ИКАО

SECURITY AND FACILITATION

Обмен киберинформацией

Опубликовано с санкции Генерального секретаря
2024 год, версия 1

МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ГРАЖДАНСКОЙ АВИАЦИИ

Содержание

СОКРАЩЕНИЯ

БАС	Беспилотная авиационная система
ВГА	Ведомство гражданской авиации
ИКАО	Международная организация гражданской авиации
ИТ	Информационные технологии
ПАНО	Поставщики аэронавигационного обслуживания
ПОК	Политика обмена киберинформацией
CERT	Группа реагирования на компьютерные инциденты
CSIRT	Группа реагирования на инциденты в области кибербезопасности
CTI	Разведданные о киберугрозах
FIRST	Форум групп оперативного реагирования и обеспечения безопасности
IoC	Признаки несанкционированного доступа
IPR	Права интеллектуальной собственности
ISAC	Центр анализа информации и обмена ею
ISMS	Система управления информационной безопасностью
OSINF	Информация из открытых источников
OSINT	Разведданные на основе открытых источников
SOC	Центр обеспечения безопасности
TLP	Протокол "Светофор"
TTP	Тактика, приемы и процедуры

КРАТКАЯ СПРАВКА

Передовой опыт, накопленный в области безопасности полетов и авиационной безопасности, свидетельствует о важности обмена информацией и его роли в снижении угроз и рисков для гражданской авиации. Не менее важен и обмен киберинформацией.

Обмен киберинформацией имеет решающее значение для управления киберрисками в гражданской авиации. Он способствует развитию полноценной культуры кибербезопасности, помогая укреплять сотрудничество и доверие. Он также позволяет получать более полную картину происходящего для оперативного и тактического управления киберрисками и стратегического планирования.

В настоящем документе приводится инструктивный материал для государств и заинтересованных сторон в отрасли по разработке плана обмена киберинформацией, включая рекомендации по разработке политики, использованию ресурсов и практическим мерам по внедрению и постоянному совершенствованию практики такого обмена.

Здесь также описаны предпосылки для обмена киберинформацией в авиационной отрасли. Перечислены различные типы киберинформации, которой можно делиться. Кроме того, в документе обсуждаются аспекты анализа и обеспечения гарантий при обмене киберинформацией, при этом подчеркивается необходимость оценки уровня доверия к источнику и достоверности информации.

Настоящий документ заменяет ранее опубликованное руководство ИКАО по использованию протокола "Светофор" (TLP) в гражданской авиации. В нем изложены правила обмена киберинформацией в авиационной отрасли на основе обновленного стандарта TLP в зависимости от типа передаваемой информации, даты/времени передачи информации и получателей (например, государственных органов, эксплуатантов, поставщиков услуг).

В целом в документе подчеркивается важность обмена различными видами киберинформации в секторе гражданской авиации с учетом анализа, обеспечения гарантий и надлежащей маркировки для эффективного распространения информации среди соответствующих заинтересованных сторон.

Это руководство согласуется со Стратегией в области авиационной кибербезопасности[1] Международной организации гражданской авиации (ИКАО) и связанным с ней Планом действий по обеспечению кибербезопасности[2] и выпущено в связи с потребностью в обмене киберинформацией. Информация, содержащаяся в настоящем документе, соответствует общим принципам инструктивных материалов ИКАО по обмену информацией о безопасности полетов и авиационной безопасности, включенным в *Руководство по авиационной безопасности* (Doc 8973 – Restricted) и *Руководство по управлению безопасностью полетов* (Doc 9859).

[1] https://www.icao.int/aviationcybersecurity/Pages/Aviation-Cybersecurity-Strategy.aspx
[2] https://www.icao.int/aviationcybersecurity/Pages/Cybersecurity-Action-Plan.aspx

ОПРЕДЕЛЕНИЯ

Авиационная кибербезопасность. Комплекс технологий, средств контроля и мер, а также процессов и практических методов, предназначенных для обеспечения конфиденциальности, целостности, доступности и общей защиты систем, сетей, программ, устройств, информации и данных от атак, повреждений, несанкционированного доступа, использования и/или эксплуатации.

Вектор атаки. Средства доступа, которые злоумышленник использовал для начала атаки.

Готовность к работе. Показатель доступности и пригодности для использования по требованию уполномоченного лица, пользователя, программы, процесса, системы или устройства.

Информационная безопасность. Сохранение конфиденциальности, целостности и доступности информации.

Кибератривы. Цифровые и физические объекты, имеющие ценность с точки зрения бизнеса, производства полетов, безопасности полетов, авиационной безопасности, эффективности и/или пропускной способности, такие как системы, информация, данные, сети, устройства, программное обеспечение, аппаратные средства, процессы, встроенное программное обеспечение, соответствующий/сертифицированный персонал и другие электронные ресурсы.

Кибератака. Преднамеренное использование электронных средств для прерывания работы, изменения, уничтожения кибератривов или получения несанкционированного доступа к ним.

Киберинцидент. Разовое киберсобытие или серия киберсобытий, которые отрицательно сказываются на безопасности полетов, авиационной безопасности, эффективности и/или пропускной способности.

Киберриски. Возможность нежелательного результата киберсобытия.

Киберсобытие. Любое наблюдаемое событие в сети или системе.

Киберугроза. Любое потенциальное киберсобытие, которое может отрицательно сказаться на безопасности полетов, авиационной безопасности, эффективности и/или пропускной способности.

Киберустойчивость. Способность кибератива обеспечивать выполнение важнейших функций в неблагоприятных или стрессовых условиях и восстанавливаться после таких неблагоприятных условий.

