МЕЖДУНАРОДНОЕ ТРАНСПОРТНОЕ ПРАВО

УДК 629.7

Альбиков Илдар Ростямович,
кандидат юридических наук, доцент,
Ульяновский институт гражданской авиации
имени Главного маршала авиации Б. П. Бугаева

Бойко Наталия Семеновна,
кандидат юридических наук, доктор исторических наук, доцент,
Ульяновский институт гражданской авиации
имени Главного маршала авиации Б. П. Бугаева

План действий по обеспечению кибербезопасности: создание надежного глобального механизма авиационной безопасности

Аннотация. Статья подробно обрисовывает план, направленный на реализацию стратегии кибербезопасности, предложенной ИКАО для авиационной отрасли. Этот план включает в себя четко определенные стратегии, разработанные с целью обеспечить безопасность в киберпространстве авиационной сферы. Это включает в себя оценку существующих мероприятий, проведенных в различных частях мира, и прогресса в области кибербезопасности. Основное внимание уделяется анализу текущей ситуации в сфере кибербезопасности в авиации, включая выявление уязвимостей, успешно реализованных мер по предотвращению киберугроз, а также внедрению современных технологий для защиты информации.

Ключевые слова: информационная безопасность; инцидент; кибербезопасность; кибератака; киберугроза; обмен информацией; политика в области кибербезопасности; событие; уязвимость; безопасность полетов; авиационная безопасность.

Ildar R. Al’bikov,
Candidate of Law, associate professor,
Ulyanovsk Civil Aviation Institute

Nataliya S. Boyko,
Candidate of Law, Doctor of Historical Sciences, associate professor,
Ulyanovsk Civil Aviation Institute

Cybersecurity action plan: building a robust global aviation security mechanism

Abstract. The current paper has presented a plan to implement the ICAO cybersecurity strategy for the aviation industry. This plan includes clearly defined strategies designed to enforce aviation security in cyberspace. This plan includes an estimation of existing activities carried out in different parts of the world and progress in the field of cybersecurity. Special attention has been paid to analyzing the current situation in the field of cybersecurity in aviation, including identifying vulnerabilities, successfully implemented measures to prevent cyber threats, as well as the introduction of modern technologies to protect information.

Keywords: information security; incident; cybersecurity; cyber-attack; cyber threat; information exchange; cybersecurity policy; event; vulnerability; flight safety; aviation security.

В контексте современной гражданской авиации прогнозируется стабильный рост объема воздушных перевозок. Технический прогресс оказывает глубокое влияние на работу гражданской авиации, повышая ее уязвимость для киберугроз. Злонамеренная деятельность в киберпространстве может нанести ущерб гражданской авиации — от незначительных неполадок в работе оборудования до катастрофических последствий. Риски постоянно возрастают, и становится очевидно, что необходим надежный механизм обеспечения кибербезопасности на международном, региональном и государственном уровнях. Создание надежной системы безопасности в киберпространстве, основанной на тесном сотрудничестве между правительствами, авиационной индустрией и Международной организацией гражданской авиации (ИКАО), способствует повышению общей осведомленности в вопросах кибербезопасности, что, в свою очередь, приведет к более безопасным и надежным авиационным системам. Таким образом, кибербезопасность в гражданской авиации становится все более важной в связи с ростом киберугроз. Авиаотрасль особенно уязвима из-за функциональной и цифровой взаимозависимости компонентов и отсутствия эффективных механизмов защиты от кибератак.

На 39-й сессии Ассамблеи Международной организации гражданской авиации ИКАО подчеркнула значимость и неотложность защиты ключевых авиационных инфраструктур от кибератак, необходимость глобального обязательства со стороны ИКАО, ее стран-участниц и заинтересованных в авиации сторон по решению проблем кибербезопасности в области информационной безопасности и устранению угроз и рисков в авиационной сфере. Принятая резолюция A39-19 «Решение проблем кибербезопасности в гражданской авиации»

указывает на действия, которые должны быть предприняты государствами и другими заинтересованными сторонами для обеспечения кибербезопасности в авиации. Кроме того, Ассамблея поручила ИКАО создать всеобъемлющий план кибербезопасности. Для выполнения этой задачи Исследовательская группа ИКАО по кибербезопасности разработала стратегию кибербезопасности для авиационной отрасли. На следующей 40-й сессии Ассамблея приняла обновленную резолюцию A40-10 «Решение проблем кибербезопасности в гражданской авиации», призывающую страны к действиям по обеспечению кибербезопасности в авиационной инфраструктуре [URL: https://www.icao.int/aviationcybersecurity/Pages/Cybersecurity-Action-Plan.aspx (дата обращения: 26 ноября 2023 г.)].

