ИКАО

Стратегическая цель “Авиационная безопасность и упрощение формальностей”

Стратегия в области авиационной кибербезопасности

Октябрь, 2019

Утверждено Генеральным секретарем и опубликовано с его санкции

МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ГРАЖДАНСКОЙ АВИАЦИИ

ИКАО

Стратегическая цель “Авиационная безопасность и упрощение формальностей”

Стратегия в области авиационной кибербезопасности

Октябрь, 2019

Утверждено Генеральным секретарем и опубликовано с его санкции

МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ГРАЖДАНСКОЙ АВИАЦИИ

Опубликовано онлайн отдельными изданиями на русском,
английском, арабском, испанском, китайском и французском языках
МЕЖДУНАРОДНОЙ ОРГАНИЗАЦИЕЙ ГРАЖДАНСКОЙ АВИАЦИИ.
999 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7

Информация о порядке оформления заказов и полный список агентов
по продаже и книготорговых фирм размещены на веб-сайте ИКАО www.icao.int.

Стратегия в области авиационной безопасности
https://www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx

СТРАТЕГИЯ В ОБЛАСТИ АВИАЦИОННОЙ КИБЕРБЕЗОПАСНОСТИ

КОНЦЕПТУАЛЬНОЕ ВИДЕНИЕ ГЛОБАЛЬНОЙ СТРАТЕГИИ АВИАЦИОННОЙ КИБЕРБЕЗОПАСНОСТИ

Сектор гражданской авиации все в большей степени зависит от наличия систем информационных и связных технологий, а также от целостности и конфиденциальности данных. Представляемая возможными киберинцидентами угроза для гражданской авиации постоянно изменяется, а носители такой угрозы вынашивают преступные намерения, ставя целью нарушение деловой активности и кражу информации по политическим, финансовым или другим мотивам.

Признавая многогранную и междисциплинарную природу кибербезопасности и отмечая, что кибератаки могут одновременно затрагивать широкий спектр областей и быстро распространяться, необходимо разработать общее концептуальное видение и определить глобальную стратегию кибербезопасности.

Концептуальное видение ИКАО глобальной кибербезопасности состоит в том, что авиационный сектор должен быть устойчив к кибератакам, сохраняя надежность и глобальное доверие к себе, продолжая при этом внедрять инновации и развиваться.

Это может быть достигнуто следующими действиями:

- признание государствами своих обязательств в рамках *Конвенции о международной гражданской авиации* (Чикагской конвенции) по обеспечению безопасности полетов, авиационной безопасности и непрерывности деятельности гражданской авиации с учетом кибербезопасности;

- согласование мер по обеспечению кибербезопасности между государственными органами в целях обеспечения эффективного и результативного управления факторами риска кибербезопасности;

- все заинтересованные стороны в сфере гражданской авиации берут на себя обязательства по дальнейшему развитию киберустойчивости и защите от кибератак, которые могут повлиять на безопасность полетов, авиационную безопасность и непрерывность деятельности системы воздушного транспорта.

Стратегия согласуется с другими инициативами ИКАО, связанными с обеспечением кибербезопасности, и координируется с соответствующими положениями по управлению безопасностью полетов и авиационной безопасностью. Цели стратегии будут достигаться посредством применения серии принципов, мер и действий, содержащихся в механизме, построенном на семи основополагающих элементах:

1. Международное сотрудничество

2. Управление

3. Эффективное законодательство и нормативные положения

4. Политика в области кибербезопасности

5. Обмен информацией

6. Планирование мероприятий на случай инцидентов и действий в чрезвычайных ситуациях

7. Наращивание потенциала, подготовка персонала и формирование культуры кибербезопасности

_____

1. МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО

1.1 В силу своей природы кибербезопасность и авиация не знают границ. Они в одинаковой степени требуют сотрудничества на национальном и международном уровне и требуют взаимного признания усилий по развитию, поддержанию и повышению кибербезопасности с целью защиты сектора гражданской авиации от всех киберугроз для безопасности полетов и авиационной безопасности.

1.2 Авиационная кибербезопасность должна быть согласована на глобальном, региональном и национальном уровнях в целях содействия глобальной упорядоченности и обеспечения полной функциональной совместимости мер защиты и систем управления факторами риска.