Конфиденциальность. Принцип, согласно которому актив не предоставляется или не раскрывается лицу, пользователю, программе, процессу, системе или устройству, не имеющему соответствующего разрешения.

Обеспечение гарантий. Запланированные и систематические действия, необходимые для обеспечения достаточной уверенности в том, что продукт или процесс удовлетворяют заданным требованиям.

Обмен информацией. Процесс, посредством которого одна организация предоставляет информацию другой или нескольким другим организациям в целях содействия принятию решений на основе оценки риска и распространения передовой практики.

Оценка киберрисков. Непрерывный процесс выявления, анализа и оценки киберрисков.

Проверка подлинности. Действие, подтверждающее утверждение об идентичности физического лица, пользователя, программы, процесса, системы или устройства.

Субъект угрозы. Субъект, частично или полностью ответственный за инцидент, который воздействует (или может воздействовать) на организацию или систему.

Тяжесть последствий. Качественный показатель величины неблагоприятных последствий угрозы.

Управление киберрисками. Непрерывный процесс выявления, уменьшения последствий, урегулирования и мониторинга киберугроз и рисков в соответствии с оценкой рисков.

Устранение последствий кибератак. Средства контроля за безопасностью, направленные на снижение киберриска, связанного с конкретной киберугрозой или уязвимостью, с учетом их воздействия на безопасность полетов, авиационную безопасность, эффективность и/или пропускную способность.

Целостность. Показатель точности и полноты актива, подтверждающий то, что представляет собой актив.

1. ВВЕДЕНИЕ

1.1 Доводы в пользу обмена киберинформацией

Обмен информацией имеет принципиально важное значение для более эффективного противодействия киберрискам в авиации. В сегодняшнем взаимосвязанном мире киберугрозы представляют собой значительный риск для сектора гражданской авиации. Объектом кибератаки может стать любой компонент авиационной системы, от систем организации воздушного движения до систем работы с данными пассажиров, что может привести к сбоям в работе и поставить под угрозу безопасность и защищенность пассажиров. Таким образом, эффективное противодействие киберрискам требует общего подхода, который включает в себя обмен информацией между заинтересованными сторонами.

Накопленный опыт обеспечения безопасности полетов и авиационной безопасности свидетельствует о том, что воспитание культуры обмена информацией позволит значительно снизить риск для гражданской авиации, создаваемый злоумышленниками. В авиационном секторе обмен информацией доказал свою эффективность в качестве ценного инструмента управления рисками в части безопасности полетов и авиационной безопасности. Тот же принцип применим к авиационной кибербезопасности. Обмениваясь киберинформацией, заинтересованные стороны могут лучше понять природу киберугроз, с которыми они сталкиваются, выявить уязвимости и принять надлежащие меры для предотвращения или смягчения последствий кибератак на гражданскую авиацию.

Обмен информацией также является важным аспектом полноценной культуры кибербезопасности. Полноценная культура кибербезопасности помогает адекватно распознавать киберугрозы и реагировать на них. Обмен информацией является неотъемлемой частью этой культуры, поскольку он способствует прозрачности в отношениях, сотрудничеству и доверию между заинтересованными сторонами. Реальный обмен киберинформацией гарантирует, что все заинтересованные стороны располагают необходимой информацией для принятия обоснованных решений, соответствующих мер, смягчения киберугроз и/или реагирования на киберинциденты и восстановления после них.

Киберинформация – это не только информация, относящаяся к конкретным киберугрозам, но и любой тип разведданных, которые могут оказать влияние на киберриски для гражданской авиации. Обмен киберинформацией не ограничивается киберразведкой. Он включает в себя любую актуальную информацию, которая может способствовать выявлению и снижению киберрисков в секторе гражданской авиации. Так, информация о нарушениях физической безопасности, внутренних угрозах, геополитических условиях, технологиях или уязвимостях цепочек поставок также может помочь заинтересованным сторонам лучше понять природу киберугроз и рисков и смягчать их последствия.

Обмен киберинформацией способствует:

- **Стратегическому планированию** в целях наращивания потенциала обеспечения авиационной кибербезопасности. Обмениваясь информацией, заинтересованные стороны могут выявить пробелы в своих возможностях в плане обеспечения кибербезопасности и разработать соответствующие стратегии повышения киберустойчивости. Стратегическое планирование гарантирует, что авиационный сектор остается защищенным и устойчивым к киберугрозам и что заинтересованные стороны готовы реагировать на потенциальные киберинциденты и восстанавливаться после них.

- **Осведомленности о ситуации** как в ежедневной работе, так и во время киберинцидентов. Обмениваясь киберинформацией, заинтересованные стороны могут лучше понять состояние своей готовности обеспечивать кибербезопасность, картину киберугроз и потенциальные уязвимости (слабые места) в своих системах. Это позволяет заинтересованным сторонам выявлять потенциальные риски и принимать надлежащие меры для предотвращения или смягчения последствий киберинцидентов.
- **Оперативному и тактическому управлению киберрисками** в преддверии киберугроз и при реагировании на них. Обмениваясь информацией, заинтересованные стороны могут выявлять киберугрозы и разрабатывать соответствующие стратегии управления рисками.
- **Антикризисному управлению** во время киберинцидентов, при котором эффективный обмен информацией позволяет заинтересованным сторонам координировать свои действия и принимать надлежащие меры для смягчения последствий инцидента.

Важно признать, что эффективный обмен информацией основан на доверии между участниками. Данный инструктивный материал призван содействовать укреплению доверия, необходимому для того, чтобы побудить участников преодолеть свои естественные сомнения относительно обмена информацией. Это предусматривает выработку набора общих правил и процедур, которые все участники обмена понимают, принимают и соблюдают. Достижение консенсуса в отношении того, какими видами киберинформации предполагается обмениваться, как организовать этот процесс и как распространять информацию, будет способствовать плодотворному обмену информацией между участниками.