Совершенствование надзора и контроля за обеспечением безопасности полетов и авиационной безопасностью признаны ИКАО основным принципом глобальной стратегии повышения уровня безопасности гражданской авиации [https://mlgvs.ru/saf.html]. Роль кибербезопасности в устойчивости бизнеса и государства становится все более значимой, и потребность в результативной безопасности оказывается одной из ключевых идей для достижения высокого уровня защищенности. Сейчас на рынке повышается потребность в измеримой кибербезопасности, направленной на достижение гарантированного результата — невозможности реализации кибератак с недопустимыми последствиями [https://www.ptsecurity.com/ru-ru/research/analytics/new-cybersecurity-from-process-to-result/].

ИКАО постоянно адаптирует свою работу в соответствии с постоянно меняющейся глобальной картиной угроз. Это соответствует резолюциям Совета Безопасности ООН, которые возлагают на государства ответственность за обеспечение безопасности воздушного движения на своей территории и призывают все государства сотрудничать с ИКАО для обеспечения того, чтобы в соответствии с Чикагской конвенцией о международной гражданской авиации 1944 г. международные стандарты безопасности анализировались, обновлялись и применялись с учетом текущих рисков. Так как угрозы кибербезопасности для гражданской авиации меняются и их масштаб, вероятно, будет расти, ИКАО принимает меры для создания эффективных механизмов смягчения и снижения рисков для критически важной авиационной инфраструктуры, связанных с незаконными вмешательствами через киберпространство и любыми событиями, которые могут повлиять на безопасность полетов, в соответствии с положением резолюции 2341 (2017) Совета Безопасности ООН. В связи с этим 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.

План действий по обеспечению кибербезопасности нацелен на достижение результатов, обозначенных для каждого из семи ключевых компонентов стратегии кибербезопасности, а также на создание эффективной системы обеспечения кибербезопасности в гражданской авиации. Принципы Плана действий включают: признание государствами-членами ответственности за кибербезопасность в соответствии с Чикагской конвенцией для обеспечения безопасности полетов и авиационной безопасности; координацию государствами-членами мер по авиационной кибербезопасности в целях эффективного и действенного глобального управления авиационной кибербезопасностью; обязательства всех участников системы гражданской авиации развивать устойчивость к киберугрозам для защиты от кибератак, исходящих от любых источников угроз, способных негативно повлиять на безопасность полетов, авиационную безопасность или функционирование авиатранспортной системы. Меры, касающиеся киберугроз, подразумевают, что каждое Договаривающееся государство обязано обеспечивать защиту критически важных систем информационных и связных технологий, используемых в гражданской авиации, в соответствии с национальными программами безопасности [Приложение 17 к Чикагской конвенции].

Существует набор принципов, мер и действий, предложенных для достижения целей семи ключевых элементов стратегии авиационной кибербезопасности: международное сотрудничество, управление, действенное законодательство и нормативные положения, политика в области кибербезопасности, обмен информацией, управление инцидентами и планирование мероприятий на случай аварийной обстановки, наращивание потенциала, подготовка персонала и культура кибербезопасности.

Международное сотрудничество подразумевает под собой развитие сотрудничества между всеми участниками на национальном и международном уровнях для защиты гражданской авиации; признание усилия по обеспечению кибербезопасности на взаимной основе; стремление к гармонизации регуляторных норм на глобальном, региональном и национальном уровнях для согласования действий и обеспечения совместимости защитных мер; привлечение государства к решению вопросов кибербезопасности международной гражданской авиации; поддерживание проведения международных мероприятий в этой области и признание общей ответственности за обеспечение кибербезопасности во всех сегментах глобальной системы гражданской авиации.

Управление включает в себя: рекомендации и развитие стратегии кибербезопасности ИКАО, национальные процессы управления и подотчетности в области кибербезопасности гражданской авиации, координацию между государственными ведомствами и национальными

органами по кибербезопасности, установку эффективных каналов координации, включение вопросов кибербезопасности в национальные и глобальные планы, а также разработку общего базового уровня для стандартов и рекомендуемой практики.

