КОГДА**
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 рисками для кибербезопасности авиации. • Признать, что сектор гражданской авиации должен быть устойчив к кибератакам и должен обеспечивать безопасность своих операций и пользоваться доверием в глобальном масштабе, в то же время продолжая использовать инновации и развиваться. • Признать, что риски для кибербезопасности подпадают под действие Конвенции о международной гражданской авиации.	ИКАО, государства-члены и отрасль	2020 г.

Приоритетный результат	**2. ОБЕСПЕЧЕНИЕ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА**	**КТО**	**КОГДА**
Приоритетные действия	• Развивать сотрудничество на национальном и международном уровнях. • Признать на взаимной основе необходимость мер (обеспечение, поддержание и повышение кибербезопасности) по защите гражданской авиации.	ИКАО, государства-члены и отрасль	На постоянной основе

	• Добиваться гармонизации на глобальном, 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.		

Приоритетный результат	**3. РАЗРАБОТКА ПРИНЦИПОВ УПРАВЛЕНИЯ И ПОДОТЧЕТНОСТИ**	**КТО**	**КОГДА**
Приоритетные действия	• Поощрять реализацию, 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 и региональные планы. • Вести работу по разработке общего базового подхода для Стандартов и Рекомендуемой практики в области кибербезопасности.	ИКАО, государства-члены и отрасль	2020 г.

Приоритетный результат	**4. РАЗРАБОТКА ДЕЙСТВЕННОГО ЗАКОНОДАТЕЛЬСТВА И НОРМАТИВНЫХ ПОЛОЖЕНИЙ**	**КТО**	**КОГДА**
Приоритетные действия	• Обеспечить наличие в международно-правовых документах надлежащих мер по предотвращению киберинцидентов, судебному преследованию в отношении киберинцидентов и своевременному реагированию на них. • Обеспечить введение в действие надлежащих нормативных положений и законодательства в области кибербезопасности. • Разработать надлежащие рекомендации для государств и отрасли по вопросу внедрения положений о кибербезопасности.	ИКАО, государства-члены и отрасль	2022–2023 гг.

Приоритетный результат	**5. РАЗРАБОТКА ПОЛИТИКИ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ**	**КТО**	**КОГДА**
Приоритетные действия	• Обеспечить включение кибербезопасности в качестве компонента систем авиационной безопасности и безопасности полетов и комплексного механизма управления риском. • Обеспечить сопоставимость различных методик оценки риска. • Разработать политику в области кибербезопасности с учетом полного жизненного цикла авиационных систем.	ИКАО, государства-члены и отрасль	2022–2023 гг.

Приоритетный результат	**6. РАЗВИТИЕ ПОТЕНЦИАЛА ДЛЯ ОБМЕНА ИНФОРМАЦИЕЙ**	**КТО**	**КОГДА**
Приоритетные действия	• Разработать платформы и механизмы обмена информацией, которые соответствуют существующим положениям ИКАО, для предотвращения, раннего обнаружения и смягчения последствий соответствующих киберсобытий.	ИКАО, государства-члены и отрасль	2022–2023 гг.

Приоритетный результат	**7. РАЗРАБОТКА МЕХАНИЗМА УПРАВЛЕНИЯ ИНЦИДЕНТАМИ И ПЛАНИРОВАНИЕ МЕРОПРИЯТИЙ НА СЛУЧАЙ АВАРИЙНОЙ ОБСТАНОВКИ**	**КТО**	**КОГДА**
Приоритетные действия	• Обеспечить составление надлежащих и масштабируемых планов, предусматривающих непрерывность деятельности воздушного транспорта во время киберинцидентов. • Поощрять использование существующих планов на случай непредвиденных обстоятельств, включать в них положения о кибербезопасности и проводить учения для тестирования киберустойчивости.	ИКАО, государства-члены и отрасль	2022–2023 гг.

Приоритетный результат	**8. НАРАЩИВАНИЕ ПОТЕНЦИАЛА, ПОДГОТОВКА ПЕРСОНАЛА И ФОРМИРОВАНИЕ КУЛЬТУРЫ КИБЕРБЕЗОПАСНОСТИ**	**КТО**	**КОГДА**
Приоритетные действия	• Обеспечить наличие квалифицированного персонала как в авиационных областях, так и в области кибербезопасности. • Повысить осведомленность о кибербезопасности. • Обеспечить включение в национальную образовательную структуру на уровне профессиональной подготовки 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.	ИКАО, государства-члены и отрасль	2022–2023 гг.

Глава 1

ВВЕДЕНИЕ

1.1. ИСХОДНАЯ ИНФОРМАЦИЯ

1.1.1. В нынешнем контексте гражданской авиации неизменно прогнозируется долгосрочный рост объема воздушных перевозок, стремительно развивается техника, деятельность пользователей воздушного пространства и 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 событий. 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 угрожать устойчивости систем, способных 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 для 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 в документе ИКАО *"Заявление о глобальном контексте риска в области авиационной безопасности"* (Doc 10108) уровень риска, связанного с кибератаками в террористических целях, был оценен как низкий. 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, таким образом, ответственных лиц невозможно преследовать в судебном порядке, так как установление источника кибератак и судебное преследование за их совершение зачастую является сложным и трудным в осуществлении процессом, а жертве атаки приходится нести расходы, связанные с возмещением ущерба. В силу этих причин чрезвычайно важно, чтобы ИКАО, государства и отрасль объединили свои усилия 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 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 государственными органами, с целью обеспечить эффективное и действенное глобальное управление кибербезопасностью;

c) обязательства всех заинтересованных сторон системы гражданской авиации продолжать развивать киберустойчивость в целях защиты авиации от кибератак, связанных с любыми источниками 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 управления 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

ОСНОВНЫЕ ПОЛОЖЕНИЯ ПЛАНА ДЕЙСТВИЙ ПО ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ

3.1 КЛЮЧЕВЫЕ ПРИОРИТЕТЫ

3.1.1 Концептуальное видение ИКАО в отношении глобальной кибербезопасности гражданской авиации заключается в том, что авиационный сектор должен обладать сопротивляемостью и устойчивостью к кибератакам и в глобальном масштабе оставаться безопасным, надежным и внушающим доверие и в то же время постоянно адаптироваться, использовать инновации и расширяться. Программа работы в области кибербезопасности направлена на поддержку этой цели, заключающейся в обеспечении того, чтобы нынешняя и будущая авиационная система являлась заслуживающей доверие и надежной средой, а авиационные заинтересованные стороны могли полагаться на продукты, услуги и информацию, предоставляемые другими партнерами, для выполнения своих производственных задач.