Данный инструктивный материал дополняет комплексную работу ИКАО в части, касающейся авиационной кибербезопасности. Он поддерживает компонент 5 "Обмен информацией" Стратегии ИКАО в области авиационной кибербезопасности и пункт 5.1 Плана действий по обеспечению кибербезопасности, в котором ИКАО предлагается разработать руководство по обмену киберинформацией.

Настоящий документ включается в ранее опубликованный отдельный инструктивный материал ИКАО по использованию протокола "Светофор" (TLP) в гражданской авиации и заменяет его. В настоящий документ включено руководство по использованию обновленной версии 2.0 стандарта TLP[3], разработанного компанией FIRST (Форум групп оперативного реагирования и обеспечения безопасности), в качестве средства обмена киберинформацией в гражданской авиации.

1.2 Контекст обмена киберинформацией

Прежде чем приступить к обмену киберинформацией, необходимо сначала рассмотреть все этапы цикла кибербразведки.

Цикл кибербразведки – это базовый и многократно повторяемый процесс, используемый при анализе разведданных. На каждом этапе цикла решаются критически важные задачи, благодаря чему информация преобразуется из необработанных данных в ценную информацию, которая может помочь с принятием решений, повышением уровня кибербезопасности и достижением различных стратегических целей организации.

Обмен информацией (также называемый "распространением" на рис. 1 ниже) является частью жизненного цикла кибербразведки, который включает в себя следующие этапы:

[3] https://www.first.org/tlp/

1. Планирование и управление. Первый этап сбора и анализа киберинформации – это планирование и управление процессом. Сюда относится определение целей сбора и анализа данных, их объема и масштаба, а также выявление заинтересованных сторон, которые должны участвовать в процессе. Планирование и управление включают также разработку политики и процедур для сбора и анализа информации, а также определение ролей и обязанностей тех, кто участвует в различных этапах.

2. Сбор данных. Второй этап – это непосредственно сбор киберинформации. Сюда относится сбор данных из различных источников (см. раздел 3). Сбор может выполняться вручную или с помощью автоматизированных процессов. Важно убедиться, что собираемые данные актуальны, точны и не устарели.

3. Обработка данных. Третий этап – это обработка собранной информации. Сюда относится конвертирование собранных данных в пригодный для использования формат, их анализ и выявление закономерностей или аномалий, которые могут, например, указывать на наличие киберугрозы. Этот шаг может включать использование инструментов обработки данных, алгоритмов и других методов анализа, например, для выявления потенциальных киберугроз или уязвимостей. Обработка также включает в себя определение значимости и срочности информации и соответствующее ранжирование ответных мер.

4. Анализ и составление отчетов. Четвертый шаг – это анализ и составлении отчетов на основе обработанных данных. Сюда относится, например, интерпретация данных, выявление закономерностей или тенденций, а также определение киберрисков для авиационной системы. В результате может быть принято решение отказаться от использования информации, если ее качество и уровень детализации недостаточны для анализа. Аналитики применяют свои знания и опыт для изучения данных и подготовки аналитических сводок, которые представляли бы ценность для их получателей, а также были точными и прикладными. Этап анализа и подготовки отчетов может также включать разработку рекомендаций по смягчению последствий или предотвращению киберугроз.

5. Распространение (обмен киберинформацией) и обратная связь. Последним шагом является распространение отчетов разведки среди соответствующих заинтересованных сторон. Сюда может относиться обмен киберинформацией с заинтересованными сторонами внутри организации, например сотрудниками внутренних служб информационных технологий (ИТ), групп обеспечения кибербезопасности и/или групп обеспечения авиационной безопасности, а также с внешними заинтересованными сторонами, например с другими авиационными организациями или государственными учреждениями. Распространение включает в себя обеспечение своевременного и безопасного обмена киберинформацией, а также наличие у заинтересованных сторон необходимой информации о контексте и понимания ситуации для принятия мер в соответствии с ней. Действенный процесс распространения помогает сформировать культуру обмена киберинформацией в секторе гражданской авиации и позволяет заинтересованным сторонам принимать соответствующие меры, которые могут способствовать предотвращению киберугроз или смягчению их последствий.

На этом этапе также собирается обратная связь для оценки эффективности и поддержания актуальности жизненного цикла киберразведки в целях его улучшения в будущих итерациях.

Рис. 1. Жизненный цикл кибербразведки

2. ПОЛИТИКА ОБМЕНА КИБЕРИНФОРМАЦИЕЙ (ПОК)

В этом разделе содержатся рекомендации по разработке и осуществлению политики обмена киберинформацией на уровне организации (например, среди заинтересованных сторон в авиации).

Данный инструктивный материал может быть также использован государствами для разработки своих планов обмена киберинформацией. Однако стоит отметить, что национальные схемы обмена киберинформацией могут быть межотраслевыми и включать не только авиационный сектор.

2.1 ПОЛИТИКА ОБМЕНА КИБЕРИНФОРМАЦИЕЙ (ПОК)

ПОК должна определять:

- доводы в пользу обмена киберинформацией;
- сферу применения, контекст и ограничения (например, источники киберинформации, ограничения, связанные с правами интеллектуальной собственности, законами о неприкосновенности частной жизни);
- состав сторон, обменивающихся киберинформацией в рамках организации, и их соответствующие обязанности;
- правила распространения (в том числе дальнейшего распространения[4]) киберинформации внутри и за пределами организации на основе правил классификации/категоризации информации и с учетом соответствующих нормативных и законодательных требований;
- процедуры работы:
  - сбор информации;
  - при необходимости, ее анонимизация;
  - подтверждение достоверности содержания;
  - распространение;
- цикл рассмотрения ПОК и документооборота (т. е. фиксация существенных изменений и процедуры подтверждения достоверности содержания).

