Руководство по Протоколу "Светофор"

Опубликовано с санкции Генерального секретаря

Сентябрь 2021 года

Международная организация гражданской авиации

РУКОВОДСТВО ПО ПРОТОКОЛУ "СВЕТОФОР"

1. Введение и сфера применения

Человеческий фактор лежит в основе решения проблем кибербезопасности и киберустойчивости в авиации. Поэтому повышение осведомленности каждого сотрудника является обязательным условием для обеспечения безопасности и устойчивости сектора. При этом не менее важно разработать политику для обеспечения внедрения четких инструктивных материалов, которые позволят свести к минимуму путаницу в действиях, которые необходимо предпринять.

Когда информация поступает по каналу связи, понимание того, какой информацией можно делиться с другими и с кем можно делиться этой информацией, является одним из основных действий, требующих повышения осведомленности. Обмен информацией за пределами предполагаемой "сферы распространения" может привести к непреднамеренному распространению конфиденциальной информации, которая может быть использована в неблаговидных целях и потенциально привести к ущербу для источника информации.

В связи с этим и в целях обеспечения четких инструктивных материалов по коммуникации и обмену информацией между всеми заинтересованными сторонами в сфере авиации ИКАО в сотрудничестве с экспертами Исследовательской группы Секретариата по кибербезопасности (SSGC) разработала данный инструктивный материал по использованию протокола "Светофор" (TLP).

Данное руководство соответствует Плану действий по обеспечению кибербезопасности,[1] в котором в пункте действий CyAP5.4 рекомендуется "Использовать TLP (протокол "Светофор") для определения уровня распространения/ограничений при распространении киберинформации и дальнейшем обмене такой информацией". Более того, использование TLP может быть расширено, чтобы TLP можно было использовать в любом сообщении с целью особо отметить разрешение на обмен информацией, полученное от источника.

Государствам и заинтересованным сторонам рекомендуется использовать данный инструктивный материал для разработки и внедрения политики использования TLP.

2. Задача

Настоящий документ содержит инструктивные материалы по требованиям в отношении использования TLP при обмене информацией.

3. Инструктивные материалы по TLP

3.1 Предназначение TLP

Протокол "Светофор" (TLP) был создан для того, чтобы способствовать более широкому обмену информацией. TLP представляет собой набор обозначений, используемых для обеспечения обмена информацией с соответствующей аудиторией. В нем используются цвета для обозначения ожидаемых границ распространения информации, которые должны применяться получателем(ями). TLP имеет четыре цвета, как указано в разделе 5 ниже.

[1] Письмо ИКАО государствам 2020/114.

TLP предоставляет простую и понятную схему для указания того, когда и каким образом можно обмениваться конфиденциальной информацией, способствуя более частому и эффективному сотрудничеству. TLP не является "контрольной маркировкой" или системой классификации. TLP не предназначен для определения условий лицензирования, правил обработки и шифрования данных, а также ограничений на действия или инструментарий, используемый в отношении информации. Маркировки TLP и их определения не предназначены для оказания какого-либо влияния на свободу распространения информации или "законы о прозрачности"[2] в какой-либо юрисдикции.

TLP оптимизирован для обеспечения простоты его принятия, удобочитаемости и обмена информацией непосредственно между людьми; он может использоваться в автоматизированных системах обмена, однако не оптимизирован для этого.

TLP отличается от правила "Чатем-Хаус" (когда совещание или его часть проводится в соответствии с правилом "Чатем-Хаус", участники могут свободно использовать полученную информацию, но при этом не раскрываются ни персональные данные, ни принадлежность к той или иной организации докладчика(ов) или любого другого участника), однако может использоваться совместно с этим правилом, если участники обмена информацией сочтут это целесообразным.

3.2 Требования в отношении TLP (T)

- T1: Источник информации обязан присвоить передаваемой информации соответствующую маркировку TLP.
- T2: Получатель информации, имеющей маркировку TLP, должен соблюдать требования маркировки TLP.
- T3: Маркировка TLP должна быть присвоена информации источником с учетом принципа нужной получателю(ям) информации и его(их) способности осуществлять действия на основе передаваемой информации и ее маркировки, присвоенной согласно TLP.
- T4: Источник обязан обеспечить, чтобы получатели информации, предоставляемой с помощью TLP, понимали руководство по обмену информацией согласно TLP и могли следовать ему.
- T5: Если получателю необходимо распространить информацию в более широком объеме, чем указано в исходном обозначении согласно TLP, он должен получить четкое разрешение на это от первоначального источника информации.
- T6: Рекомендуется иметь единую маркировку TLP для каждого документа, однако если документ содержит различные маркировки TLP, маркировка каждой строки или раздела должна быть четко обозначена.
- T7: Если имеются некоторые специфические ограничения для дальнейшего распространения, выходящие за рамки определения присвоенной маркировки TLP (например, TLP: ЗЕЛЕНЫЙ, только для авиационного сообщества), это должно быть четко обозначено.
- T8: Получатель информации с маркировкой TLP не должен изменять маркировку TLP при дальнейшем распространении информации, полученной от источника.