3.1.2 Этот план действий призван сконцентрировать ресурсы и действия на выработке системного подхода к управлению кибербезопасностью в гражданской авиации, включая нынешние и традиционные системы, с конечной целью создать подход по принципу "системы систем", который позволяет гражданской авиации своевременно адаптироваться и таким образом противостоять новым угрозам без значительных сбоев. Учитывая острую необходимость в защите гражданской авиации от кибератак, ИКАО должна провести инвентаризацию текущих предпринимаемых инициатив по обеспечению кибербезопасности гражданской авиации и, опираясь на них, заявить о необходимости принятия в качестве базовой меры основных исходных мер безопасности, которые, как правило, вводятся в любой системе информационных/эксплуатационных технологий (ИТ/ЭТ) (например, надлежащая киберпрофилактика), включая внедрение существующих Стандартов и Рекомендуемой практики в области кибербезопасности, содержащихся в Приложении 17. Таким образом, руководящий принцип для такого курса действий должен заключаться в том, чтобы направлять действия ИКАО. Эти цели могут быть достигнуты путем сосредоточения внимания на четырех главных направлениях:

a) **Создание культуры кибербезопасности.** За последние десятилетия авиационная отрасль достигла значительного прогресса за счет использования инновационных технологий и обработки всевозрастающего объема данных. Однако за это время появились новые угрозы. Желательной целью является формирование в авиации культуры кибербезопасности, которая соответствует существующим понятиям культуры безопасности полетов и культуры авиационной безопасности и закрепляет кибербезопасность в жизненном цикле системы[2].

b) **Обеспечение киберустойчивости системы гражданской авиации.** Киберустойчивая система гражданской авиации – это система, которая, подвергшись атаке, может сохранить свои критические функциональные

[2] Руководство ИКАО по управлению безопасностью полетов (Doc 9859) определяет систему как организованную структуру с заданной целью, состоящую из взаимосвязанных и взаимозависимых элементов и компонентов, а также связанной с ними политики, процедур и практики, созданную в целях осуществления конкретной деятельности или решения проблемы.

возможности, т. е. обеспечить безопасное и надежное производство полетов с минимальными перебоями, если таковые имеют место. Она смягчает негативные последствия кибератак в возможно короткие сроки и в максимально возможной степени с помощью целостного, многоуровневого защитного механизма. Такой механизм должен гарантировать, что успешная атака на один уровень (например, нарушение аутентификации, которое позволяет вторжение) не ставит под угрозу другие уровни системы и/или не приводит к потере функций, критически важных для обеспечения безопасности полетов или непрерывности деятельности. Система должна также основываться на принципе непрерывного совершенствования для обеспечения необходимого приспособления к плановым техническим или процедурным нововведениям, а также внесения изменений и постоянного совершенствования системы с учетом приобретенного опыта. Наконец, система должна включать надлежащие механизмы сотрудничества и обмена информацией между авиационными заинтересованными сторонами, такими как государственные и отраслевые организации, а также, в соответствующих случаях, между гражданскими и военными органами власти.

c) **Обеспечить самоукрепление гражданской авиации за счет принятия подхода "встроенной безопасности".** Принятие подхода встроенной безопасности для гражданской авиации требует, чтобы с самого начала разработки концепции системы учитывались цели обеспечения безопасности, которые должны быть достигнуты в процессе проектирования системы наряду с традиционными эксплуатационными целями и целями обеспечения безопасности полетов. Обеспечение безопасности критических элементов и процессов на этапе разработки меняет парадигму безопасности с реагирующей (привязанной к событию) на проактивную и способствует формированию самоукрепляющейся системы гражданской авиации, тем самым создавая условия для ее развития и обеспечивая повышенную устойчивость в более автоматизированном режиме при доказанной эффективности.

d) **Приведение в соответствие с другими инициативами ИКАО в области кибербезопасности, координация с положениями об управлении безопасностью полетов и авиационной безопасностью и использование существующих инициатив.** Существующие группы экспертов ИКАО в настоящее время занимаются различными аспектами кибербезопасности. Потенциальное отсутствие координации проводимой работы может привести к непоследовательности, пробелам и дублированию. Поэтому крайне важно обеспечить между ними надлежащую координацию. Надлежащая координация между группами экспертов, занимающимися вопросами кибербезопасности, имеет первостепенное значение для исключения возможного дублирования усилий, несоответствий или пропущенных требований. Особенно важно, чтобы эти группы экспертов достигли одинакового понимания задач и элементов работы друг друга для обеспечения общей эффективности и результативности деятельности ИКАО в этой области и оптимизации использования имеющихся ограниченных ресурсов. В этой связи всеми заинтересованными сторонами должны быть введены процедуры сотрудничества, а существующие процедуры должны быть усовершенствованы, с тем чтобы учесть следующие принципы:

- общее понимание целей и общее видение;
- совместная разработка;
- принцип взаимности;
- совместное использование ресурсов;
- регулярность.

3.1.3 Крайне важно обеспечить комплексное и согласованное управление рисками для гражданской авиации путем координации положений об управлении безопасностью полетов и авиационной безопасностью. Необходимо провести анализ положений Приложения 17 *"Безопасность"*, Приложения 19 *"Управление безопасностью полетов"* и других соответствующих положений об управлении риском в области кибербезопасности, с тем чтобы убедиться в отсутствии дублирования, пробелов или расхождений. Кибербезопасность должна быть связана с другими дисциплинами (безопасность полетов, эффективность) подобно тому, как связана в настоящее время "традиционная" авиационная безопасность, с тем чтобы гарантировать точную оценку подверженности угрозам в области кибербезопасности и обеспечить разработку эффективных и действенных, основанных на оценке риска стратегий киберзащиты. В деле обеспечения кибербезопасности необходимо "навести мосты" между авиационной безопасностью и безопасностью полетов, поскольку ввиду многодисциплинарного характера кибербезопасности необходимо использовать достигнутые результаты в следующих областях:

- авиационная безопасность: профилирование источников угрозы и определение защитных мер (уяснение источников угрозы и возможные меры по контролю риска);
- безопасность полетов: понимание принципов функционирования систем и операций сектора гражданской авиации (уяснение уязвимых областей и направлений атаки, а также последствий/воздействия атак, которые могут поставить под угрозу безопасность полетов и непрерывность деятельности).

3.1.4 Следует использовать существующие инициативы в области кибербезопасности для реализации основных требований в отношении кибербезопасности. Для управления угрозами и рисками для кибербезопасности инициировано множество мероприятий на местном, региональном и/или глобальном уровнях. Некоторые из них конкретно относятся к потребностям сектора гражданской авиации, а некоторые другие, не относящиеся к нему, тем не менее могут иметь значительную ценность при их приспособлении к нуждам гражданской авиации, учитывая тот факт, что кибербезопасность гражданской авиации имеет много общего с другими отраслевыми секторами. Поскольку требуется безотлагательно принимать меры для противодействия киберугрозам, необходимо составить полный перечень этих инициатив, прежде чем начинать работу по конкретным направлениям.

Глава 4

СТРАТЕГИЧЕСКИЙ ПЛАН ДЕЙСТВИЙ

4.1. СЕМЬ ОСНОВОПОЛАГАЮЩИХ ЭЛЕМЕНТОВ СТРАТЕГИИ КИБЕРБЕЗОПАСНОСТИ

4.1.1 Приведенные в настоящей главе компоненты разработаны с целью предложить серию принципов, мер и действий, направленных на достижение целей семи основополагающих элементов стратегии 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. • Признавать на взаимной основе усилия (разработка мер, поддержание и совершенствование кибербезопасности), направленные на защиту гражданской авиации. • Достичь 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.

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 надлежащих мер по предотвращению киберинцидентов, судебному преследованию в отношении киберинцидентов и своевременному на них реагированию.

- Обеспечить введение в действие надлежащих нормативных положений и законодательства в области кибербезопасности.

- 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 авиационной безопасности и безопасности полетов и комплексных механизмов управления риском.

- Обеспечить сопоставимость различных методик оценки риска.

- Разработать политику в области кибербезопасности с учетом полного жизненного цикла авиационных систем.

ОСНОВОПОЛАГАЮЩИЙ ЭЛЕМЕНТ 5. ОБМЕН ИНФОРМАЦИЕЙ

- Разработать платформы и механизмы обмена информацией, которые соответствуют существующим положениям ИКАО, для предотвращения, раннего обнаружения и смягчения последствий соответствующих киберсобытий.

