Международная организация гражданской авиации

AN-Conf/14-WP/113[1]
28/6/24

РАБОЧИЙ ДОКУМЕНТ

ЧЕТЫРНАДЦАТАЯ АЭРОНАВИГАЦИОННАЯ КОНФЕРЕНЦИЯ

Монреаль, Канада, 26 августа – 6 сентября 2024 года

Пункт 4 повестки дня. Гиперсвязность аэронавигационной системы
4.2. Кибербезопасность и устойчивость информационных систем

УПРАВЛЕНИЕ РИСКОМ И СОСТАВЛЕНИЕ РЕЕСТРА ИНФОРМАЦИОННЫХ КИБЕРАКТИВОВ В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В ОБЛАСТИ АЭРОНАВИГАЦИОННОГО ОБСЛУЖИВАНИЯ (ANS)

(Представлено Чили при поддержке 20 государств – членов Латиноамериканской комиссии гражданской авиации (ЛАКГА)[2])

КРАТКАЯ СПРАВКА

В настоящем документе представлены общие рекомендации по обеспечению кибербезопасности, подлежащие рассмотрению аэронавигационными службами (ANS) в целях противодействия современным угрозам для используемых в этой области технологических систем. В условиях постоянного обмена информацией такие системы становятся потенциальными объектами для кибератак.

Эти обстоятельства обусловлены функциональной структурой авиационной системы, включающей полномочные органы гражданской авиации, поставщиков аэронавигационного обслуживания (ПАНО), эксплуатантов аэропортов и любые другие соответствующие организации.

Действия: Конференции предлагается:

a) содействовать разработке плана управления риском в области ANS, позволяющего выявлять и устранять любые угрозы для кибербезопасности при проектировании, установке и эксплуатации необходимых сетей и систем;

b) содействовать разработке функциональных элементов, способствующих управлению риском и позволяющих при необходимости выявлять угрозы с указанием уровней приоритетности действий, проводить техническое обслуживание и обеспечивать быстрое восстановление системы, таких как отдельный комплексный реестр для каждого киберактива в области ANS;

c) вновь подтвердить обязательство по постоянному усовершенствованию различных процессов, в том числе тех, которые указаны как критически важные, с целью достижения оптимального уровня кибербезопасности в области ANS.

[1] Текст на испанском языке представлен Чили.

[2] Аргентина, Аруба, Белиз, Бразилия, Венесуэла (Боливарианская Республика), Гватемала, Гондурас, Доминиканская Республика, Колумбия, Коста-Рика, Куба, Мексика, Никарагуа, Панама, Парагвай, Перу, Сальвадор, Уругвай, Эквадор и Ямайка.

1. ВВЕДЕНИЕ

1.1 Технологические изменения, осуществляемые в различных публичных организациях, приводят к тому, что эти организации становятся все более подвержены киберпреступлениям. Предоставление аэронавигационного обслуживания (ANS) также не застраховано от этой проблемы, поэтому возникает необходимость в разработке стратегий и установлении барьеров для защиты от этой скрытой, растущей угрозы, которая потенциально может повлиять на оптимальные уровни эксплуатационной безопасности.

1.2 Необходимость разработки методов управления риском для выявления и уменьшения любых угроз для кибербезопасности системы ANS требует новых усилий по обеспечению постоянного усовершенствования различных процессов, включая те, которые определены организацией как критически важные.

1.3 Политика в области кибербезопасности, разработанная службами ANS, должна учитывать весь жизненный цикл авиационной системы и включать такие элементы, как культура кибербезопасности, повышение уровня безопасности при проектировании, обеспечение безопасности цепочки поставок ИТ-программ и оборудования, целостность данных, надлежащий контроль доступа, упреждающее управление уязвимостями, более высокая периодичность обновления систем и внедрение систем и процессов мониторинга данных.

2. РАССМОТРЕНИЕ ВОПРОСА

2.1 Цель создания глобальной функционально совместимой навигационной системы предполагает наличие общих сетей и объектов ИТ-инфраструктуры, архитектуры и операций, основанных на сетевых технологиях. В будущем информационный обмен не будет ограничиваться связью между двумя узлами, а будет использовать также архитектуру открытых систем и информационные потоки на основе Интернета. Все это повышает уязвимость систем к кибератакам.

