Инструктивный материал по политике в области кибербезопасности

Опубликовано с санкции Генерального секретаря

Январь 2022 г.

Международная организация гражданской авиации

1. Введение

Настоящий инструктивный материал соответствует Стратегии ИКАО в области авиационной кибербезопасности[1] и Плану действий по обеспечению кибербезопасности[2], в пункте действий ПДоК0.1 которого рекомендуется, чтобы Международная организация гражданской авиации (ИКАО) разработала типовую политику в области кибербезопасности, которой государства-члены и отрасль будут руководствоваться при разработке своей собственной национальной/внутренней политики.

Типовая политика в области кибербезопасности приведена в добавлении А к настоящему инструктивному материалу.

2. Сфера применения

Типовая политика в области кибербезопасности, изложенная в добавлении А настоящего документа, касается защиты и устойчивости критической инфраструктуры международной гражданской авиации перед лицом киберугроз и предусматривает необходимость в международном сотрудничестве в системе гражданской авиации, а также с местными ведомствами, например военными органами, органами по обеспечению кибербезопасности и национальной безопасности.

3. Цели

Типовая политика в области кибербезопасности призвана служить государствам и отрасли в качестве руководства, с тем чтобы они могли сосредоточить ресурсы и действия для достижения системного подхода к кибербезопасности в гражданской авиации, включая существующие и прежние системы. Конечная цель состоит в том, чтобы государства и заинтересованные стороны могли разработать подход, основанный на системе систем, который позволит защитить гражданскую авиацию от киберугроз и своевременно реагировать на киберинциденты и восстанавливаться после них, и тем самым противостоять новым угрозам без значительных нарушений деятельности.

Главными ожидаемыми результатами применения политики в области кибербезопасности являются:

3.1 Обеспечение защиты гражданской авиации от киберугроз

Защита гражданской авиации от киберугроз обеспечивается за счет внедрения Стандартов и Рекомендуемой практики, процедур и инструктивного материала ИКАО в области кибербезопасности. Это предусматривает внедрение эффективной практики управления рисками, определение критической инфраструктуры и применение целостного, многоуровневого подхода к кибербезопасности. Такой подход должен гарантировать, что успешная атака на один уровень не ставит под угрозу другие уровни системы и/или не приводит к потере функций, критически важных для обеспечения безопасности полетов, авиационной безопасности или непрерывности деятельности. Система должна также основываться на принципе непрерывного совершенствования для обеспечения координации, принятия и поддержания на должном уровне мер, необходимых для повышения функциональных возможностей, с учетом планируемых технических или процедурных нововведений.

---

[1] https://www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx
[2] Письмо государствам ИКАО 2020/114

3.2 **Обеспечение киберустойчивости гражданской авиации**

Киберустойчивая система гражданской авиации – это система, которая, подвергшись атаке, может сохранить свои критические функциональные возможности, т. е. обеспечить безопасное и надежное производство полетов с минимальными возможными перебоями. Такая 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 правоохранительными органами и военными полномочными органами.

3.3 **Обеспечение самоукрепления 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 по "встроенному" принципу на этапе разработки меняет парадигму безопасности с реагирующей на проактивную и способствует формированию самозащищенной системы гражданской авиации, тем самым создавая условия для ее развития и обеспечивая повышенную безопасность и устойчивость.

3.4 **Обеспечение координации авиационной кибербезопасности в системе гражданской авиации и с соответствующими неавиационными заинтересованными сторонами**

Для того чтобы обеспечить последовательный и взаимодополняющий подход к авиационной кибербезопасности по всем авиационным дисциплинам, система гражданской авиации должна гарантировать комплексное управление киберрисками для гражданской авиации путем координации аспектов авиационной кибербезопасности, касающихся безопасности полетов и авиационной безопасности. Кроме того, координация авиационной кибербезопасности должна выходить за рамки гражданской авиации и распространяться на другие соответствующие организации, такие как национальные, региональные, международные органы по обеспечению кибербезопасности, правоохранительные, военные органы и т. д.

4. **Элементы политики в области кибербезопасности**

В настоящем разделе содержится инструктивный материал по элементам, включенным в типовую политику в области кибербезопасности, приведенную в добавлении A. Поэтому рекомендуется читать этот материал вместе с типовой политикой в области кибербезопасности.

4.1 **Управление и организация**

4.1.1 Государства должны назначить соответствующий полномочный орган по авиационной кибербезопасности (ОА/Кибер), наделенный всеобъемлющими полномочиями и ответственностью за обеспечение авиационной кибербезопасности и киберустойчивости.