ПОК должна быть утверждена организацией в составе системы управления информационной безопасностью (ISMS)[5]. Она должна периодически (например, ежегодно) пересматриваться после любых существенных изменений политики или после любого киберинцидента, в целях учета соответствующих извлеченных уроков.

2.2 Нормативные и договорные требования[6]

ПОК должна соответствовать всем применимым нормативным актам и существующим соглашениям, связанным с обменом киберинформацией, например:

- межотраслевым национальным, региональным и/или международным нормативным актам;
- авиационным национальным, региональным и/или международным нормативным актам;

[4] Дальнейший обмен информацией обсуждается в разделе 5 настоящего документа.
[5] ISO 27001, глава A.5.14 *"Передача информации"*.
[6] Дополнительную информацию (межотраслевую) можно найти по следующим ссылкам:
NIST. SP.800-150 – Руководство по обмену информацией о киберугрозах
ENISA Cyber Security Information Sharing (Обмен информацией о кибербезопасности): обзор нормативных и прочих подходов
https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

- соглашениям с национальными и/или международными центрами обмена и анализа информации (ISAC) и группами реагирования на компьютерные инциденты/группами реагирования на инциденты в области кибербезопасности (CERT/CSIRT) (например, авиационными ISAC, группой реагирования на компьютерные инциденты Европейской системы организации воздушного движения (EATM-CERT), национальными CERT/CSIRT).

2.3 Ресурсы

Организация должна определить ресурсы, необходимые для надлежащей реализации ПОК, в том числе:

- кадровые ресурсы: привлекайте сотрудников существующих подразделений по кибербезопасности, например центра обеспечения безопасности (SOC), по мере необходимости нанимайте новых сотрудников;
- технические ресурсы: сайт, электронная почта, телефон, текстовые сообщения, а также защищенные и/или надежные платформы для обмена информацией;
- финансовые ресурсы: расходы, связанные с закупкой и/или разработкой систем, подготовкой кадров и т. д.

2.4 Внедрение

Внедрение ПОК включает в себя следующие этапы:

- оценка сферы охвата работ – определение источников информации и киберинформации, подлежащей обмену через ПОК;
- определение инструментов, которые будут использоваться для обмена киберинформацией;
- выбор координатора сети обмена киберинформацией и разработка процедуры хранения информации;
- тестирование систем и процессов обмена киберинформацией и их корректировка по мере необходимости;
- введение в строй (ввод в эксплуатацию) механизма обмена киберинформацией;
- непрерывное наблюдение и контроль;
- постоянный пересмотр и совершенствование.

3. УПРАВЛЕНИЕ КИБЕРИНФОРМАЦИЕЙ И ОБМЕН ЕЮ

3.1 Типы киберинформации

Следующими видами киберинформации можно обмениваться.

КИБЕРРАЗВЕДДАННЫЕ

- **Разведданные о киберугрозах (CTI)**: сюда относится картина киберугроз, разведданные о целях хакеров и т. д.
  - **Данные стратегического характера**: стратегическая информация помогает организации понять природу киберугроз, а также возможности и мотивы злоумышленников.
    - Помогает сформировать общее понимание намерений и возможностей субъектов, представляющих киберугрозу.
    - Помогает принимать решения и/или служит источником раннего оповещения.
    - Может включать в себя описание тенденций (например, целей, поведения злоумышленников), статистику, информацию, связанную с киберугрозами (например, серьезные сохраняющиеся угрозы (APT), отчеты о киберинцидентах, директивные документы, неофициальные/научные документы) и т. д.
    - *Примером стратегических разведданных о киберугрозах является комплексный отчет о новых киберугрозах для критически важной инфраструктуры государства, в котором описываются потенциальные уязвимые места и векторы атак. Этот отчет обычно используется высокопоставленными лицами, принимающими решения, при определении долгосрочной политики и стратегии кибербезопасности.*
  - **Данные оперативного характера:**
    - Описывают контекст киберинцидентов, позволяя защитникам выявлять любые возможные источники опасности.
    - Позволяют выявлять потенциальное влияние киберинцидентов на рабочие процессы (например, тактику, приемы и процедуры (TTP), мотивы, последствия, сроки).
    - Помогают распределять ресурсы и ранжировать задачи по приоритетности.
    - *Примером оперативных данных является информация о продолжающейся фишинговой атаке, мишенью которой является авиация. К ним относятся такие подробности, как TTP, используемые злоумышленниками. Такая информация представляет ценность для сотрудников служб обеспечения безопасности, поскольку позволяет обнаруживать непосредственные киберугрозы и реагировать на них.*
  - **Данные тактического характера**: разведданные, используемые организациями для работы на упреждение при разработке систем безопасности, способных противостоять атакам (например, признаки несанкционированного доступа (IoC), TTP, уязвимости).
    - *Примером тактических разведданных являются признаки несанкционированного доступа, связанные с конкретной разновидностью вредоносного ПО. Сюда относятся конкретные IP-адреса, контрольные суммы файлов и сценарии поведения,*

характерные для вредоносного ПО. Такая информация тактического характера используется аналитиками первого звена по вопросам кибербезопасности для выявления и смягчения последствий киберугроз в режиме реального времени.

- **Признаки несанкционированного доступа (IoC)**. Признаки несанкционированного доступа – это, например, вредоносные IP-адреса, вредоносные URL-адреса, вредоносные доменные имена или контрольные суммы вредоносного ПО.
  - Обмен этой информацией поможет принимающим сторонам лучше защищать свои системы/сервисы.
  - При обмене информацией о признаках несанкционированного доступа нет необходимости раскрывать личность тех, кто их обнаружил.