[2] Законы о прозрачности – это нормативные акты, требующие прозрачности и раскрытия информации в правительстве или бизнесе. Законы о прозрачности обеспечивают доступность отчетов о совещаниях, протоколов, результатов голосования, информации об обсуждениях и других официальных действий для общественного контроля, участия и/или проверки.

4. Как использовать TLP

4.1 Как использовать TLP в электронной почте

В электронной корреспонденции, обозначенной при помощи TLP, цветовое обозначение информации согласно TLP должно быть указано в строке темы и в тексте письма перед самой маркированной информацией. Цвет TLP должен быть указан прописными буквами: TLP:КРАСНЫЙ, TLP:ЖЕЛТЫЙ, TLP:ЗЕЛЕНЫЙ или TLP:БЕЛЫЙ. Ниже приведен пример указания цвета TLP:

4.2 Как использовать TLP в документах

В документах с маркировкой TLP присвоенное информации цветовое обозначение TLP должно быть указано в верхнем и нижнем колонтитулах каждой страницы. Во избежание путаницы с существующими схемами контрольной маркировки рекомендуется наносить маркировку TLP справа. Цвет TLP должен быть указан прописными буквами и шрифтом размером 12 или больше. Ниже приведен образец указания цвета TLP:

5. Определения TLP[3] [4]

Протокол "Светофор" (TLP) предоставляет источнику информации возможность классифицировать информацию и указать ограничения на распространение каждой категории информации, которую он предоставляет.

Обозначения TLP и связанные с ними запреты на использование и ограничения являются следующими:

МАРКИРОВКА TLP	ОГРАНИЧЕНИЯ В ОТНОШЕНИИ ДОСТУПА И ИСПОЛЬЗОВАНИЯ	ПРИМЕР
TLP:КРАСНЫЙ	Раскрытию не подлежит, информация предназначена только для получателей. Источники могут использовать TLP:КРАСНЫЙ, когда информация не может быть эффективно использована другими сторонами и в случае ее злонамеренного использования, она может негативно повлиять на конфиденциальность, репутацию или деятельность той или иной стороны.	Обмен информацией с участниками совещания; прямое электронное сообщение с маркировкой TLP:КРАСНЫЙ.

[3] См. https://www.cisa.gov/tlp
[4] См. https://www.first.org/tlp

	Получателям нельзя обмениваться информацией с маркировкой TLP:КРАСНЫЙ с какой-либо стороной за пределами особой процедуры обмена, совещания или переговоров, в ходе которых она была первоначально раскрыта. Например, в контексте совещания информация с маркировкой TLP:КРАСНЫЙ предназначена только для лиц, присутствующих на данном совещании. В большинстве случаев информацией с маркировкой TLP:КРАСНЫЙ следует обмениваться устно или лично.	
TLP:ЖЕЛТЫЙ	Ограниченное раскрытие информации только в рамках организаций получателей. Источники могут использовать TLP:ЖЕЛТЫЙ, когда для эффективных действий по этой информации требуется определенная поддержка, но она создает риск для конфиденциальности, репутации или деятельности, если ею обмениваться за пределами участвующих организаций. Получателям разрешается обмениваться информацией с маркировкой TLP:ЖЕЛТЫЙ только с сотрудниками их собственной организации и с клиентами или потребителями, которым необходимо знать эту информацию для своей защиты или предотвращения дальнейшего ущерба. **Источники могут указать дополнительные желаемые ограничения обмена информацией: они должны соблюдаться.**	Информирование CSIRT организации о признаках несанкционированного доступа к данным (IoCS). Такие сообщения могут быть направлены в SOC для дальнейших действий.
TLP:ЗЕЛЕНЫЙ	Ограниченное раскрытие информации только в рамках определенного сообщества. Источники могут использовать TLP:ЗЕЛЕНЫЙ, когда информация полезна для оповещения всех участвующих организаций, а также организаций с равным статусом в пределах более широкого сообщества или сектора. Получателям разрешается обмениваться информацией с маркировкой TLP:ЗЕЛЕНЫЙ с	Обмен результатами анализа вредоносного программного средства с местным сектором авиационной отрасли.

	организациями с равным статусом и партнерскими организациями в пределах их сектора или сообщества, но не через общедоступные каналы. Информацию этой категории можно широко распространять в пределах конкретного сообщества. Раскрытие информации с маркировкой TLP:ЗЕЛЕНЫЙ за пределами конкретного сообщества не допускается.	
TLP:БЕЛЫЙ	Раскрытие информации не ограничено. Источники могут использовать TLP:БЕЛЫЙ в соответствии с применяемыми правилами и порядком открытой публикации, когда информация сопряжена с минимальным риском или предположительно отсутствует риск злонамеренного использования. При условии соблюдения стандартных авторских прав информация с маркировкой TLP:БЕЛЫЙ может распространяться без ограничений.	Памятка по вопросам общественной безопасности.

6. Сокращения

CSIRT	Группа реагирования на инциденты в области компьютерной безопасности
ICT	Информационные и коммуникационные технологии
IoCS	Признаки несанкционированного доступа к данным
SOC	Центр обеспечения безопасности
TLP	Протокол "Светофор"

— КОНЕЦ —