1.3 ИКАО является надлежащим всемирным форумом для привлечения государств к рассмотрению вопросов кибербезопасности в международной гражданской авиации. С этой целью ИКАО будет организовывать, поддерживать и способствовать проведению международных мероприятий, служащих платформой для обмена знаниями между государствами, международными организациями и отраслью. Государствам рекомендуется принимать участие в обсуждениях вопросов кибербезопасности в гражданской авиации.

2. УПРАВЛЕНИЕ

2.1 Всем государствам-членам ИКАО рекомендуется поддерживать и развивать стратегию авиационной кибербезопасности ИКАО для обеспечения безопасности полетов и авиационной безопасности гражданской авиации в мире, который подвергается все большему количеству киберугроз.

2.2 Государствам рекомендуется разработать четкие структуры национального управления и подотчетности в области авиационной кибербезопасности. Ведомствам гражданской авиации рекомендуется обеспечивать координацию со своим компетентным национальным органом в области кибербезопасности, признавая, что общая ответственность за обеспечение кибербезопасности во всех секторах может выходить за рамки ведомства гражданской авиации. Также необходимо установить соответствующие каналы координации деятельности различных государственных органов и заинтересованных сторон от отрасли.

2.3 Кроме того, государствам-членам рекомендуется включать кибербезопасность в свои национальные программы обеспечения безопасности полетов и авиационной безопасности. С этой целью ИКАО следует также включить вопросы кибербезопасности в региональные и глобальные планы и работать над общими исходными параметрами для Стандартов и Рекомендуемой практики в области кибербезопасности (SARPS).

3. ЭФФЕКТИВНОЕ ЗАКОНОДАТЕЛЬСТВО И НОРМАТИВНЫЕ ПОЛОЖЕНИЯ

3.1 *Основной целью международного, регионального и национального законодательства и* нормативных положений о кибербезопасности для гражданской авиации является оказание поддержки в осуществлении комплексной стратегии кибербезопасности для защиты гражданской авиации и пассажиров от последствий кибератак.

3.2 Руководствуясь положениями ИКАО, государства-члены должны разработать и применять соответствующее законодательство и нормативные положения до реализации своей национальной политики в области кибербезопасности для гражданской авиации. Необходимо продолжать разработку соответствующего инструктивного материала для государств и отрасли, связанного с выполнением положений по кибербезопасности. С этой целью ИКАО обязуется разрабатывать, пересматривать и по необходимости

изменять инструктивный материал, связанный с включением аспектов кибербезопасности в меры по обеспечению безопасности полетов и авиационной безопасности.

3.3 Следует проанализировать соответствующие документы международного права, чтобы выявить существующие или отсутствующие ключевые правовые положения в воздушном праве, связанные с предотвращением, преследованием в судебном порядке и своевременным реагированием на киберинциденты, чтобы сформировать основу для последовательного и упорядоченного применения законодательства и нормативных положений в области кибербезопасности во всем мировом авиационном секторе. Тем временем государствам предлагается ратифицировать документы ИКАО, в том числе *Конвенцию о борьбе с незаконными актами в отношении международной гражданской авиации* (Пекинскую конвенцию) и *Протокол, дополняющий Конвенцию о борьбе с незаконным захватом воздушных судов* (Пекинский протокол).

3.4 Государствам рекомендуется рассмотреть вопрос о необходимости обновления их национального законодательства или принятия нового национального законодательства, обеспечивающего преследование в судебном порядке связанных с терроризмом киберугроз, а также кибератак, имеющих отрицательные последствия для гражданской авиации. Одновременно государствам предлагается создать соответствующие механизмы для сотрудничества с "добросовестными" исследованиями в области безопасности, представляющих собой исследовательскую деятельность, которая осуществляется в условиях, позволяющих избегать последствий для безопасности полетов, авиационной безопасности и непрерывности деятельности гражданской авиации.

4. ПОЛИТИКА КИБЕРБЕЗОПАСНОСТИ

4.1 Кибербезопасность должна быть включена в государственные системы контроля над обеспечением авиационной безопасности и безопасности полетов как часть комплексной системы управления факторами риска.

4.2 Признавая существование различных методик оценки факторов риска, следует отдавать приоритет возможной разработке и изменениям инструктивного материала, связанного с оценками угроз кибербезопасности и факторов риска, чтобы достичь сопоставимости результатов таких оценок.

