Международная организация гражданской авиации

РАБОЧИЙ ДОКУМЕНТ

AN-Conf/14-WP/136
30/6/24
Revision No.1
30/7/24

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

ОБМЕН ИНФОРМАЦИЕЙ С ИСПОЛЬЗОВАНИЕМ ПЛАТФОРМЫ ДЛЯ ОБМЕНА ИНФОРМАЦИЕЙ О ВРЕДОНОСНЫХ ПРОГРАММАХ (MISP) И ЕЕ ВКЛАД В ПОВЫШЕНИЕ КИБЕРБЕЗОПАСНОСТИ И УСТОЙЧИВОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

(Представлено Бразилией при поддержке 20 государств – членов[1] Латиноамериканской комиссии гражданской авиации (ЛАКГА):

ПЕРЕСМОТРЕННЫЙ ВАРИАНТ № 1

КРАТКАЯ СПРАВКА

В настоящем рабочем документе основное внимание уделяется усилиям Бразилии по обеспечению авиационной кибербезопасности, касающимся обмена информацией по кибербезопасности через платформу для обмена информацией о вредоносных программах (MISP) в соответствии с предложениями Группы экспертов ИКАО по кибербезопасности (CYSECP). В нем подчеркивается, что это решение не требует каких-либо дополнительных расходов на кибербезопасность и способствует развитию сотрудничества между государствами, организациями и отраслью в вопросах повышения кибербезопасности.

Действия: Конференции предлагается:

a) принять к сведению полученный к настоящему времени Департаментом контроля воздушного пространства (DECEA) Бразилии положительный опыт использования платформы MISP в качестве платформы для обмена информацией по кибербезопасности;

b) рекомендовать государствам-членам внедрить MISP в качестве платформы для обмена информацией по кибербезопасности;

c) передать поднятый в настоящем документе вопрос на рассмотрение Группе экспертов по кибербезопасности (CYSECP) и создать рабочую группу для обсуждения вопросов стандартизации обмена информацией по кибербезопасности и потенциальной возможности использования платформы MISP государствами-членами.

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

1. ВВЕДЕНИЕ

1.1 ИКАО продолжает совершенствовать свои стандарты и правила с учетом постоянно меняющегося характера глобальных угроз в соответствии с резолюциями Совета Безопасности Организации Объединенных Наций, в которых подчеркивается обязательство государств обеспечивать безопасность воздушных перевозок в рамках своей юрисдикции. В этих резолюциях всем государствам настоятельно рекомендуется сотрудничать с ИКАО в вопросах оценки, усовершенствования и внедрения международных стандартов безопасности. Для эффективного достижения целей, предусмотренных в семи основополагающих элементах Стратегии в области авиационной кибербезопасности, а также для создания надежного механизма обеспечения кибербезопасности был разработан План действий по обеспечению кибербезопасности (ПДоК).

1.2 В основные обязанности DECEA входит контроль за деятельностью служб управления воздушным движением, безопасности полетов, поиска и спасания, а также управление системой электросвязи гражданской авиации Бразилии. Кроме того, DECEA отвечает за материально-техническое обеспечение и техническое обслуживание систем кибербезопасности, необходимых для выполнения этих задач.

2. РАССМОТРЕНИЕ ВОПРОСА

2.1 Обмен информацией по кибербезопасности

2.1.1 Глобальные угрозы вызывают все более серьезную обеспокоенность. В целях обеспечения безопасности и непрерывности авиасообщения аэронавигационные системы и системы наблюдения должны быть защищены при осуществлении глобального обмена информацией. Идентификация таких систем и контроль за ними имеют основополагающее значение для предотвращения использования уязвимых мест, что приводит к нарушениям в работе или ее приостановлению. Кроме того, появление новых систем, являющихся результатом гиперсвязности аэронавигации, станет серьезной проблемой к 2030 году. В этой связи своевременное выявление угроз является существенным фактором, позволяющим более эффективно использовать средства обеспечения кибербезопасности для защиты систем обслуживания авиации.

2.1.2 Таким образом, практика обмена информацией о киберугрозах полностью соответствует Национальной политике в области кибербезопасности (PNCiber) Бразилии, утвержденной указом № 11 856 от 26 декабря 2023 года, в котором в качестве одной из целей указано следующее:

— "реализация стратегий взаимодействия для развития международного сотрудничества в области кибербезопасности" (см. пункт XI статьи 3)

2.1.3 В рамках ИКАО основные принципы обмена информацией по кибербезопасности изложены во втором издании Плана действий по обеспечению кибербезопасности (ПДоК), опубликованном в январе 2022 года. В пункте 3.1.1 ПДоК конкретно указано, что обмен информацией является одним из основополагающих элементов Стратегии в области авиационной кибербезопасности.