- **Тактика, методы и процедуры (TTP)**. TTP – это сценарии атак и излюбленные методы хакеров[7].

- **Уязвимости**:
  - **Со стороны пользователя киберактива**: следует сообщать киберинформацию, в основном, связанную с киберактивами (например, аппаратным обеспечением, программным обеспечением, услугами, протоколами, стандартами), в которых была обнаружена уязвимость. Нет смысла обмениваться информацией о личности пользователя киберактива.
    - Такая информация может быть передана другим сторонам с целью помочь им защитить себя.
    - Нет необходимости во всех подробностях раскрывать личность того, кто обнаружил уязвимость.
    - Что касается ответственного раскрытия уязвимостей, то в рамках программы управления уязвимостями организации может быть создан своего рода "зал славы" или аналогичная инициатива для признания заслуг людей в деле выявления уязвимостей.
  - **Со стороны владельца киберактива**: владельцу киберактива следует сообщать об уязвимостях его пользователям.
    - Владелец данного киберактива должен выпустить устраняющее уязвимость обновление / решение проблемы.
    - Передовая практика включает в себя обмен информацией об этих уязвимостях с CERT/CSIRT (национальными или отраслевыми) для поддержки их мер реагировании на любые киберинциденты, связанные с рассматриваемым киберактивом.
  - Можно рассмотреть разницу между потенциальными, подтвержденными и использованными уязвимостями с точки зрения того, как организовать обмен информацией об этих уязвимостях.

ОТЧЕТ О КИБЕРИНЦИДЕНТЕ

- В нем содержится информация о киберинциденте, затрагивающем организацию.
- По возможности в отчеты о киберинцидентах должна быть включена следующая информация: краткое описание, тип, точная дата и время происшествия, место происшествия, продолжительность, хронология (т. е. последовательность событий), IOC, TTP, контекст, уязвимость (уязвимости),

[7] Компания MITRE ATT&CK разработала и ведет классификацию TTP, которую можно найти на их сайте: https://attack.mitre.org/

последствия (с точки зрения безопасности полетов, авиационной безопасности, эффективности, потенциала, бизнеса, финансов, репутации), серьезность, мотивация, цель, субъект угрозы, затронутые услуги и организация (организации) и т. д.
- Как правило, чем больше информации предоставлено, тем полезнее отчет.

УСТРАНЕНИЕ ПОСЛЕДСТВИЙ КИБЕРУГРОЗ

- Здесь содержится информация о методах:
  - устранения уязвимостей;
  - устранения последствий киберугроз;
  - реагирования на киберинциденты и восстановления после них.
- К распространенным форматам такой информации относятся обновления, устраняющие уязвимости, обновления антивируса для блокировки уязвимостей и инструкции по очистке сетей от вредоносного ПО.

СИТУАЦИОННАЯ ОСВЕДОМЛЕННОСТЬ

- Сюда относится информация, которая предоставляется лицам, принимающим решения, телеметрия в режиме реального времени об используемых уязвимостях, активных угрозах и кибератаках, которые могут потребоваться для реагирования на киберинцидент.
- Здесь также может содержаться информация о целях атак и состоянии критически важных открытых или частных компьютерных сетей.

ПЕРЕДОВАЯ ПРАКТИКА

- Сюда относится информация о том, как разрабатывается и поставляется программное обеспечение и услуги, например о механизмах управления работой системы безопасности, методах разработки и реагирования на инциденты, а также об установке устраняющих уязвимости обновлений или показателях эффективности программного обеспечения.

3.2 Отправители, получатели и источники киберинформации

- Для обмена киберинформацией требуются отправитель, получатель и источник информации (если информация исходит не от отправителя).
- В таблице ниже приведены примеры отправителей, получателей и источников киберинформации в гражданской авиации.

Отправители/получатели	• Пользователи воздушного пространства (например, авиакомпании, авиация общего назначения, эксплуатанты беспилотных авиационных систем (БАС)) • Поставщики аэронавигационного обслуживания (ПАНО) • Эксплуатанты аэропортов • Полномочные органы (например, ведомства гражданской авиации (ВГА)) • Поставщики авиационных услуг • Производители • Авиационные и неавиационные предприятия цепочки поставок • Прочие субъекты
Источники	• Отправители/получатели, перечисленные выше • Воздушные суда (например, БАС, самолеты) • Источники разведданных из открытых источников (OSINT) • Поставщики информации о киберугрозах • Международные ассоциации и организации (например, ассоциации авиакомпаний/аэропортов/ПАНО) • Международные/национальные/региональные центры авиационной кибербезопасности и авиационные CERT/ISAC • Прочие субъекты

- В добавлении A приводится рекомендуемый список типов киберинформации, которая может быть передана различным заинтересованным сторонам в авиации.

3.3 Оценка киберинформации, ее анализ и маркировка по протоколу "Светофор" (TLP) со стороны отправителя

3.3.1 Оценка и анализ

Прежде чем делиться киберинформацией, отправитель должен проанализировать ее по следующим критериям:

- оценить достоверность и надежность источника (см. п. 3.3.1.1 и добавления B и D);
- проанализировать правдоподобность и достоверность информации (см. п. 3.3.1.2 и добавления C и D);
- проанализировать актуальность информации для своей организации, других организаций, участвующих в обмене информацией (получающих информацию), и авиационной системы.

Этот шаг имеет решающее значение для обмена киберинформацией. Без этого информация превращается просто в набор вырванных из контекста данных и выводов.