4.1.2 Нельзя рекомендовать универсальную схему с указанием конкретного подразделения в организационной структуре гражданской авиации отдельных государств, в состав которого войдет ОА/Кибер. На такое решение повлияют несколько соображений, относящихся к национальным авиационным и соответствующим неавиационным структурам в плане их организации и полномочий. Тем не менее весьма важно, чтобы ОА/Кибер были предоставлены требуемые ресурсы и полномочия, с тем чтобы он мог выполнять свой мандат, включая переговоры и координацию с соответствующими неавиационными заинтересованными сторонами.

4.1.3 В целом назначенный ОА/Кибер должен:

- определять при взаимодействии с национальным компетентным полномочным органом по кибербезопасности роль и функции каждого ведомства;
- руководить разработкой нормативных положений в области авиационной кибербезопасности;
- четко определять роль и ответственность различных секторов гражданской авиации в структуре национального компетентного ведомства гражданской авиации;
- координировать определение роли и ответственности органов гражданской авиации, находящихся под контролем национального компетентного ведомства гражданской авиации, в рамках национальных программ по обеспечению безопасности полетов и авиационной безопасности;
- определять элементы культуры кибербезопасности гражданской авиации и осуществлять мониторинг их внедрения;
- определять нормативные положения, процессы, требования и функции управления кризисными ситуациями в области кибербезопасности, включая требования к тестированию и периодичности;
- координировать комплексные вопросы авиационной кибербезопасности с соответствующими неавиационными заинтересованными сторонами, занятыми в обеспечении авиационной кибербезопасности, например вопросы обмена информацией и расследования инцидентов.

4.2 Управление рисками

4.2.1 Управление рисками для кибербезопасности должно опираться на системы управления рисками для безопасности полетов и авиационной безопасности, с тем чтобы разработать комплексную и точную оценку угроз и рисков для кибербезопасности и обеспечить разработку и внедрение эффективных мер по снижению рисков, которые учитывают требования к безопасности полетов и последствия таких мер для безопасности полетов и непрерывной деятельности гражданской авиации.

4.2.2 Все данные и системы следует всегда идентифицировать по их принадлежности. Идентификация и сохранение принадлежности создает подотчетность и обеспечивает управление данными и системами с их принятия до ликвидации. Таким образом, владельцы данных должны установить правила и процессы с включением физического местонахождения данных и систем, прав доступа, прав управления и требований к безопасности исходя из классификации данных и систем. Это в конечном счете обеспечит надлежащее использование данных и систем теми, для кого они предназначены, с разработкой и внедрением стандартов по контролю качества и с разрешением проблем и конфликтов.

4.3 Безопасность критических систем

4.3.1 Для защиты критических систем следует применять принципы глубокоэшелонированной защиты. Глубокоэшелонированная защита объединяет людей, технику и производственные мощности для создания меняющихся барьеров по многочисленным уровням и задачам организации[3]. Это такой подход к кибербезопасности, в котором для защиты критических систем, данных и информации применяется серия защитных механизмов, расположенных на различных уровнях.

[3] Специальная публикация NIST 800-53 Rev.5: https://doi.org/10.6028/NIST.SP.800-53r5

Такой многоуровневый подход с намеренной избыточностью повышает безопасность системы в целом и охватывает много различных векторов атаки[4].

4.3.2 ОА/Кибер должен обеспечить, чтобы организации гражданской авиации идентифицировали и надлежащим образом защищали свои критические системы, а также развивали способность обнаруживать киберинциденты, реагировать на них и восстанавливаться от их последствий.

4.4 Безопасность данных

4.4.1 Следует предусмотреть надежное автономное резервное копирование критических данных как инструмент обеспечения доступности и целостности информации. Однако чрезвычайно важно разработать эффективные нормативные правила резервного копирования данных в соответствии с оценками риска, поскольку автономное резервное копирование, проводимое в процессе кибератаки, уже будет поставлено под угрозу и поэтому не может быть использовано для восстановления допуска к критической информации.

4.4.2 Следует предусмотреть криптографическую защиту конфиденциальных данных как инструмент обеспечения конфиденциальности информации. Однако важно определить в соответствии с оценками риска порядок использования криптографической защиты, чтобы обеспечить надлежащий баланс между уровнем конфиденциальности и требованиями в отношении эксплуатационных характеристик, в особенности в части оперативных данных, необходимых для обеспечения безопасности полетов, а также с учетом ресурсов, требуемых для управления данными.

4.4.3 Следует установить порядок действий с целью обеспечить непрерывность критических функций в случае недоступности и/или потери целостности данных.