2.2 При обеспечении кибербезопасности в области ANS следует уделять внимание защите и устойчивости сетей, системам и их эксплуатационной совместимости, конфиденциальности, целостности и доступности информации. Последнее требует анализа эксплуатационных последствий и жизненного цикла системы.

2.3 Под киберинцидентом подразумевается любое событие, создающее угрозу для доступности, подлинности, целостности или конфиденциальности систем или хранимых, передаваемых или обрабатываемых данных, а также для соответствующих видов обслуживания, предоставляемых с помощью информационных систем и соответствующей инфраструктуры, что может отрицательно сказаться на их нормальной работе.

2.4 Системы ANS подвержены целому ряду киберугроз, таких как утечка информации, пассивный перехват информации, активный перехват информации, изменение конфигурации системы или данных, нарушение конфигурации системы, атаки, направленные на приостановление обслуживания или отказ в обслуживании, и т. д.

2.5 ПАНО следует определить логические и физические элементы поддержки критически важных информационных систем, используемых в рамках осуществления их деятельности, а также рассмотреть степень воздействия на эти системы в случае их повреждения или нарушения их работы.

2.6 Меры по защите критически важных информационных систем должны предприниматься как можно раньше на этапе проектирования, чтобы обеспечить их максимальную устойчивость к кибератакам.

2.7 В качестве мер по обеспечению безопасности инфраструктуры следует рассматривать меры по обеспечению безопасности при проектировании, разделение сетей и удаленный доступ.

2.8 В качестве мер по обеспечению безопасности цепочки поставок в отношении логических и физических элементов поддержки следует рассматривать периодическое обновление авиационных информационно-коммуникационных систем, необходимость которого обусловлена изменениями эксплуатационных требований и модернизацией логических элементов поддержки.

2.9 Реализация плана управления риском в области ANS требует как минимум определения кибератив, используемых для организации воздушного движения (ОрВД) и определения уровней классификации инцидентов, угроз и воздействия на систему.

	DESCRIPTION OF PROCESSES							
Strategic product	Process	Sub-process	Asset name	Identifier or Code	Type	Location	Person responsible / Owner	Support

				CRITICALITY ANALYSIS			
Storage medium	Retention time	Disposal	Search criterion	Confidentiality	Integrity	Availability	Criticality

Рис. 1. Схема идентификации и каталогизации киберактивов, используемых в области ОрВД