При проведении вышеуказанного анализа важно помнить о том, что:

- разные аналитические задачи требуют разных подходов;
- аналитикам следует помнить о свойственных им субъективных суждениях и прилагать как можно больше усилий для их преодоления путем проведения объективного анализа с использованием соответствующих методов и инструментов.

Чтобы проиллюстрировать роль оценки и анализа киберинформации, на рис. 2 и 3 ниже показана разница между информацией из открытых источников и разведданными на

основе открытых источников, из чего становится очевидно, что удобство использования информации значительно возрастает при надлежащем анализе и проверке перед распространением.

- **OSINF (информация из открытых источников) –** собранная информация распространяется в исходном виде.

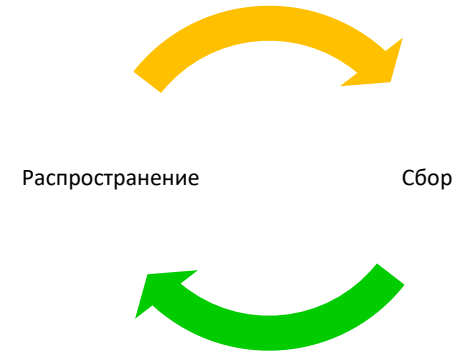

Рис. 2. Информация из открытых источников

- **OSINT (разведданные на основе открытых источников) –** после сбора информация подвергается описанному ниже процессу обработки.

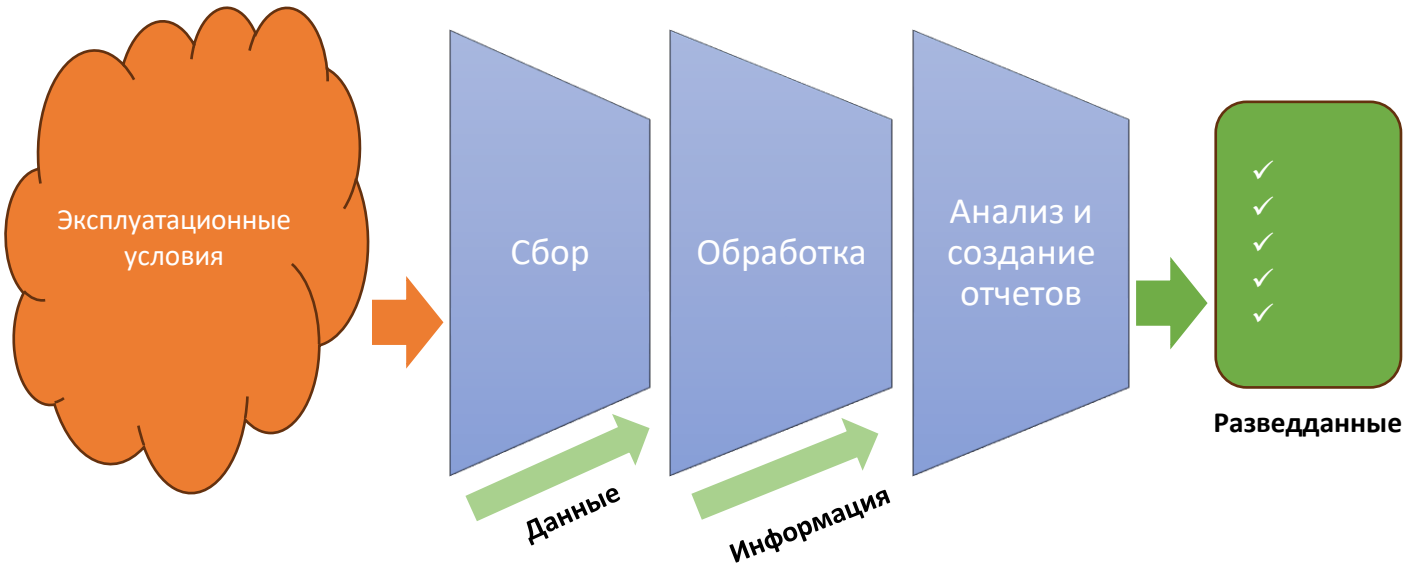

Рис. 3. Подготовка киберразведданных[8]

3.3.1.1 Оценка достоверности и надежности источника

Оценка уровня достоверности и надежности источника киберинформации/ разведданных имеет решающее значение для принятия взвешенных решений.

В добавлении B приведен пример механизма определения критериев и предложена схема оценки для измерения достоверности и надежности источника киберинформации/разведданных.

Весовые коэффициенты и шкала оценок, используемые в добавлении B, могут быть скорректированы в соответствии с требованиями конкретной организации и с учетом предельно допустимого для нее уровня риска.

В добавлении D приводится еще один пример схемы оценки уровня доверия к информации для оценки как надежности источника, так и достоверности информации (см. п. 3.3.1.2 ниже) с использованием другого метода: "кодекса Адмиралтейства" (или системы НАТО).

Организациям следует регулярно пересматривать и обновлять оценки уровня доверия по мере изменения картины киберугроз и источников информации об угрозах.

3.3.1.2 Анализ правдоподобности/достоверности киберинформации

Оценка уровня правдоподобности/достоверности киберинформации/разведданных имеет принципиальное значение.

В добавлении C приведен пример механизма определения критериев и предложена схема оценки для измерения правдоподобности и достоверности киберинформации/разведданных.

[8] Адаптированные материалы из совместной публикации 2-0, *Joint Intelligence* ("Совместная разведка") (2013 год).

Весовые коэффициенты и шкала оценок, используемые в добавлении C, могут быть скорректированы в соответствии с требованиями конкретной организации и с учетом предельно допустимого для нее уровня риска.