4.5 Безопасность цепи поставок

4.5.1 Организации должны гарантировать соответствие программного обеспечения и аппаратных средств, используемых в критических авиационных функциях, требованиям к кибербезопасности на протяжении жизненного цикла авиационных систем – от проектирования и разработки и в течение эксплуатации и технического обслуживания, вплоть до безопасной и надежной ликвидации.

4.5.2 Для включения требований к кибербезопасности в части аппаратных средств и программного обеспечения, а также в отношении обновления, модернизации и выпуска патчей в случае обнаружения уязвимостей, можно использовать соглашения об уровне обслуживания.

4.6 Физическая безопасность

4.6.1 Примеры мер физической защиты, относящихся к авиационной кибербезопасности, включают, помимо прочего, порядок регулирования и контролирования физического доступа, проверки анкетных данных персонала, обладающего административными правами в отношении систем/баз данных или правом доступа к конфиденциальным и/или критическим данным, рекомендации в отношении разделения обязанностей и/или ротации персонала с доступом к критическим системам или возможностью модифицировать эти системы и т. д.

---

[4] Глубоко эшелонированная защита обычно называется "за́мковым подходом", поскольку она повторяет многоуровневую защиту средневекового за́мка, когда, для того чтобы проникнуть в за́мок, нападающей стороне необходимо преодолеть ров, подъемный мост, крепостной вал, башни и т. д.

4.7 **Безопасность информационных и связных технологий (ICT)**

4.7.1 Примеры мер контроля за обеспечением безопасности ICT, относящихся к авиационной кибербезопасности, включают, помимо прочего, порядок контроля доступа и применения принципов минимальных привилегий, брандмауэры программного обеспечения/аппаратных средств и сетевую защиту, криптографию, использование кодов идентификации в организации, защиту конечной точки, сетевой мониторинг и обнаружение отклонений, разделение сетей, управление устройствами и т. д.

4.8 **Управление инцидентами и непрерывность критических функций**

4.8.1 ОА/Кибер должен определить правила, процессы, требования и функции для управления киберинцидентами, восстановления и непрерывного функционирования критических систем.

4.8.2 Для включения порядка ответных действий и восстановления после киберинцидентов следует использовать существующие планы управления кризисными ситуациями и обеспечения непрерывности производственной деятельности.

4.8.3 Следует периодически проводить испытания планов мероприятий на случай аварийной обстановки и обеспечения непрерывности деятельности в целях совершенствования планов, а также повышения возможностей реагирующих служб. В испытаниях должны участвовать все соответствующие заинтересованные стороны и они должны включать как теоретические учения (ТТХ), так и испытания а реальных условиях.

4.9 **Культура кибербезопасности**

4.9.1 Во всех авиационных организациях должна быть внедрена культура кибербезопасности.

4.9.2 Культура кибербезопасности должна быть одобрена руководством организации и должна включать программу, подлежащую выполнению всем персоналом.

4.9.3 Такая программа должна включать переподготовку в области кибербезопасности (включая принципы практики киберпрофилактики), осведомленность о последних угрозах, подготовку и тестирование (как в рамках подготовки, так и в виде реального моделирования атак) в целях оценки уровня киберосведомленности/профилактики.

4.9.4 Культура кибербезопасности должна включать элементы культуры безопасности полетов и авиационной безопасности, например предоставление данных на индивидуальной основе, сообщения о подозрительном поведении/практике, справедливую культуру и т. д.

— — — — — — — —

Добавление A

Типовая политика в области кибербезопасности

1. Введение

1.1 Настоящая политика в области кибербезопасности служит основой для дальнейшей разработки и реализации авиационной кибербезопасности. Ее следует опубликовать, направить соответствующим заинтересованным сторонам и периодически пересматривать.

1.2 В целях содействия внедрению настоящей политики в области кибербезопасности должен быть разработан дополнительный инструктивный материал.

2. Сфера применения

2.1 Авиационная кибербезопасность затрагивает вопросы обеспечения безопасности и устойчивости системы гражданской авиации, а также способствует сотрудничеству с соответствующими неавиационными организациями и ведомствами, включая, при необходимости, национальные органы по обеспечению кибербезопасности, национальной безопасности, правоохранительные и военные органы.

2.2 Обеспечение авиационной кибербезопасности координируется на национальном уровне с органами по обеспечению безопасности полетов, авиационной безопасности, защиты критической инфраструктуры, киберзащиты и с военными органами.

2.3 Обеспечение авиационной кибербезопасности координируется на международном уровне с эквивалентными иностранными надлежащими ведомствами, назначенными для обеспечения авиационной кибербезопасности.