ОСНОВОПОЛАГАЮЩИЙ ЭЛЕМЕНТ 6. УПРАВЛЕНИЕ ИНЦИДЕНТАМИ И ПЛАНИРОВАНИЕ МЕРОПРИЯТИЙ НА СЛУЧАЙ АВАРИЙНОЙ ОБСТАНОВКИ
• Обеспечить составление надлежащих и масштабируемых планов, предусматривающих непрерывность деятельности воздушного транспорта во время киберинцидентов. • Поощрять использование существующих планов на случай непредвиденных обстоятельств и включать в них положения о кибербезопасности и о проведении учений по тестированию киберустойчивости.

ОСНОВОПОЛАГАЮЩИЙ ЭЛЕМЕНТ 7. НАРАЩИВАНИЕ ПОТЕНЦИАЛА, ПОДГОТОВКА ПЕРСОНАЛА И КУЛЬТУРА КИБЕРБЕЗОПАСНОСТИ
• Обеспечить наличие квалифицированного персонала как в авиационных областях, так и в области кибербезопасности. • Повысить осведомленность о кибербезопасности. • 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 5

РЕАЛИЗАЦИЯ, МОНИТОРИНГ И ПЕРЕСМОТР

5.1. РЕАЛИЗАЦИЯ

ПДоК применяется в отношении ИКАО, ее государств-членов, отрасли и других заинтересованных сторон. Каждой организации рекомендуется соблюдать контрольные сроки, установленные в дорожной карте (см. добавление А), 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 кибербезопасности.

5.2. 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.

5.3. 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.

5.4. РОЛЬ ИКАО, ГОСУДАРСТВ И ЗАИНТЕРЕСОВАННЫХ СТОРОН

5.4.1. 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 SARPS и PANS, а также руководств и другого инструктивного материала;
- мониторинг и анализ ландшафта киберугроз и рисков;
- оказание целенаправленной помощи для устранения недостатков в системе авиационной кибербезопасности.

5.4.2. 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 6

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО[3]

6.1. СОСТАВЛЕНИЕ ПЕРЕЧНЯ ИНИЦИАТИВ В ОБЛАСТИ АВИАЦИОННОЙ КИБЕРБЕЗОПАСНОСТИ

6.1.1. 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).

6.2. СОЗДАНИЕ ОБЩЕЙ ОСНОВЫ ДЛЯ ИНТЕРОПЕРАБЕЛЬНОСТИ МЕР КИБЕРБЕЗОПАСНОСТИ И СИСТЕМ УПРАВЛЕНИЯ[4]

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

6.2.2. Поскольку доверие лежит в основе единообразного и интероперабельного управления информационными технологиями/системами связи, необходимо разработать механизм доверия, который обеспечивает глобальное, эффективное, единообразное и интероперабельное управление такими системами. Этот механизм доверия должен базироваться, помимо прочих элементов, на следующих категориях доверия:

- доверие, исходя из атрибутов: на основе идентификации и поведения;
- доверие, исходя из способов получения его подтверждения: либо напрямую, либо по рекомендации, включая использованные средства;
- доверие, исходя из определенной роли: либо установленной в каком-то кодексе/процедуре, третьей стороной, либо доверие к средствам и способам исполнения;
- доверие, исходя из субъективной или объективной оценки.

6.2.3. 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 и национальной безопасности следует разработать типовые формы для таких соглашений. В этой связи в качестве базовых принципов типовых соглашений необходимо определить следующие аспекты:

[3] Действия, относящиеся к настоящей главе, приведены в таблице 1 добавления A к плану действий.

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

- предмет и цель соглашения;
- меры, которые могут быть приняты сторонами для повышения кибербезопасности в гражданской авиации и которые подлежат координации;
- субъекты, которые могли бы заключить такие соглашения.

6.2.4. 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;
- принятие мер в поддержку наращивания потенциала там, где это требуется.

6.2.5. 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 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.

6.3. РАЗРАБОТКА ОБЩЕЙ ТЕРМИНОЛОГИИ

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

6.3.2. 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.

6.4. РАЗРАБОТКА ТИПОВОЙ СХЕМЫ ОБМЕНА ИНФОРМАЦИЕЙ/ ВЗАИМОДЕЙСТВИЯ В АВИАЦИИ

6.4.1. 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.

6.4.2. Эта высокоуровневая схема обмена информацией/взаимодействия должна носить достаточно общий характер, чтобы охватить все типы 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 6.6), могут быть предоставлены другим заинтересованным сторонам и использоваться ими. 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.

6.5. СОЗДАНИЕ СИСТЕМЫ МЕЖОРГАНИЗАЦИОННОГО ОБМЕНА ИНФОРМАЦИЕЙ О РИСКАХ

6.5.1. 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 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.

6.5.2. Для создания общей основы для такого типа обмена следует изучить возможность разработки стандартизированного внешнего соглашения, которое предусматривает разрешение проблем информационной безопасности в отношении внешнего интерфейса и/или использования продуктов третьих сторон (в настоящее время имеется несколько примеров такого соглашения). Концепция внешнего соглашения предусматривает требование об обмене соответствующей информацией о безопасности в отношении интерфейса или продукта для поддержки управления общими угрозами и рисками во всей цепи поставок.

6.6. ОПРЕДЕЛЕНИЕ КРИТЕРИЕВ СОПОСТАВИМОСТИ ПОЗИЦИЙ В ОТНОШЕНИИ ОЦЕНКИ РИСКОВ

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

6.7. ОБЕСПЕЧЕНИЕ НАДЛЕЖАЩЕЙ КООРДИНАЦИИ ГРАЖДАНСКИХ И ВОЕННЫХ ОРГАНОВ

6.7.1. По возможности и в соответствии с требованиями национальной безопасности и национальной обороны следует обеспечивать взаимодействие гражданских и военных авиационных органов с должным учетом требований национальной безопасности и обороны в плане конфиденциальности и безопасности, а также в соответствующих случаях и надлежащих условиях следует предусмотреть взаимодействие со структурами других государств.

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

6.7.3. 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.

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

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

Глава 7

УПРАВЛЕНИЕ

7.1 ИКАО ДОЛЖНА СОЗДАТЬ СТРУКТУРУ УПРАВЛЕНИЯ

7.1.1. ИКАО следует создать структуру управления и подотчетности для авиационной кибербезопасности, в которую войдут обладающие надлежащей квалификацией специалисты в области авиационной безопасности, безопасности полетов, устойчивости и эксплуатационной непрерывности от государств и отрасли (авиационное сообщество и сообщество кибербезопасности). Эта структура должна отвечать критериям, одобренным 40-й сессией Ассамблеи ИКАО.

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

7.2.1. 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.

7.3 РАЗРАБОТКА СИСТЕМЫ УПРАВЛЕНИЯ И ПОДОТЧЕТНОСТИ

7.3.1. ИКАО следует разработать инструктивный материал по политике в области кибербезопасности в целях обеспечения гармонизации и согласованности глобальной, региональной и национальной политики. Аспекты, характерные для конкретных стран, должны быть обоснованы и должны способствовать транснациональной согласованности.

7.3.2. Государствам и организациям рекомендуется ввести в действие систему менеджмента информационной безопасности (СМИБ) с учетом общего подхода к управлению и определить конкретные функции и обязанности в области кибербезопасности гражданской авиации. Государствам следует на национальном уровне предпринимать значимые действия по непрерывному повышению эффективности, качества и согласованности процессов управления кибербезопасностью.