2.2 Платформа для обмена информацией о вредоносных программах

2.2.1 Платформа для обмена информацией о вредоносных программах (MISP) является важнейшим средством обеспечения кибербезопасности, предназначенным для обмена

информацией об угрозах. Масштабы ее внедрения расширяются благодаря многочисленным преимуществам, которые она предоставляет организациям и специалистам по кибербезопасности. Основные преимущества заключаются в следующем:

a) Платформа MISP упрощает сотрудничество между организациями, обеспечивая безопасный обмен информацией об угрозах. Это имеет ключевое значение в условиях постоянного изменения характера киберугроз. Возможность обмена индикаторами несанкционированного доступа и информацией об угрозах в режиме реального времени позволяет обеспечить более надежную и эффективную защиту.

b) Благодаря централизации доступа к информации об угрозах и обмену ею платформа MISP позволяет организациям получать доступ к данным об угрозах в режиме реального времени. Это ускоряет процесс выявления инцидентов и реагирования на них, повышая общий уровень безопасности.

c) Платформа MISP включает множество функций настройки и расширения, что позволяет организациям адаптировать эту платформу к своим конкретным потребностям. Это включает возможности добавления пользовательских параметров, создания специализированных моделей угроз и объединения платформы MISP с другими средствами обеспечения безопасности.

d) Платформа MISP предоставляет пользователям возможность поддерживать связь с мировым сообществом по вопросам кибербезопасности, способствуя обмену информацией с другими специалистами и организациями. Это позволяет расширить имеющийся объем знаний и укрепить защиту от крупномасштабных угроз, обеспечивая понимание тактических, методических и организационных (ТМО) аспектов действий киберпреступников.

e) Платформа MISP включает передовые средства контроля доступа и обеспечения конфиденциальности, что позволяет организациям осуществлять выборочный и безопасный обмен информацией. Это является необходимым условием для защиты конфиденциальных данных и соблюдения норм конфиденциальности.

2.2.2 В целом платформа MISP играет важную роль в устранении киберугроз в качестве эффективной платформы для обмена информацией по кибербезопасности. Ее внедрение способствует повышению эффективности защиты организаций и укреплению кибербезопасности на национальном, региональном и глобальном уровнях.

2.3 Использование платформы MISP в DECEA

2.3.1 DECEA начал внедрять платформу MISP в 2021 году и с тех пор использует и совершенствует этот инструмент. Постоянное усовершенствование способов применения платформы MISP подчеркивает стремление DECEA адаптироваться к меняющемуся характеру проблем в области кибербезопасности.

2.3.2 Внедрение платформы MISP позволяет DECEA эффективно сотрудничать в вопросах обмена важнейшими данными об угрозах с другими бразильскими заинтересованными сторонами, включая Центр реагирования на сетевые инциденты ВВС Бразилии (CTIR.FAB), Бразильскую нефтяную компанию (Petrobras), Национальное агентство электросвязи (ANATEL) и Бразильскую банковскую федерацию (FEBRABAN). Это сотрудничество не только укрепляет

собственные защитные механизмы DECEA, но и способствует повышению общего уровня безопасности в системе контроля воздушного пространства Бразилии (SISCEAB).

2.3.3 Индикаторы угроз и предупреждения, полученные через платформу MISP от других пользователей, обрабатываются и служат основой для составления черных списков или установления правил межсетевого экрана. Эти индикаторы содержат важные сведения о потенциальных угрозах безопасности, позволяющие организациям заблаговременно обеспечивать защиту своих сетей и систем от противоправных действий, упреждая возникающие угрозы и укрепляя свою кибербезопасность.

2.3.4 Связанные с угрозами правила определяются меняющимся со временем уровнем риска. Этот уровень риска для каждой угрозы постоянно обновляется на основе показателей, полученных через платформу MISP. Посредством оперативной корректировки уровня риска, связанного с каждой угрозой, организации могут обеспечивать неизменную эффективность и гибкость правил межсетевого экрана для повышения уровня безопасности. Такой подход позволяет осуществлять более адаптивные и конкретизированные стратегии борьбы с угрозами, повышая при этом общий уровень киберустойчивости.

2.3.5 В качестве примера на рисунке 1 показаны десять наиболее распространенных типов угроз, о которых DECEA стало известно через платформу MISP в прошлом году, таких как троянская программа "Зевс", наличие фишинговых URL в результатах поиска, обновленные эмуляторы IOC, троянская программа "Цитадель" и фишинговые веб-сайты.