3. Цели

3.1 Общие цели настоящей политики в области авиационной кибербезопасности заключаются в обеспечении безопасности, устойчивости и самоукрепления системы гражданской авиации перед лицом киберугроз и риска, а также в осуществлении координации в вопросах авиационной кибербезопасности с соответствующими национальными ведомствами и организациями.

4. Управление и организация

4.1 В соответствии с [ссылка на нормативные положения/законодательство, в силу которых производится данное назначение], [название организации] является соответствующим органом по авиационной кибербезопасности (ОА/Кибер) с общим мандатом на обеспечение авиационной кибербезопасности и киберустойчивости.

4.2 ОА/Кибер:

- взаимодействует с национальным компетентным органом по кибербезопасности с целью определить роль и обязанности каждого ведомства в области кибербезопасности гражданской авиации;
- координирует разработку нормативных положений в области авиационной кибербезопасности и участвует в ней;
- определяет, координирует требования в отношении кибербезопасности и оказывает поддержку соответствующим органам по безопасности полетов и авиационной

безопасности в деле включения этих требований, в том числе элементов надзора и контроля качества, в государственную программу по безопасности полетов (ГосПБП) и национальную программу безопасности гражданской авиации (НПБГА);

- определяет, поддерживает внедрение программ формирования культуры кибербезопасности всеми заинтересованными сторонами гражданской авиации и осуществляет мониторинг;
- определяет нормативные положения, процессы, требования и функции в части управления кризисными ситуациями в области кибербезопасности;
- координирует комплексные вопросы авиационной кибербезопасности с соответствующими неавиационными заинтересованными сторонами, занятыми в обеспечении авиационной кибербезопасности.

5. Управление рисками

5.1 Обеспечение кибербезопасности основывается на разведданных, факторах угрозы и на управлении рисками.

5.2 Управление рисками является неотъемлемой частью полного жизненного цикла систем.

5.3 Все данные и системы всегда имеют идентифицированную принадлежность.

6. Безопасность критических систем

6.1 Критические функции, системы и инфраструктура идентифицируются в ходе процессов управления рисками.

6.2 Для защиты критических систем применяется на этапе проектирования подход встроенной безопасности в сочетании с принципами глубокоэшелонированной защиты.

6.3 Избыточность критических систем считается инструментом обеспечения системной безопасности.

7. Безопасность данных

7.1 Данные и информация защищаются во время хранения и передачи в соответствии с их профилем конфиденциальности.

8. Безопасность цепи поставок

8.1 Сквозное управление цепью поставок программного обеспечения/аппаратных средств является частью управления авиационной кибербезопасностью.

8.2 Используемые в критических авиационных функциях программное обеспечение и аппаратные средства соответствуют требованиям к кибербезопасности на протяжении всего жизненного цикла авиационных систем.

9. Физическая безопасность

9.1 Физическая безопасность (включая безопасность персонала) является частью управления авиационной кибербезопасностью.

9.2 Физическая безопасность защищает людей, инфраструктуру, средства и службы, оборудование, материалы и документы от незаконного вмешательства, а также критические авиационные системы от несанкционированного физического доступа.

9.3 Физическая безопасность способствует управлению рисками за счет содействия идентификации носителей угрозы и/или выявления вероятности атак на критическую инфраструктуру гражданской авиации.

10. Безопасность информационных и связных технологий (ICT)

10.1 Безопасность ICT является частью управления авиационной кибербезопасностью.

10.2 Безопасность ICT определяет и принимает логические меры безопасности, а также способствует управлению киберинцидентами, восстановлению и осуществлению процессов непрерывности деятельности.

10.3 Безопасность ICT способствует управлению рисками за счет выявления уязвимостей, векторов атаки и мониторинга эволюции ландшафта угроз для авиационной кибербезопасности.

11. Управление инцидентами и непрерывность критических функций

11.1 Безопасность полетов и непрерывность критических функций являются основными движущими факторами в процессах управления инцидентами.

11.2 Испытания планов управления кризисной ситуацией и восстановления являются неотъемлемой частью управления инцидентами.

12. Культура кибербезопасности

12.1 План проведения образовательных мероприятий, повышения осведомленности, подготовки и учений является неотъемлемой частью управления авиационной кибербезопасностью.

12.2 Культура кибербезопасности полностью координируется с существующей культурой безопасности полетов и культурой авиационной безопасности.

12.3 Культура кибербезопасности обеспечивается эффективной внутренней и, по мере возможности, внешней практикой обмена информацией.

— КОНЕЦ —