Международная организация гражданской авиации

A41-WP/231[1]
EX/104
2/8/22

РАБОЧИЙ ДОКУМЕНТ

АССАМБЛЕЯ — 41-Я СЕССИЯ

ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ

Пункт 14 повестки дня. Авиационная безопасность. Политика

СТРАТЕГИЯ КУЛЬТУРЫ КИБЕРБЕЗОПАСНОСТИ

(Представлено Саудовской Аравией от имени государств – членов Арабской организации гражданской авиации (АСАО)[2])

КРАТКАЯ СПРАВКА

В секторе гражданской авиации наблюдается постоянный рост кибератак, что, в свою очередь, влияет на деятельность аэродромов, авиакомпаний, на воздушное движение, а также на пассажиров. Наилучшим способом минимизации киберрисков является разработка стратегии культуры кибербезопасности, направленной на повышение кадрового потенциала, продвижение целей кибербезопасности и защиту организаций от внутренних и внешних киберугроз. Стратегия культуры кибербезопасности призвана сыграть важнейшую роль в соблюдении требований кибербезопасности и укреплении сотрудничества на корпоративном, национальном и международном уровнях. Стратегия культуры кибербезопасности должна охватывать весь персонал любой организации, поскольку ее целью является создание и поддержание культуры кибербезопасности для оказания содействия людям, применению технологий и деятельности по обеспечению кибербезопасности.

Действия: Ассамблее предлагается:

a) настоятельно призвать государства-члены принять стратегию культуры кибербезопасности в гражданской авиации в свете значительного увеличения числа кибератак по всему миру;

b) призвать ИКАО разработать для персонала гражданской авиации программу повышения осведомленности о кибербезопасности параллельно с программой повышения культуры авиационной безопасности.

Стратегические цели	Данный рабочий документ связан со стратегической целью *"Авиационная безопасность и упрощение формальностей"*
Финансовые последствия	
Справочный материал	

[1] *Версия на арабском языке представлена Саудовской Аравией.*

[2] *Государства – члены Арабской организации гражданской авиации (АСАО): Алжир, Бахрейн, Джибути, Египет, Иордания, Ирак, Йемен, Катар, Коморские Острова, Кувейт, Ливан, Ливия, Мавритания, Марокко, Объединенные Арабские Эмираты, Оман, Палестина, Саудовская Аравия, Сирийская Арабская Республика, Сомали, Судан, Тунис.*

1. ВВЕДЕНИЕ

1.1 Основной причиной кибератак и нарушений кибербезопасности в 2021 году были названы человеческие ошибки, что свидетельствует о том, что самым слабым звеном в цепочке кибербезопасности является персонал. Кроме того, киберпреступники стали осуществлять атаки, нацеленные на пользователей системы, чтобы использовать их уязвимости. Соответственно, организации должны разработать стратегии культуры кибербезопасности, чтобы обеспечить своим сотрудникам возможность должным образом справиться с широким спектром киберугроз, нацеленных на них или их рабочие места. В этом смысле, они становятся первой линией обороны своих организаций.

1.2 Люди, процессы и технологии составляют три основных столпа кибербезопасности. Эти три столпа изначально зависят от развитой культуры кибербезопасности, поскольку технологии без надлежащего обучения персонала будут создавать уязвимости. Процессы сами по себе также неэффективны, если они не реализуются персоналом должным образом.

1.3 Человеческая ошибка не ограничивается только переходом пользователей по подозрительным ссылкам или загрузкой вредоносных программ. Наиболее значительный риск возникает из-за того, что неквалифицированные разработчики систем допускают ошибку при конфигурировании или настройке какой-либо критически важной системы или не соблюдают процедуры управления изменениями при вводе изменений в систему, тем самым подвергая всю техническую инфраструктуру внешним киберугрозам.

1.4 Все сотрудники должны осознавать свои роли и обязанности в применении принципов корпоративной программы кибербезопасности. Они также должны понимать свои обязательства в соответствии с политикой кибербезопасности и любым национальным уголовным законодательством, охватывающим деятельность в киберпространстве.

1.5 Высшее руководство и члены совета директоров играют решающую роль в продвижении требований кибербезопасности и устранении киберрисков. В этом своем качестве они должны осознавать важность кибербезопасности и относиться к киберрискам как к рискам организационного уровня.

2. КУЛЬТУРА КИБЕРБЕЗОПАСНОСТИ

2.1 Культура кибербезопасности способствует обмену информацией между государствами-членами в целях активного выявления и устранения киберуязвимостей и угроз.

2.2 Эффективные изменения начинаются с повышения осведомленности и обучения в области кибербезопасности. Поэтому организациям следует предпринять дополнительные шаги для реализации поведенческих изменений путем внедрения культуры кибербезопасности.

2.3 Культура кибербезопасности включает в себя следующие три этапа:

a) *Определение стратегических целей:* определение целей культуры кибербезопасности является первым шагом в процессе ее реализации. Такие цели могут включать, в частности, обеспечение полного понимания персоналом рисков кибербезопасности для организации и осознание своих соответствующих роли и обязанностей, а также повышение уровня знаний и компетенций в области кибербезопасности.

b) *Оценка существующей ситуации:* цель состоит в том, чтобы оценить существующую культуру на корпоративном и индивидуальном уровнях. Корпоративный уровень отражает управление со стороны организации и поощрение надлежащего поведения. Это может включать политику и процедуры, политику приемлемого использования, роли и обязанности, осведомленность и обучение, организационную структуру, структуры кибербезопасности, отчеты об инцидентах и документацию комитета по кибербезопасности. С другой стороны, индивидуальный уровень предполагает исследует осведомленность персонала о кибербезопасности с помощью обучающих платформ или симуляций кибератак. При отсутствии необходимых технологий может быть разработан и распространен опросный лист для сбора необходимой информации.

c) *Разработка программы:* заключительным шагом является определение расхождения между текущей и желаемой ситуациями и выработка программы для реализации ранее определенных стратегических целей.

— КОНЕЦ—