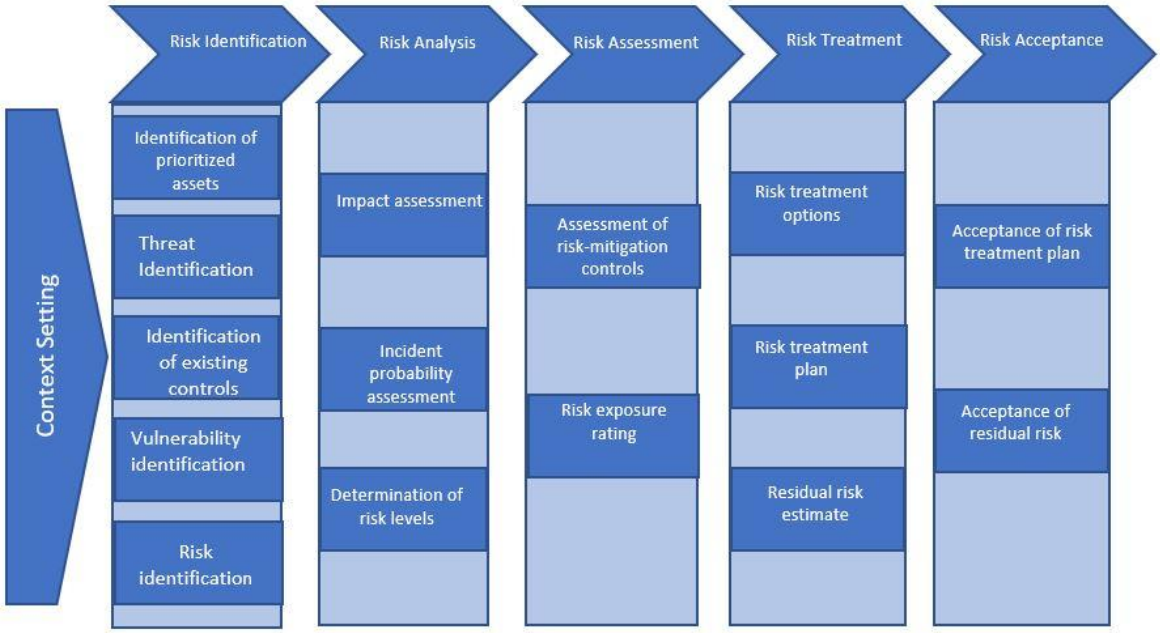

Рис. 2. Схема управления риском

		Susceptibilty						Risk																
								Probability of occurrence									Impact							
								Threat agent factors				Vulnerability factors					Technical factors					Business fac		
ASSET ID	Vulnerability	Identity fraud (Authenticity)	Manipulation (Integrity)	Rejection (No Rejection)	Information disclosure (Confidentiality)	Denial of service (Availability)	Privilege escalation (Authorization)	Skill level	Motivation	Opportunity	Size	Ease of discovery	Ease of exploitation	Awareness	Intrusion detection	Total probability of occurrence	Loss of confidentiality	Loss of integrity	Loss of availability	Loss of responsibility	Overall technical impact	Financial loss	Reputational damage	Non-compliance
ASST 17	Description of vulnerability	S	T	R	I		E	9	4	4	3	4	3	3	4	**4.25**	2	2	2	2	**2**	6	3	3
ASST 17		S	T		I	D	E	4	4	7	4	4	4	7	4	**4.75**	4	4	3	3	**3.5**	3	4	4
ASST 17		S	T	R	I	D	E	4	4	7	9	9	9	9	3	**6.75**	7	7	0	0	**3.5**	0	0	0
ASST 16 & 17		S	T	R	I	D	E	4	4	7	9	9	9	9	3	**6.75**	2	2	2	2	**2**	2	2	2
ASST 17		S	T		I	D	E	0	0	0	0	0	0	0	0	**0**	0	0	0	0	**0**	0	0	0
ASST 16 & 17		S	T		I	D	E	0	0	0	0	0	0	0	0	**0**	0	0	0	0	**0**	0	0	0

Рис. 3. Анализ рисков и данные об уязвимости для указанных активов

2.10 Разработка плана управления риском должна позволить прогнозировать последствия реализации таких угроз, как кибератаки и невраждебные киберинциденты, исходя из результатов анализа и оценки риска, которому подвергаются сети и системы, с тем чтобы не допускать таких случаев или сократить их количество. Возможные последствия могут быть смягчены путем определения немедленных действий и мер по постепенному улучшению ситуации с использованием соответствующих показателей, мер контроля и документации.

2.11 В качестве вспомогательного элемента управления рисками следует рассмотреть возможность создания отдельного реестра для каждого идентифицированного кибератива в области ОрВД. Этот позволит:

a) обобщать кибератривы одного типа и/или одинакового жизненного цикла;

b) обеспечивать целостность данных;

c) способствовать успешному выполнению действий по поддержанию устойчивости системы;

d) предотвращать дублирование или устаревание элементов;

e) сократить усилия, необходимые для проведения анализа и принятия решений.

3. ВЫВОД

3.1 Для реализации стратегий по обеспечению кибербезопасности путем противодействия цифровым угрозам в области ANS поставщикам данного вида обслуживания необходимо разработать планы и рабочие процедуры для защиты систем и соответствующей инфраструктуры, а также обеспечить их достаточную устойчивость для сохранения *конфиденциальности, целостности и доступности* информации.

3.2 С учетом вышеизложенного и в контексте Плана действий ИКАО по обеспечению кибербезопасности Конференции предлагается согласиться со следующей рекомендацией:

ПАНО:

a) разработать план управления риском в области кибербезопасности, который как минимум будет включать идентификацию киберактивов в области ОрВД, классификацию инцидентов, классификацию уровней опасности, степень воздействия на систему и порядок действий по восстановлению системы;

b) рассмотреть факторы, способствующие управлению риском, такие как разработка отдельного реестра для каждого функционально совместимого киберактива в области ОрВД;

c) вновь подтвердить обязательство по постоянному усовершенствованию различных процессов, в том числе тех, которые указаны как критически важные, с целью достижения оптимального уровня кибербезопасности в области аэронавигационного обслуживания (ANS).

— КОНЕЦ —