Действенное законодательство и нормативные положения направлены на обеспечение эффективного предотвращения киберинцидентов и судебного преследования их виновников. Задачи включают анализ и при необходимости обновление национального законодательства по предотвращению и расследованию кибератак, воздействующих на безопасность гражданской авиации. Необходимы также внедрение соответствующих национальных нормативов в области кибербезопасности и разработка рекомендаций для государств и отрасли по внедрению мер по обеспечению кибербезопасности гражданской авиации.

Политика кибербезопасности нацелена на интеграцию ее в системы безопасности и управления рисками в гражданской авиации. Задачи включают обеспечение согласованности методов оценки риска в кибербезопасности и разработку политики, учитывающей жизненный цикл авиационных систем.

Для эффективного обмена информацией необходимо использовать платформы, соответствующие стандартам ИКАО, для предотвращения, обнаружения и смягчения последствий киберсобытий. Также важно информировать компетентные органы о киберинцидентах и уязвимостях, представляющих риск для безопасности полетов и авиационной безопасности.

Управление инцидентами и планирование мероприятий на случай киберинцидентов включает разработку планов реагирования на инциденты и восстановления после них, поощрение использования существующих планов и проведение регулярных учений.

Наращивание потенциала, подготовка персонала и культура кибербезопасности включают обеспечение квалификации персонала, повышение осведомленности о кибербезопасности, включение учебных программ по авиационной кибербезопасности в образовательную структуру и включение вопросов кибербезопасности в стратегию подготовки специалистов.

План предназначен для ИКАО и других заинтересованных сторон, включая государства и отрасль. Это поможет организациям сосредоточиться на эффективных мерах по созданию надежного глобального механизма авиационной кибербезопасности. ИКАО планирует пересматривать план по мере необходимости и предоставлять информацию о выполнении задач и соблюдении сроков. Будут указаны области, требующие помощи от государств и в развитии потенциала. Все заинтересованные стороны должны участвовать в мероприятиях по повышению кибербезопасности в гражданской авиации. План включает

общие рамки участия и определяет действия для ИКАО, государств и отрасли. ИКАО играет важную роль в контроле и координации реализации плана, включая обновление плана и стандартов. ИКАО разрабатывает и обновляет список инициатив в сфере кибербезопасности. Список содержит существующие инициативы по авиационной безопасности, а также другие инициативы, связанные с кибербезопасностью в транспортной сфере и других секторах. Государства и представители отрасли должны следовать определенным принципам и применять соответствующие инструменты и системы для управления информационными технологиями и коммуникационными системами. ИКАО поддерживает разработку международного механизма авиационного доверия для управления данными и обеспечения интероперабельности. Политики и процедуры должны быть как можно более универсальными и применяться всеми заинтересованными сторонами для повышения интероперабельности мер по управлению кибербезопасностью. ИКАО должна уделить особое внимание согласованию авиационной терминологии, особенно в контексте комплексного управления рисками. Важно различать авиационную безопасность, которая имеет дело с незаконными и преднамеренными действиями, и безопасность полетов, которая имеет дело со случайными и непреднамеренными угрозами. Комплексное управление рисками может охватывать как авиационную безопасность, так и безопасность полетов. ИКАО должна сотрудничать с другими организациями для обмена информацией о рисках кибербезопасности. Это поможет понять, как риски могут распространяться на другие организации и как их можно устранить. Важно заключать соглашения с внешними поставщиками для обмена конфиденциальной информацией о кибербезопасности.

ИКАО должна создать систему управления кибербезопасностью гражданской авиации. Государствам следует разработать свои собственные структуры управления и определить роли и обязанности всех участников на национальном уровне. Необходимо согласовать План действий по обеспечению кибербезопасности с существующими Глобальным планом обеспечения авиационной безопасности, Глобальным аэронавигационным планом и Глобальным планом обеспечения безопасности полетов и включить туда аспекты кибербезопасности. ИКАО проанализирует существующие документы международного воздушного законодательства на предмет пробелов в отношении киберрисков. Может потребоваться разработка новых положений в дополнение к существующим правилам и стандартам. Это должно быть сделано на индивидуальной основе и при необходимости должно быть согласовано со всеми заинтересованными сторонами. Государствам рекомендовано ратифицировать Конвенцию о борьбе с незаконным захватом воздушных судов, заключенную в Гааге в 1970 г., измененную Пекинским протоколом 2010 г., и принять законодательство в области кибербезопасности

гражданской авиации для устранения пробелов. Также важно внедрить механизм правоприменения для судебного преследования за незаконные действия в киберпространстве.