7.3.3. Меры по управлению кибербезопасностью должны быть обусловлены проводимой политикой и должно быть обеспечено их введение, также необходимо определить подотчетность для контроля соблюдения. Персонал должен соблюдать положения, аналогичные положениям систем управления авиационной безопасностью и безопасностью полетов. На национальном уровне программа по кибербезопасности в гражданской авиации должна реализовываться по принципу "сверху – вниз", с тем чтобы способствовать осуществлению процессов и достижению целей и обеспечивать следование протоколам. На всем протяжении жизненного цикла программы старшее руководство должно принимать участие в ее выполнении[5].

[5] При разработке программы по кибербезопасности на национальном уровне государства могут обратиться к материалам ИСО 27001 для определения принципов руководства[5], 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 8

ДЕЙСТВЕННОЕ ЗАКОНОДАТЕЛЬСТВО И НОРМАТИВНО-ПРАВОВАЯ БАЗА

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

8.1.1 ИКАО проведет анализ существующих документов международного воздушного права, с тем чтобы выявить действительные и потенциальные недостающие положения, касающиеся киберугроз, и предложить потенциальные решения для ликвидации выявленных пробелов в целях дальнейшей защиты гражданской авиации.

8.2 ПРИВЕДЕНИЕ ПОЛОЖЕНИЙ ИКАО В СООТВЕТСТВИЕ С ПОТРЕБНОСТЯМИ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

8.2.1. 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 то соображение, что добавления новых положений следует избегать, насколько это возможно, и при необходимости такое добавление должно координироваться между всеми соответствующими группами экспертов.

8.3 РАТИФИКАЦИЯ ПЕКИНСКОЙ КОНВЕНЦИИ И ПРОТОКОЛА

8.3.1 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).

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

8.4.1. 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 в отношении конкретных элементов кибербезопасности гражданской авиации. Другим ключевым компонентом является механизм правоприменения, который государствам рекомендуется ввести в действие для криминализации и судебного преследования в случае совершения незаконных кибератов, направленных против гражданской авиации.

Глава 9

ПОЛИТИКА В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

9.1. РАЗРАБОТКА И ВНЕДРЕНИЕ ПОЛИТИКИ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

9.1.1. Наряду с рядом политических мер, касающихся управления риском для кибербезопасности гражданской авиации, на глобальном, региональном и национальном уровнях следует разработать инструктивный материал в поддержку эффективной реализации СМИБ.

9.1.2. Такой инструктивный материал может быть разработан на базе уже существующих документов:

- для оказания помощи в определении сферы применения СМИБ;
- для самооценки текущего статуса;
- для установления контрольных сроков достижения зрелости системы;
- для разработки плана для соблюдения контрольного срока достижения зрелости системы.

9.1.3. Необходимо разработать политику в области кибербезопасности на национальном и организационном уровнях. Государства должны использовать критерии разработки четкой и действенной политики в области кибербезопасности, включающей:

- 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 управление информационной безопасностью;
- положения, обеспечивающие, что политика полностью документирована и доступна в виде официального документа;
- положения, обеспечивающие, что политика должным образом распространяется.

9.2. ВЫЯВЛЕНИЕ И ОЦЕНКА КИБЕРРИСКОВ ДЛЯ ГРАЖДАНСКОЙ АВИАЦИИ

9.2.1. Одна из проблем выявления риска и его оценки заключается в способности предвидеть весьма быстрые изменения в источниках 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.

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

9.2.3. Поскольку со значительной частью рисков для кибербезопасности гражданской авиации сталкиваются многие заинтересованные стороны, рекомендуется рассмотреть схему обмена информацией/взаимодействия в авиации (см. главу 6.1). 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.

9.2.4. Практически невозможно оценить риски для всех возможных сценариев, которые могут существовать в мире. Поэтому необходимо рассмотреть типовую архитектурную и оперативную основу кибербезопасности гражданской авиации, которая позволит выявлять и оценивать типовые риски. Участвующие в деятельности гражданской авиации стороны должны будут при необходимости повторно изучать эти типовые риски на индивидуальной основе и затем адаптировать их с учетом конкретных инфраструктурных и эксплуатационных требований своей системы. Для того чтобы они могли уяснить контекст анализов типовых рисков и адаптировать результаты оценки рисков к своим конкретным условиям, все допущения в рамках моделируемых типовых рисков должны быть полностью документированы.

9.2.5. Поскольку уровень серьезности рисков для кибербезопасности будет со временем меняться (т. е. 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).

9.2.6. Рекомендуется, чтобы деятельность по выявлению и оценке типовых 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.

9.2.7. Эта группа экспертов должна отвечать за разработку заявления о контексте киберриска, дополняющего существующий документ Doc 10108 в части аспектов кибербезопасности.

9.2.8. Группа экспертов должна тесно сотрудничать с WGTR и другими группами экспертов по мере необходимости для обеспечения отсутствия каких-либо пробелов, дублирования или несоответствий при оценке рисков для кибербезопасности и согласования своих рекомендаций с рекомендациями AVSECP и других групп экспертов в соответствующих случаях.

Глава 10

ОБМЕН ИНФОРМАЦИЕЙ

Обмен информацией в поддержку управления авиационной безопасностью необходим для защиты систем гражданской авиации и укрепления кибербезопасности. Исходя из понимания того, что содействие обмену информацией является ключевым элементом создания культуры кибербезопасности, заинтересованным сторонам гражданской авиации следует разработать и внедрить программы, обеспечивающие возможность обмена 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 защиты гражданской авиации в соответствии с известными и возникающими угрозами безопасности. Они должны способствовать развитию:

- ситуационной осведомленности как в обычных повседневных операциях, так и в кризисной ситуации или при возникновении инцидента;
- 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.

10.1. РАЗРАБОТКА СИСТЕМЫ ОБМЕНА ИНФОРМАЦИЕЙ О РИСКАХ

10.1.1. 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 цепочки поставок).

10.1.2. Установлено, что существует много типов информации, касающейся кибербезопасности, например:

- *Киберразведданные* (ландшафт угроз, разведданные о возможностях и намерениях киберзлоумышленников): они могут быть конфиденциальными и возможны ограничения (протокол "светофор" или маркировка TLP могут до некоторой степени помочь в деле обмена ими).

- *Показатели компрометации (IoC):* ими можно обмениваться, поскольку они не относятся к индивидуальным системам/службам (все еще следует использовать TLP (протокол "светофор")). IOC – это, например, вредоносный IP, вредоносный URL, хеширование вредоносной программы. Обмен такой информацией

поможет другим сторонам обеспечить свою защиту; аналогичным образом, получение такой информации от других сторон поможет организациям эффективнее защитить свои системы/службы. Нет необходимости более подробно раскрывать, кто их обнаружил (будь то ПАНО A или ПАНО B, или эксплуатант аэропорта C, или эксплуатант аэропорта D, или пользователь воздушного пространства E, или пользователь воздушного пространства F и т. д.), поскольку это не добавляет какой-либо значимости.

- *Тактика, методы и процедуры (TTPs)* (сценарии атак, предпочтительные методы, используемые хакерами): этой информацией можно обмениваться (все еще следует использовать TLP), поскольку она, как правило, не относится к конкретным системам/службам.

- *Уязвимости:* следует обмениваться только значимой информацией об уязвимостях (аппаратное оборудование, программное обеспечение, служба, протокол, стандарт и т. д.), включая возможные сценарии эксплуатации, но не о тех, кто может их использовать.

- *Донесения об инцидентах:* можно использовать TLP и удалить идентификационные данные для обмена информацией о некоторых инцидентах, а информация о некоторых инцидентах может обмену не подлежать.
  a) серьезные инциденты: допускается обмен информацией из обязательных донесений на национальном/региональном уровнях (например, согласно общим правилам кибербезопасности и защите данных, таким как Общие правила защиты данных Европейского союза – GDPR, или национальным или региональным правилам по критическим инфраструктурам, например директиве NIS);

  b) инциденты, не являющиеся серьезными, и потенциальные инциденты: информация может предоставляться (с удалением идентификационных данных).