Организациям следует регулярно пересматривать и обновлять оценки правдоподобности/достоверности по мере поступления новой информации/разведданных и изменения картины киберугроз.

В добавлении D приводится еще один пример схемы оценки уровня доверия к информации для оценки как надежности источника (см. п. 3.3.1.1 выше), так и достоверности информации с использованием другого метода: "кодекса Адмиралтейства" (или системы НАТО).

3.3.2 Маркировка по протоколу "Светофор" (TLP)[9,10]

3.3.2.1 Использование протокола TLP в авиации

Протокол TLP включает в себя пять видов маркировки: КРАСНЫЙ, ЖЕЛТЫЙ, ЖЕЛТЫЙ+СТРОГИЙ, ЗЕЛЕНЫЙ и БЕСЦВЕТНЫЙ.

Поскольку маркировка **TLP:БЕСЦВЕТНЫЙ** никоим образом не ограничивает распространение полученной информации по каким бы то ни было каналам, а маркировка **TLP:КРАСНЫЙ** ограничивает раскрытие информации исключительно конкретным получателем (получателями) без возможности дальнейшего распространения, то эти две маркировки не обсуждаются в этом разделе. Три вида маркировки, которые требуют некоторых пояснений в плане того, как их применять в авиационном контексте, это:

- **TLP:ЗЕЛЕНЫЙ**
- **TLP:ЖЕЛТЫЙ**
- **TLP:ЖЕЛТЫЙ+СТРОГИЙ**

TLP:ЗЕЛЕНЫЙ	- Информация, помеченная как TLP:ЗЕЛЕНЫЙ, может распространяться в рамках авиационного сообщества. - Получатель информации, маркированной TLP:ЗЕЛЕНЫЙ, может в дальнейшем распространять ее среди любых авиационных организаций (ВГА, ПАНО, эксплуатанты аэропортов, пользователи воздушного пространства, производители, поставщики авиационных услуг и т. д.). - Она также может быть передана тем организациям, отвечающим за обеспечение кибербезопасности, которые взаимодействуют с авиационным сектором (национальные центры кибербезопасности, национальные/региональные/ международные авиационные CERT/CSIRT, авиационные ISAC и т. д.).

[9] Протокол "Светофор" (TLP) — это стандарт, разработанный компанией FIRST (Форум групп оперативного реагирования и обеспечения безопасности) для упрощения обмена информацией с соответствующей аудиторией. В этом документе содержатся рекомендации по использованию версии 2.0 стандарта TLP, с которыми можно ознакомиться по следующей ссылке: https://www.first.org/tlp/.

[10] Руководство, содержащееся в настоящем документе, заменяет собой "Руководство по протоколу 'Светофор'", опубликованное ИКАО в 2021 году.

	- Кроме того, она может быть передана неавиационным организациям, использующим аналогичные технологии (например, информацию, связанную с операционными или информационными технологиями), сталкивающимся с аналогичными киберугрозами или предоставляющим услуги для авиации (например, телекоммуникационные системы или услуги, энергетические системы или услуги). Эти неавиационные организации могут относиться к другим секторам (например, эксплуатанты, полномочные органы, производители) или организациям, связанным с кибербезопасностью (национальные центры кибербезопасности, CERT/CSIRT, относящиеся к другим секторам, ISAC других секторов).

TLP:ЖЕЛТЫЙ	- Информация, помеченная как TLP:ЖЕЛТЫЙ, допускает раскрытие **при наличии служебной необходимости** в рамках организации получателя и среди ее клиентов. - Хотя значение термина "организация" самоочевидно, в случае с авиацией значение термина "клиенты", имеющие **"служебную необходимость"**, следует толковать следующим образом: ○ ВГА могут обмениваться такой информацией: ▪ в пределах своего государства с: • заинтересованными сторонами из числа субъектов национальной авиационной системы; • национальным центром (национальными центрами) кибербезопасности; • национальными авиационными CERT/CSIRT и ISAC. ▪ вне пределов своего государства с: • другими ВГА; • национальными/региональными/ международными авиационными CERT/CSIRT и ISAC. ○ Заинтересованные стороны в авиации (ПАНО, эксплуатанты аэропортов, пользователи воздушного пространства, поставщики авиационных услуг) могут обмениваться такой информацией с: ▪ их национальными ВГА; ▪ организациями, помогающими им с оказанием услуг; ▪ национальными/региональными/ международными авиационными CERT/CSIRT и ISAC; ▪ их клиентами за исключением пассажиров (например, туристическими агентствами, магазинами беспошлинной торговли). ○ Производители могут делиться такой информацией с: ▪ национальными ВГА; ▪ своими клиентами (например, авиакомпаниями, аэропортами);

	▪ национальными/региональными/ международными авиационными CERT/CSIRT и ISAC; ▪ их субподрядчиками.
TLP: ЖЕЛТЫЙ+СТРОГИЙ	- Информация, помеченная как TLP:ЖЕЛТЫЙ+СТРОГИЙ, допускает раскрытие **при наличии служебной необходимости** только в рамках организации получателя.

3.3.2.2 Рекомендуемая маркировка различной киберинформации по TLP

В авиации рекомендуется руководствоваться следующими инструкциями при маркировке киберинформации. Некоторые соображения могут привести к необходимости отклониться от приведенных ниже рекомендаций, включая, помимо прочего, следующие:

- Маркировка TLP может меняться с течением времени: киберинформация может быть помечена как более закрытая при ее первом распространении, а затем ее маркировка может быть пересмотрена в сторону снижения степени секретности, поскольку риск, связанный с информацией, снижается при более массовом ее раскрытии.
- Мнения государства и отрасли по поводу маркировки: правила маркировки киберинформации, принятые в государстве, могут отличаться от таковых у заинтересованных сторон в авиации в силу разных соображений (например, ограничений по соображениям национальной безопасности).
- Национальные ограничения, применимые к отрасли: государство может иметь специальную маркировку для определенного типа информации, которая применяется к критической национальной инфраструктуре (например, первоначальное раскрытие таких IOC, как подозрительные IP-адреса).