2.3.6 На рисунке 2 показано ежедневное количество случаев блокировки вредоносных программ на основе индикаторов, полученных через платформу MISP, за недельный период. Как показано на представленной ниже диаграмме, на долю платформы MISP приходится около 40 000 000 случаев блокировки вредоносных программ в год.

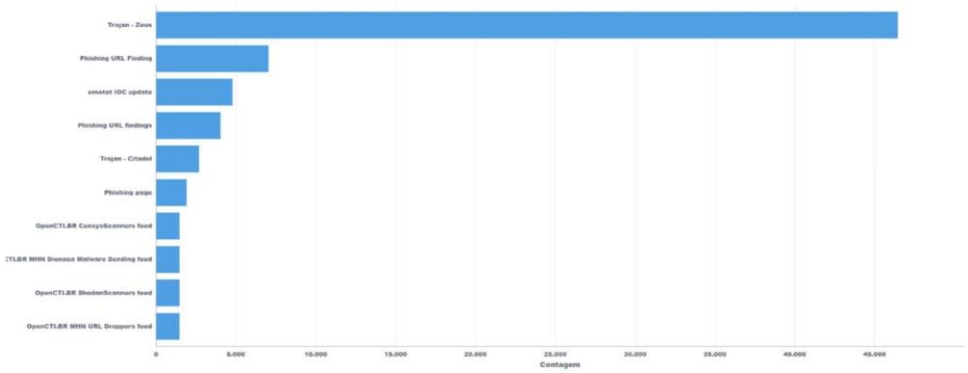

Рис. 1. 10 наиболее распространенных типов угроз, сведения о которых были получены DECEA

Рис. 2. Вредоносные программы, заблокированные на основе индикаторов платформы MISP

2.3.7 В настоящее время платформа MISP помогает получать и/или отправлять уведомления о любых подтвержденных или предполагаемых неблагоприятных событиях, связанных с безопасностью компьютерных систем или компьютерных сетей, в целях содействия обеспечению информационной безопасности в рамках SISCEAB.

3. ВЫВОД

3.1 В заключение следует отметить, что использование платформы MISP в DECEA значительно повышает уровень авиационной кибербезопасности в Бразилии. Этот упреждающий подход соответствует международным стандартам, в частности положениям Плана действий ИКАО по обеспечению кибербезопасности (ПДоК). DECEA также оказывает поддержку Национальному агентству гражданской авиации (ANAC) Бразилии в использовании платформы MISP в целях повышения эффективности обмена информацией о киберугрозах в секторе гражданской авиации Бразилии с использованием функциональных возможностей платформы MISP для обмена данными в режиме реального времени и соблюдения открытых стандартов.

3.2 Бразилия вновь подтверждает свою готовность вносить вклад в обеспечение международной авиационной безопасности, особенно в сфере кибербезопасности. Ее основанный на сотрудничестве подход способствует повышению безопасности полетов во всем мире. Поскольку гиперсвязность увеличивает уязвимые места аэронавигационных систем, Бразилия стремится внедрять оптимальные стратегии и технологии для защиты своей важнейшей авиационной инфраструктуры от возникающих киберугроз.

3.3 Бразилия намерена содействовать использованию платформы MISP в Карибском и Южноамериканском (CAR/SAM) регионе, а также ознакомиться с инициативой по обмену информацией о киберугрозах и принимать в ней активное участие, способствуя тем самым использованию платформы MISP в качестве надежной платформы для сотрудничества. Цель заключается в повышении киберустойчивости региональной авиации для обеспечения будущей глобальной интеграции в соответствии с рекомендациями ИКАО.

3.4 С учетом вышеизложенного Конференции предлагается согласиться со следующей рекомендацией:

Рекомендация 4.2/x. Кибербезопасность и устойчивость информационных систем

a) принять к сведению полученный к настоящему времени Департаментом контроля воздушного пространства (DECEA) Бразилии положительный опыт использования платформы MISP в качестве платформы для обмена информацией по кибербезопасности;

b) рекомендовать государствам-членам внедрить MISP в качестве платформы для обмена информацией по кибербезопасности;

c) передать поднятый в настоящем документе вопрос на рассмотрение Группе экспертов по кибербезопасности (CYSECP) и создать рабочую группу для обсуждения вопросов стандартизации обмена информацией по кибербезопасности и потенциальной возможности использования платформы MISP государствами-членами.

— КОНЕЦ —