10.1.3. 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).

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

10.1.5. При распространении и более широком обмене киберинформацией рекомендуется использовать TLP, с тем чтобы указать уровень распространения/ограничений (см. добавление B).

10.1.6. В подавляющем большинстве случаев киберинформацией можно обмениваться без использования системы классификации информации (например, конфиденциальная/секретная/совершенно секретная). Использование такой системы должно быть скорее исключением, чем правилом.

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

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

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

10.2.2. Инструктивные указания относительно этих принципов (касающиеся, помимо других вопросов, например, обнаружения, уведомления, расследования, разрешения и раскрытия) 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.

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

10.3.1. В государствах и отрасли отсутствует единообразие в части распределения ответственности за кибербезопасность, а специалисты, обладающие надлежащими знаниями в этой области, рассредоточены по самым разным внешним 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.

10.4. ГЛОБАЛЬНАЯ СИСТЕМА ОБМЕНА ИНФОРМАЦИЕЙ О КИБЕРБЕЗОПАСНОСТИ ДЛЯ АВИАЦИИ

10.4.1. 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.

Глава 11

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ И ПЛАНИРОВАНИЕ МЕРОПРИЯТИЙ НА СЛУЧАЙ АВАРИЙНОЙ ОБСТАНОВКИ

11.1. РАЗРАБОТКА СРЕДСТВ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ И ПЛАНИРОВАНИЕ МЕРОПРИЯТИЙ НА СЛУЧАЙ АВАРИЙНОЙ ОБСТАНОВКИ

11.1.1. 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 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;
- координацию систем представления данных об инцидентах в области гражданской авиации и в области кибербезопасности на национальном, региональном и, по возможности, международном уровнях.

11.2. ОБНАРУЖЕНИЕ И АНАЛИЗ ИНЦИДЕНТОВ И СРЕДСТВА РЕАГИРОВАНИЯ НА НИХ НА УРОВНЕ ЗАИНТЕРЕСОВАННЫХ СТОРОН

11.2.1. 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.

11.3. СОЗДАНИЕ В ГРАЖДАНСКОЙ АВИАЦИИ ПОДРАЗДЕЛЕНИЯ ДЛЯ КООРДИНАЦИИ ДЕЙСТВИЙ В КРИЗИСНОЙ СИТУАЦИИ

11.3.1. 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.

11.3.2. Следует на регулярной основе проводить периодические учения, в частности теоретические учения (ТТХ), основанные на реальных инцидентах, с привлечением представителей всех соответствующих заинтересованных сторон отрасли.

Глава 12

НАРАЩИВАНИЕ ПОТЕНЦИАЛА, ПОДГОТОВКА ПЕРСОНАЛА, КУЛЬТУРА КИБЕРБЕЗОПАСНОСТИ И ОБРАЗОВАНИЕ

12.1. НАРАЩИВАНИЕ ТЕХНИЧЕСКОГО ПОТЕНЦИАЛА, ПОДГОТОВКА ПЕРСОНАЛА, КУЛЬТУРА КИБЕРБЕЗОПАСНОСТИ И ОБРАЗОВАТЕЛЬНЫЕ МАТЕРИАЛЫ

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

12.1.2 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 и создающий возможность для передачи технических знаний, обеспечивающих 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).

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

12.1.4 Формирование такой культуры кибербезопасности и популяризация культуры кибербезопасности и образовательных материалов в этой области должны способствовать

взаимному/общему пониманию в сообществах, отвечающих за авиационную безопасность и безопасность полетов, ландшафта рисков в области кибербезопасности, а также укреплению взаимной уверенности в принимаемых контрмерах.

12.1.5 ИКАО следует поощрять осуществление транснациональных/трансрегиональных программ обмена в области образования и подготовки по кибербезопасности[6].

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

- проектирование (безопасность аппаратных средств, программного обеспечения и данных, управление изменениями, управление уязвимостью);
- изготовление/приобретение (включая отраслевую цепь поставок);
- эксплуатацию (включая управление доступом, целостность данных, безопасное функционирование систем);
- техническое обслуживание (включая стратегию выпуска патчей и обновлений);
- ликвидацию (включая управление идентификаторами и остаточными данными на запоминающих устройствах).

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

Глава 13

ВЫВОД

План действий по обеспечению кибербезопасности объединит 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 продемонстрирует то, что кибербезопасность является комплексной проблемой и затрагивает все сферы авиационного сектора. Этот план будет способствовать выполнению ИКАО, государствами, отраслью и другими заинтересованными сторонами своих обязательств, вытекающих из стратегии кибербезопасности ИКАО, в целях создания 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 следует решать в рамках Конвенции о международной гражданской авиации.

Действия

Действие #	**Исполнитель**	**Конкретные меры/задачи**	**Показатели**	**Зрелость**	**Контрольный срок**
ПДоК 0.1	ИКАО	ИКАО должна разработать типовое заявление о политике в области кибербезопасности на международном уровне. Государствам-членам и отрасли следует разработать такие типовые заявления о политике на национальном и организационном уровне.	Типовой образец имеется для предоставления государствам и отрасли		2020 г.
ПДоК 0.2	ИКАО и государства-члены	Начать работу по реализации стратегии кибер-безопасности 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		2021 г.
ПДоК 0.3	ИКАО	Провести исследование для определения того, как государства реализуют стратегию кибербезопасности ИКАО (вопросник относительно того, разработали ли государства план действий по реализации стратегии).	Исследование/вопросник ИКАО, направленный государствам-членам		2022 г.

ОСНОВОПОЛАГАЮЩИЕ ЭЛЕМЕНТЫ СТРАТЕГИИ КИБЕРБЕЗОПАСНОСТИ

Приоритетный результат	**1. ОБЕСПЕЧЕНИЕ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА**
Приоритетные действия	• Развивать сотрудничество на национальном и международном уровнях. • Признать на взаимной основе необходимость мер (обеспечение, поддержание и повышение кибербезопасности) по защите гражданской авиации. • Добиться регуляторной гармонизации на глобальном, региональном и национальном уровне, 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.

Действия

Действие #	**Исполнитель**	**Прослежи-ваемость связи со стратегией кибербезо-пасности**	**Прослежи-ваемость связи с планом действий**	**Конкретные меры/задачи**	**Показатели**	**Зрелость**	**Контроль-ный срок**
ПДоК 1.1	ИКАО	1.1.	6.2	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	н. д.	На постоянной основе
ПДоК 1.2	ИКАО	1.1.	6.1 См. также ПДоК 4.7 (п. 9.2 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	н. д.	На постоянной основе
ПДоК 1.3	ИКАО	1.1	6.1	Составить перечень всех инициатив в области кибербезопасности, связанных с различными группами экспертов, поддерживающими ИКАО.			2020 г.

ПДоК 1.4	ИКАО	1.2	6.2.3 и 6.5 См. также ПДоК 5.1 (п. 10.2 плана действий)	A) Разработать образцы типовых меморандумов о взаимопонимании/ сотрудничестве и внешних соглашений; B) дать рекомендации относительно методики разработки/ внедрения/обзора этих соглашений.	Наличие шаблона и рекомендаций	н. д.	2022–2023 гг.
ПДоК 1.5	ИКАО	1.2	6.5	A) Разработать образцы типовых внешних соглашений, связанных с управлением общими рисками; B) дать рекомендации относительно методики разработки этих соглашений.			
ПДоК 1.6	ИКАО	1.2	6.3	Разработать общую 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	н. д.	2021 г.
ПДоК 1.7	ИКАО, государства-члены и отрасль	1.2	6.4	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	Высокая	2022 г.