Необходимо разработать национальную и организационную политику кибербезопасности, включающую цели, обязательства, управление с внешними сторонами, постоянное совершенствование механизма обеспечения, документирование и распространение политики. Проблема оценки риска в киберсреде требует предвидения быстрых изменений угроз. Предвидение важно для адаптации стратегии защиты гражданской авиации, особенно в условиях асимметрии между нарушителями и защитниками. Рекомендуется разработать механизм идентификации и оценки рисков, учитывая потенциальные последствия атак на авиацию, используя матрицы киберриска; рассмотреть схему обмена информацией в авиации для понимания взаимодействия заинтересованных сторон и их зависимости от рисков; адаптировать меры реагирования мировой авиации на меняющиеся риски; координировать деятельность по выявлению и оценке рисков группой экспертов в области кибербезопасности гражданской авиации, приоритетно с опытом в этой области. Группа должна формулировать заявление о глобальном контексте риска в кибербезопасности.

Обмен информацией важен для управления кибербезопасностью в гражданской авиации. Заинтересованным сторонам рекомендуется создать программы обмена, способствующие партнерствам и обеспечивающие обмен информацией внутри и между организациями. Программы должны адаптироваться к киберугрозам, обеспечивая ситуационную осведомленность и эффективное управление рисками. Обмен киберинформацией должен быть двусторонним и многосторонним на разных уровнях — от национального до глобального. Типы информации включают киберразведданные, показатели компрометации, тактики, методы, уязвимости и донесения об инцидентах. Необходимо учитывать различия в национальном законодательстве и характере киберинформации при организации обмена. Использование протокола «Светофор» рекомендуется для регулирования уровней распространения и ограничений. При распространении киберинформации важно удалять конфиденциальные данные. Для ответственного раскрытия уязвимостей следует разработать принципы и инструкции, включая образовательные компоненты. Отсутствие единообразия в распределении ответственности за кибербезопасность требует назначения единого координатора для создания эффективных каналов связи. Системы обмена информацией должны быть глобальными, региональными и национальными, способствуя культуре кибербезопасности. Форумы обмена информацией должны поддерживать обмен между государственными и частными структурами. Участие в доверенных сообществах поможет содействовать обмену передовым опытом и информацией об угрозах.

Заинтересованным сторонам рекомендуется разработать и испытать планы реагирования на киберинциденты в гражданской авиации. Это включает в себя адаптацию существующих планов на случай непредвиденных обстоятельств, обеспечение масштабируемости и безопасности полетов в условиях киберугроз, а также разработку механизмов реагирования и восстановления. Важно привлекать военные авиационные органы к планированию и обеспечивать эффективность и минимальные уровни обслуживания. Также необходимо классифицировать донесения о киберинцидентах, координировать их представление на разных уровнях и проводить учения для проверки планов реагирования. Заинтересованным сторонам следует разработать механизмы обнаружения и анализа инцидентов, следить за кибербезопасностью систем и внедрять планы реагирования при необходимости. Предлагается создание подразделения по координации кризисных ситуаций в гражданской авиации, включая экспертов по кибербезопасности, и регулярное проведение учений с участием всех заинтересованных сторон.

Необходимо активно развивать образование, подготовку персонала и повышение осведомленности в кибербезопасности гражданской авиации на мировом, региональном и национальном уровнях. Культуру кибербезопасности следует внедрять в организации гражданской авиации, начиная с высшего руководства. Образовательные мероприятия должны охватывать широкий спектр тем, включая принципы безопасности на этапе разработки, координацию интересов сторон, профилактику кибератак, и поддерживать понятие «справедливой культуры» для стимулирования донесений о непреднамеренных инцидентах. Продвижение культуры кибербезопасности и образовательных программ должно способствовать взаимному пониманию и укреплению доверия в сообществах, ответственных за безопасность полетов и авиационную безопасность.

Важно также поощрять транснациональные программы обмена в области кибербезопасности. Эти инициативы должны акцентировать внимание не только на функционировании систем, но и на их полном жизненном цикле, включая требования, проектирование, разработку, изготовление, эксплуатацию, техническое обслуживание и ликвидацию.

Таким образом, План действий по кибербезопасности объединяет усилия ИКАО, государств, авиационной отрасли и других заинтересованных сторон для применения комплексного и координированного подхода к решению текущих и будущих проблем в этой области. Кибербезопасность рассматривается как общая проблема для всех секторов авиации. План поддерживает стратегию ИКАО в области авиационной кибербезопасности и направлен на создание надежной глобальной системы кибербезопасности.