4.3 В секторе гражданской авиации политика кибербезопасности может охватывать весь жизненный цикл авиационной системы и включать следующие элементы: культура кибербезопасности, популяризация безопасных конструкторских решений, безопасность цепочек поставок для программного и аппаратного обеспечения, целостность данных, надлежащий контроль доступа, упреждающее управление уязвимостями, повышение гибкости процесса обновления систем безопасности без ущерба безопасности полетов, а также включение систем и процессов мониторинга данных, относящихся к кибербезопасности.

5. ОБМЕН ИНФОРМАЦИЕЙ

5.1 Поскольку сектор гражданской авиации - это глобальная, взаимозависимая система, охватывающая множество общих систем, кибератаки могут легко распространяться и приводить к глобальным последствиям. Задачами обмена информацией являются предотвращение, раннее обнаружение и смягчение воздействия соответствующих событий в сфере кибербезопасности до того, как они приведут к более широким последствиям для безопасности полетов или авиационной безопасности. Культура обмена информацией, доказавшая свою значимость для безопасности полетов и авиационной безопасности, значительно снизит уровень системного киберриска в авиационном секторе.

5.2 Обмен информацией по таким аспектам, как уязвимости, угрозы, события и передовая практика, осуществляемый в рамках налаженных и доверительных отношений, способен снизить воздействие

постоянных атак. В соответствии с существующими положениями ИКАО должны быть признаны надлежащие механизмы обмена информацией.

6. ПЛАНИРОВАНИЕ МЕРОПРИЯТИЙ НА СЛУЧАЙ ИНЦИДЕНТОВ И ДЕЙСТВИЙ В ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ

6.1 В соответствии с существующими механизмами управления инцидентами существует потребность в наличии надлежащих и масштабируемых планов, обеспечивающих непрерывность деятельности воздушного транспорта во время киберинцидентов. Государствам и авиационному сектору рекомендуется применять уже разработанные планы действий в чрезвычайных ситуациях и внести в них поправки, включив положения о кибербезопасности.

6.2 Учения в области кибербезопасности являются полезным инструментом для проверки существующей киберустойчивости и поиска улучшений, поэтому настоятельно рекомендуется их проведение. Такие учения могут иметь разные формы (например, штабные учения, моделирование ситуаций или учения в реальном времени) и разные уровни (международный, национальный, организационный).

7. НАРАЩИВАНИЕ ПОТЕНЦИАЛА, ПОДГОТОВКА ПЕРСОНАЛА И ФОРМИРОВАНИЕ КУЛЬТУРЫ КИБЕРБЕЗОПАСНОСТИ

7.1 Человеческий элемент заложен в саму основу кибербезопасности. Для сектора гражданской авиации чрезвычайно важно предпринять ощутимые шаги по увеличению количества квалифицированного персонала, обладающего экспертными знаниями в области авиации и кибербезопасности. Это может быть сделано повышением осведомленности о кибербезопасности, а также образованием, наймом и подготовкой. Учебные планы по кибербезопасности и, если это практически возможно, по авиационной кибербезопасности на всех уровнях должны быть включены в структуру национального образования, а также в соответствующие международные программы подготовки. Следует искать инновационные решения для совмещения и перекрестного взаимодействия традиционных информационных технологий, киберпрофессий и специалистов, имеющих отношение к авиации.

7.2 Поддержка и стимулирование развития навыков существующей и новой рабочей силы должны способствовать инновациям в области кибербезопасности и соответствующим научным исследованиям и разработкам в авиационном секторе. Для поддержки персонала в выполнении его повседневных обязанностей должна постоянно проводиться соответствующая профессиональная подготовка.

7.3 Кибербезопасность может быть включена в стратегию следующего поколения авиационных специалистов, поскольку ИКАО лучше всего подходит для сотрудничества с государствами и отраслью в разработке требований к компетентности авиационных специалистов, исходя из их повседневных ролей.

7.4 Сектору гражданской авиации удалось достичь завидного уровня безопасности полетов, который основан на культуре упреждающих мер обеспечения безопасности полетов, являющихся обязанностью каждого. Принципы этой культуры безопасности полетов должны применяться в разработке и поддержании культуры кибербезопасности во всем авиационном секторе.

— КОНЕЦ —