ПДоК 1.8	ИКАО в сотрудничестве с государствами-членами при необходимости	1.2	6.7 См. также ПДоК 6.2 и п. 11.2 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. Государствам-членам следует сотрудничать с ИКАО по мере необходимости.	Доказательство наличия таких моделей/руководящих указаний для сотрудничества и интероперабельности гражданских и военных органов в сфере кибербезопасности Опубликованный перечень критериев и минимального количества требуемых мер взаимодействия	Высокая	2021 г.
ПДоК 1.9	ИКАО, государства-члены и отрасль	1.3	6.8	ИКАО при поддержке государств-членов и отрасли должна планировать, организовать и поддерживать международные и региональные мероприятия по содействию повышению кибербезопасности в гражданской авиации.	Международное сотрудничество в проведении мероприятий, повышении осведомленности	н. д.	Доклад Ассамблее к 2022 г.
ПДоК 1.10	ИКАО, государства-члены и отрасль	1.3	6.4	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.	Низкая	На постоянной основе
ПДоК 1.11	ИКАО	1.3	6.2	ИКАО должна обеспечить включение государствами-членами вопросов кибербезопасности в их национальные программы гражданской авиации по безопасности полетов и авиационной безопасности.	Обзор ИКАО: число государств, которые включили вопросы кибербезопасности в свои национальные программы по безопасности полетов и авиационной безопасности	н. д.	Обзор 2020 г. Дальнейшие действия на постоянной основе
ПДоК 1.12	ИКАО, государства-члены и отрасль	1.2	6.2.2	Разработать механизм доверия в рамках международной авиации, позволяющий организациям взаимодействовать исходя из их доверия к другим заинтересованным сторонам.	Разработка механизма доверия, используемого многими организациями	Высокая	2022–2023 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 планом действий**	**Конкретные меры/задачи**	**Показатели**	**Зрелость**	**Контроль-ный срок**
ПДоК 2.1	ИКАО		7.1	Создать структуру управления в области кибербезопасности.	Определение наиболее целесообразной структуры управления кибербезопасностью	**н. д.**	2021 г.
ПДоК 2.2	ИКАО	2.2	7.3	ИКАО должна разработать общий набор принципов создания надлежащей системы управления кибербезопасностью. Государствам-членам следует разработать такие принципы на национальном уровне в соответствии с моделью ИКАО.	Публикация общих принципов	Средняя	2022–2023 гг.
ПДоК 2.3	ИКАО, государства-члены и отрасль	2.2	7.3.2 См. также п. 9.1. плана действий	Разработать инструктивный материал для оказания помощи организациям в реализации скоординированной СМИБ и оценить зрелость и эффективность СМИБ.	Публикация инструктивных указаний	Средняя	2021 г.

ПДоК 2.4	ИКАО и государства-члены	2.2	7.3	Содействовать созданию механизмов координации между ведомствами гражданской авиации и органами по кибербезопасности	Обзор ИКАО: число выявленных существующих действующих координационных механизмов	Средняя	2020 г.
ПДоК 2.5	ИКАО	2.3	7.2.1 См. также ПДоК 1.10 (п. 6.2 плана действий)	ИКАО должна включить вопросы кибербезопасности в региональные и глобальные планы	Публикация обновленных планов	н. д.	2022–2023 гг.
ПДоК 2.6	ИКАО		7.2	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	Государства-члены	3.2	7.3, 6.2	Разработать критерии и контрольные перечни для включения вопросов кибербезопасности в программы проверки.	Разработка критериев и контрольных перечней Включение вопросов кибербезопасности в директивные документы государств по организации контроля за обеспечением безопасности полетов и авиационной безопасности	Высокая	2022–2023 гг.
ПДоК 2.8	ИКАО, государства-члены и отрасль	3.2	7.3	ИКАО должна разработать типовой порядок действий по представлению данных о киберинцидентах. Государствам-членам и отрасли следует разработать национальный и организационный порядок действий по представлению данных о киберинцидентах.	Порядок действий по представлению данных о киберинцидентах/числе инцидентов, о которых представлены данные в установленном порядке	Высокая	2022–2023 гг.

Приоритетный результат	**3. РАЗРАБОТКА ДЕЙСТВЕННОГО ЗАКОНОДАТЕЛЬСТВА И НОРМАТИВНЫХ ПОЛОЖЕНИЙ**
Приоритетные действия	• Обеспечить введение в действие надлежащих нормативных положений и законодательства в области кибербезопасности. • Разработать для государств и отрасли надлежащие инструктивные указания относительно внедрения положений о кибербезопасности. • Обеспечить наличие в международных правовых документах надлежащих мер по предотвращению киберинцидентов, возбуждению судебного преследования в связи с киберинцидентами и по своевременному реагированию на них.

Действия

Действие #	**Исполнитель**	**Прослежи-ваемость связи со стратегией кибербезо-пасности**	**Прослежи-ваемость связи с планом действий**	**Конкретные меры/задачи**	**Показатели**	**Зрелость**	**Контроль-ный срок**
ПДоК 3.1	Государства-члены	3.3	8.4	Государства-члены должны ратифицировать пекинские документы.	Число государств, ратифицировавших пекинские документы	Низкая	На постоянной основе
ПДоК 3.2	ИКАО	3.3	8.3	Анализ документов по международному воздушному праву	Доклад и обновление плана	н. д.	2020 г.
ПДоК 3.3	ИКАО и государства-члены	3.3	8.2	Анализ существующего международного и национального законодательства в области кибербезопасности и выявление пробелов, в том числе в уголовном праве	Стимулирование ратификации документов по инкриминированию незаконных кибератактов.	Средняя	2022–2023 гг.
ПДоК 3.4	ИКАО, государства-члены и отрасль	3.3	8.1	Проанализировать существующие стандарты по авиационной безопасности ИКАО для выявления необходимости их обновления на предмет кибербезопасности.	Анализ пробелов в нормативных положениях	Высокая	2021 г.
ПДоК 3.5	ИКАО	3.2	5.4	Создать, пересматривать и изменять инструктивный материал, касающийся внедрения требований по обеспечению кибербезопасности.	Принятый и согласованный инструктивный материал по кибербезопасности	Высокая	2021–2022 гг.

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

Действия							
Действие #	**Исполнитель**	**Прослеживаемость связи со стратегией кибербезопасности**	**Прослеживаемость связи с планом действий**	**Конкретные меры/задачи**	**Показатели**	**Зрелость**	**Контрольный срок**
ПДоК 4.1	ИКАО, государства-члены и отрасль	4.1	9.1	ИКАО должна разработать политику в области кибербезопасности (с использованием модели, разработанной ИКАО в соответствии с действием ПДоК 0.1) для содействия согласованию национальной политики с глобальной и региональной политикой. Аспекты, характерные для конкретных стран, должны быть обоснованы и должны способствовать транснациональной согласованности. Государствам-членам и отрасли следует разработать национальную и организационную политику. Разработка мероприятий по наращиванию потенциала	Разработка мероприятий по наращиванию потенциала Публикация исследования ИКАО относительно политики государств-членов в области кибербезопасности	Низкая	2022–2023 гг.
ПДоК 4.2	Государства-члены и отрасль	4.1.	9.1	В организациях руководство высшего звена должно взять обязательство по принятию и поддержке мер своих организаций в области кибербезопасности.	Кампания по повышению осведомленности/доказательства взятия обязательств, такие как декларации об обязательствах, обязанности в области кибербезопасности,	Средняя	2022–2023 гг.

				Государства-члены (в лице национальных ведомств гражданской авиации) и отрасль должны обеспечить взятие обязательств их руководством.	определенные в руководствах по управлению органов власти и организаций		
ПДоК 4.3	ИКАО, государства-члены и отрасль	4.3	9.2 См. также п. 6.11 плана действий	Содействовать проведению научно-исследовательской работы в гражданской авиации в области кибербезопасности путем установления контактов с университетами, институтами, исследовательскими сообществами и т. д.	Число контактов и проектов	Высокая	2022–2023 гг.
ПДоК 4.4	ИКАО, государства-члены и отрасль	4.2.	6.6 и 9.2	Установить критерии проведения совместной трансорганизационной оценки риска наряду с определением подлежащей обмену информации, а необходимые критерии сопоставимости рисков будут разработаны ИКАО. Государствам-членам следует установить такие критерии на национальном уровне, а отрасли – на организационном уровне.	Публикация целей и критериев совместной трансорганизационной оценки риска	Высокая	2022 г.
ПДоК 4.5	ИКАО, государства-члены и отрасль	4.3	9.1	Разработать политику обеспечения безопасности на этапе разработки в качестве основы для безопасного жизненного цикла авиационных систем.	Разработанная политика безопасного жизненного цикла авиационных систем	Средняя	2022–2023 гг.
ПДоК 4.6	ИКАО, государства-члены и отрасль	4.2.	9.2	ИКАО должна организовать международные форумы для обсуждения задач трансорганизационной/трансфункциональной безопасности и устойчивости минимального уровня функциональных возможностей, критически необходимых для сектора гражданской авиации. Государствам-членам следует организовывать такие форумы на национальном региональном уровне, а отрасли следует организовывать специальные форумы и	Количество форумов для обсуждения задач	Высокая	2022–2023 гг.

				активно участвовать в форумах, организуемых ИКАО и государствами-членами.			
СуАР 4.7	ИКАО, государства-члены и отрасль	4.3	9.2	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	Средняя	2020 г.
ПДоК 4.8	ИКАО, государства-члены и отрасль	4.3	9.3	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 в поддержку ПДоК 4.7	Высокая	2022 - 2023
ПДоК 4.9	ICAO, государства-члены и отрасль		9.2	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	Высокая	2022 г.
ПДоК 4.10	ИКАО		9.2	Создать реестр угроз и рисков в области кибербезопасности для дополнения заявления WGTR о контексте риска материалами по кибербезопасности, не связанными с терроризмом, даже если это будет реестром теоретических угроз и рисков.	Наличие реестра угроз и рисков в области кибербезопасности	н. д.	2020 г.

Приоритетный результат	**5. РАЗВИТИЕ ПОТЕНЦИАЛА ДЛЯ ОБМЕНА ИНФОРМАЦИЕЙ**						
Приоритетные действия	• Разработать платформы и механизмы обмена информацией, которые соответствуют существующим положениям ИКАО, для предотвращения, раннего обнаружения и смягчения последствий соответствующих киберсобытий.						
Действия							
Действие #	**Исполнитель**	**Прослеживаемость связи со стратегией кибербезопасности**	**Прослеживаемость связи с планом действий**	**Конкретные меры/задачи**	**Показатели**	**Зрелость**	**Контрольный срок**
ПДоК 5.1	ИКАО и государства-члены	**5**	10.2 См. также ПДоК 1.3 (п. 6.5 плана действий)	ИКАО должна изучить концепцию стандартизированного внешнего соглашения и разработать в соответствии с действием ПДоК 1.3 типовое соглашение ИКАО, которое охватывает проблемы информационной безопасности, связанные с внешним интерфейсом и/или использованием продуктов третьих сторон. Государствам-членам следует на основе типового соглашения ИКАО разработать национальные типовые соглашения. Разработать типовое внешнее соглашение, если будет сочтено необходимым.	Публикация образца.	Высокая	2022–2023 гг.
ПДоК 5.2	ИКАО, государства-члены и отрасль	5.1.	10.1 10.2	ИКАО при поддержке государств-членов и отрасли должна разработать инструктивный материал по обмену информацией.	Инструктивный материал по обмену информацией, доступный сообществу	Высокая	2022–2023 гг.
ПДоК 5.3	ИКАО, государства-члены и отрасль	5.1.	10.1	ИКАО при поддержке государств-членов и отрасли должна определить потребности в обмене информацией о кибербезопасности и сотрудничестве (включая, в частности, во	Разработать перечень потенциальной подлежащей обмену информации	н. д.	2020–2023 гг.

				время кризисных ситуаций), а также политику.			
ПДоК 5.4	ИКАО, государства-члены и отрасль	5.1.	10.1	Использовать TLP (протокол "светофор") для определения уровня распространения/ограничений при распространении киберинформации и дальнейшем обмене такой информацией.	Публикация инструктивного материала по политике использования TLP при распространении и обмене	Высокая	2020 г.
ПДоК 5.5	ИКАО, государства-члены и отрасль	5.2.	10.2	Определить принципы ответственного раскрытия уязвимостей.	Наличие и распространение принципов ответственного раскрытия уязвимостей	Высокая	2020 г.
ПДоК 5.6	ИКАО, государства-члены и отрасль	5.2	10.4	ИКАО должна разработать и поддерживать сеть координаторов по вопросам кибербезопасности на международном уровне для государств-членов и отрасли. Государствам-членам следует в сотрудничестве с ИКАО разработать такую сеть на национальном уровне.	Создание сети по вопросам кибербезопасности Публикация сети координаторов	Средняя	2021–2023 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 деятельности воздушного транспорта во время киберинцидентов. • Поощрять использование существующих планов на случай непредвиденных обстоятельств, включать в них положения о кибербезопасности и проводить учения для тестирования киберустойчивости.

Действия

Действие #	**Исполнитель**	**Прослежи-ваемость связи со стратегией кибербезо-пасности**	**Прослежи ваемость связи с планом действий**	**Конкретные меры/задачи**	**Показатели**	**Зрелость**	**Контроль-ный срок**
ПДоК 6.1	Государства-члены устанавливают задачи Отрасль выполняет задачи	6.1.	11.1	Государства-члены должны установить задачи и минимальные уровни функциональных возможностей, имеющих важное значение для сектора гражданской авиации. Отрасль должна выполнить установленные задачи (согласно действию ПДоК 4.6).	Публикация перечня задач и минимальных приемлемых уровней для авиационного сообщества	Высокая	2022–2023 гг.
ПДоК 6.2	ИКАО и государства-члены	6.1.	11.2	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.	Определение процессов сотрудничества гражданских/ военных органов в сфере реагирования на киберинциденты	Высокая	2022–2023 гг.

ПДоК 6.3	ИКАО, государства-члены и отрасль	6.1.	11.1	ИКАО должна разработать инструктивный материал по созданию механизмов реагирования на киберинциденты и восстановления после них, включая планы мероприятий на случай непредвиденной и аварийной обстановки. Государствам-членам и отрасли следует разработать такие инструктивные указания в соответствии с моделью ИКАО на национальном и организационном уровне.	Публикация инструктивного материала по созданию механизмов реагирования на киберинциденты и восстановления после них, включая планы мероприятий на случай непредвиденной и аварийной обстановки.	Высокая	2022–2023 гг.
ПДоК 6.4	Государства-члены	6.1.	11.2 и 11.3	Государства-члены должны подготовить инструктивный материал, создать механизмы и разработать планы для обнаружения и анализа киберинцидентов и мер реагирования на них на оперативном уровне в целях осуществления контроля за деятельностью отрасли.	Исследование об уровне или степени готовности плана	Высокая	2026 г.
ПДоК 6.5	Государства-члены	6.1.	11.1	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 Представленный типовой порядок действий	Средняя	2022–2023 гг.
ПДоК 6.6	Государства-члены и отрасль	6.1	11.3	Периодически проводить теоретические учения (ТТХ), основанные на реальных инцидентах.	Выводы, сделанные по итогам ТТХ	Высокая	2022–2023 гг.

Приоритетный результат	**7. НАРАЩИВАНИЕ ПОТЕНЦИАЛА, ПОДГОТОВКА ПЕРСОНАЛА И ФОРМИРОВАНИЕ КУЛЬТУРЫ КИБЕРБЕЗОПАСНОСТИ**
Приоритетные действия	• Обеспечить наличие квалифицированного персонала как в авиационных областях, так и в области кибербезопасности. • Повысить осведомленность о кибербезопасности. • Обеспечить включение в национальную образовательную структуру на уровне профессиональной подготовки надлежащей учебной программы по авиационной кибербезопасности с целью обеспечения наличия багажа знаний по всем аспектам безопасности полетов и авиационной безопасности на всех уровнях организации, начиная с руководства 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 планом действий**	**Конкретные меры/задачи**	**Показатели**	**Зрелость**	**Контроль-ный срок**
ПДоК 7.1	ИКАО, государства-члены и отрасль	7.1.	12.1	Определить и популяризировать культуру и образование в области кибербезопасности гражданской авиации.	Наличие курсов и инструктивного материала, касающихся культуры кибербезопасности гражданской авиации	Средняя	2022–2023 гг.
ПДоК 7.2	ИКАО, государства-члены и отрасль	7.2.	12.1	ИКАО должна выявить пробелы в существующих должностных обязанностях в авиационной области, с тем чтобы надлежащим образом решить проблемы кибербезопасности, а также разработать инструктивный материал и специальную подготовку. Государствам-членам и отрасли следует разработать требования к подготовке на всех уровнях в рамках их организаций.	Разработка надлежащей подготовки по выполнению должностных обязанностей	Высокая	2022–2023 гг.

ПДоК 7.3	ИКАО и государства-члены	7.3.	12.1	ИКАО должна включить кибербезопасность в стратегию NGAP. Государствам-членам следует, вслед за ИКАО, включить кибербезопасность в свои национальные стратегии, связанные со стратегией по следующему поколению авиационных специалистов.	Включение кибербезопасности в NGAP	Средняя	2022–2023 гг.
ПДоК 7.4	ИКАО, государства-члены и отрасль	7.3.	12.1	Проанализировать способы и средства разработки квалификационных требований на основе ролевых моделей. ИКАО должна создать рабочую группу с кругом полномочий для разработки таких требований. Государствам-членам и отрасли следует принять участие в этой рабочей группе и разработать квалификационные требования на национальном и организационном уровнях.	Включение кибербезопасности в документы Doc 7192 и 9868 ИКАО	Высокая	2022–2023 гг.

— — — — — — —

ДОБАВЛЕНИЕ В

Определение протокола "светофор" (TLP)

Протокол "светофор" (TLP) – это метод, с помощью которого лицо, которое предоставляет информацию, информирует свою аудиторию о любых ограничениях в отношении дальнейшего распространения такой информации.

Протокол "светофор" (TLP) был разработан и введен в действие в 2000 году Координационным центром правительства Соединенного Королевства по безопасности национальной структуры (NISCC, в настоящее время Центр по защите национальной инфраструктуры – CPNI)

TLP указывает, когда и как можно обмениваться конфиденциальной информацией, и способствует осуществлению более частых и эффективных контактов в рамках сотрудничества. Он широко используется в таких организациях, как CERT, CSIRT и ISAC.

В дополнение к TLP можно использовать другие элементы, такие как правила "Чатем-Хаус", общая система оценки уязвимости (CVSS) и политика в области обмена информацией (IEP) – форума FIRST. В принципе, TLP пользоваться легко: предоставляющий информацию субъект маркирует данную информацию определенным цветом. Маркировка информации состоит просто в обозначении документа или его части пометкой "TLP: ЦВЕТ". Цвет указывает на возможность дальнейшего распространения данной информации. Со временем в TLP стали использоваться различные формулировки, однако недавно сообщество CSIRT предприняло попытку разъяснить значение TLP.

ЦВЕТ	ЗНАЧЕНИЕ	ПРИМЕР
КРАСНЫЙ	Раскрытию не подлежит, только для участников. Источники могут использовать TLP: КРАСНЫЙ, когда другим сторонам нельзя практически использовать информацию и она, в случае злонамеренного использования, может негативно повлиять на конфиденциальность, репутацию или операции определенной стороны. Получателям нельзя обмениваться информацией с маркировкой TLP: КРАСНЫЙ с какой-либо стороной за пределами особой процедуры обмена, совещания или переговоров, в ходе которых она была первоначально раскрыта. Например, в контексте совещания информация с маркировкой TLP: КРАСНЫЙ предназначена только для лиц, присутствующих на данном совещании. В большинстве случаев информацией с маркировкой TLP: КРАСНЫЙ следует обмениваться устно или лично.	Обмен информацией с участниками совещания; прямая эл. почта.

ЦВЕТ	ЗНАЧЕНИЕ	ПРИМЕР
ЖЕЛТЫЙ	Ограниченное раскрытие, только для участвующих организаций. Источники могут использовать TLP: ЖЕЛТЫЙ, когда для эффективных действий по этой информации требуется определенная поддержка, но она создает риск для конфиденциальности, репутации или операций, если ею обмениваться за пределами участвующих организаций. Получателям разрешается обмениваться информацией с маркировкой TLP: ЖЕЛТЫЙ только с членами их собственной организации и с клиентами или потребителями, которым необходимо знать эту информацию для своей защиты или предотвращения дальнейшего ущерба. Источники могут указать дополнительные предполагаемые ограничения обмена информацией: они должны соблюдаться.	Предоставление показателей компрометации (IoC) группе CSIRT организации. Они могут быть направлены в SOC для дальнейших действий.
ЗЕЛЕНЫЙ	Ограниченное распространение, только для сообщества. Источники могут использовать TLP: ЗЕЛЕНЫЙ, когда информация полезна для оповещения всех участвующих организаций, а также организаций с равным статусом в пределах более широкого сообщества или сектора. Получателям разрешается обмениваться информацией с маркировкой TLP: ЗЕЛЕНЫЙ с организациями с равным статусом и партнерами в пределах их сектора или сообщества, но не через публично доступные каналы. Информацию этой категории можно широко распространять в пределах конкретного сообщества. Не допускается раскрытие информации с маркировкой TLP: ЗЕЛЕНЫЙ за пределами данного сообщества.	Обмен результатами анализа вредоносного программного средства с конкретным отраслевым сектором

ЦВЕТ	ЗНАЧЕНИЕ	ПРИМЕР
БЕЛЫЙ	Раскрытие не ограничено. Источники могут использовать TLP: БЕЛЫЙ в соответствии с применяемыми правилами и порядком открытой публикации, когда в информации содержится минимальный или отсутствует предполагаемый риск злонамеренного использования. При условии соблюдения стандартных авторских прав информация с маркировкой TLP: БЕЛЫЙ может распространяться без ограничений.	Уведомление общественности о состоянии безопасности

— КОНЕЦ —