КИБЕРРАЗВЕДДАННЫЕ

- **Разведданные о киберугрозах (CTI)**:
  - **Стратегические данные:** зависят от характера стратегических CTI и получателей (например, совет директоров, высшее руководство, аналитики CTI, специалисты по расследованию нарушений безопасности)
    - **TLP:КРАСНЫЙ:** конкретные и предельно конфиденциальные разведданные о конкретной киберугрозе, мишенью которой является организация. О них должно быть осведомлено ограниченное число лиц, принимающих конкретные решения.
    - **TLP:ЖЕЛТЫЙ:** высшее руководство, члены совета директоров или принимающих решения комитетов должны быть осведомлены о конкретной киберугрозе, нацеленной на организацию, имеющей отношение к авиации (например, цепочка поставок, подключенная заинтересованная сторона) и/или относящейся к критической национальной инфраструктуре.
    - **TLP:ЗЕЛЕНЫЙ:** информация, которой следует делиться с сообществом, чтобы обеспечить широкую осведомленность и принятие соответствующих мер (например, директивные документы, технические доклады, тенденции, статистика).

- **Оперативные данные:**
  - **TLP:КРАСНЫЙ:** для конкретных оперативных, технических сотрудников и сотрудников службы безопасности, которым необходимо действовать, полагаясь на конкретные разведданные о конкретной киберугрозе или инциденте, направленных против соответствующих авиационных заинтересованных сторон или критической национальной инфраструктуры (например, цепочки поставок, подключенной заинтересованной стороны).
  - **TLP:ЖЕЛТЫЙ:** для оперативных, технических сотрудников и сотрудников службы безопасности, которым необходимо быть в курсе конкретной киберугрозы или инцидента, направленных против организации или имеющих отношение к авиации или критической национальной инфраструктуре.
  - **TLP:ЗЕЛЕНЫЙ:** информация, которой следует делиться с сообществом, чтобы обеспечить широкую осведомленность и принятие соответствующих мер.
- **Тактические данные:**
  - **TLP:КРАСНЫЙ:** для конкретных сотрудников службы безопасности и технических сотрудников, которым необходимо реагировать на конкретную киберугрозу, направленную против организацию, или которым необходимо быть в курсе текущего киберинцидента.
  - **TLP:ЖЕЛТЫЙ:** для технических сотрудников и сотрудников службы безопасности, которым необходимо быть в курсе киберугрозы или продолжающегося киберинцидента или сохраняющейся уязвимости, направленных против организации или имеющих отношение к авиации или критической национальной инфраструктуре.
  - **TLP:ЗЕЛЕНЫЙ:** информация, которой следует делиться с сообществом, чтобы обеспечить широкую осведомленность и принятие соответствующих мер.

- **IOC: TLP:ЗЕЛЕНЫЙ**
- **TTP: TLP:ЗЕЛЕНЫЙ**
- **Уязвимости:**
  - Использованная уязвимость: **TLP:КРАСНЫЙ**
  - Подтвержденная уязвимость (с устраняющим проблему обновлением или без него): **TLP:ЖЕЛТЫЙ**
  - Потенциальная уязвимость без устраняющего проблему обновления: **TLP:ЖЕЛТЫЙ**
  - Потенциальная уязвимость с устраняющим проблему обновлением: **TLP:ЗЕЛЕНЫЙ**

ОТЧЕТ О КИБЕРИНЦИДЕНТЕ

- Никаких рекомендаций по этому вопросу нет, поскольку все зависит от характера, обстоятельств и времени инцидента (то есть времени, прошедшего

между киберинцидентом и обменом информацией). **TLP:БЕСЦВЕТНЫЙ** может быть исключен на ранних стадиях, хотя через какое-то время такая маркировка может применяться.

3.4 Оценка и анализ информации со стороны получателя

Получатель киберинформации должен проанализировать полученную информацию, чтобы установить:

1. **Уровень доверия к ней / ее надежность / ее качество**: уровень доверия[11] к киберинформации может быть сочтен недостаточным для того, чтобы на ее основании инициировать какие-либо действия со стороны получателя.
2. **Актуальность**: примером актуальности является ситуация, когда получатель не может действовать на основе информации (например, в отсутствие служебной необходимости), хотя информация актуальна для другого сотрудника в организации. Это может стать помехой, если полученная информация маркирована как **TLP:КРАСНЫЙ**. В этом случае получатель должен связаться с отправителем, чтобы либо получить согласие отправителя на пересылку информации соответствующему получателю (получателям) путем получения версии информации с более низкой маркировкой, либо связать отправителя с другим контактным лицом в организации для получения версии информации с маркировкой **TLP:КРАСНЫЙ**.
3. **Прикладной характер**: маркировка TLP может помешать получателю предпринять какие-либо действия на основе информации и потребовать дальнейшего согласования действий отправителя и получателя, с тем чтобы принять какие-либо меры на основе полученной информации. Например:
    - Если информация маркирована как **TLP:КРАСНЫЙ** и получателю необходимо взаимодействовать с другими членами организации, чтобы принять меры на ее основе, но заинтересованные лица не получили такую же информацию.
    - Если информация маркирована как **TLP:ЖЕЛТЫЙ+СТРОГИЙ** и получателю необходимо взаимодействовать с другой организацией, чтобы принять меры в соответствии с распространяемой информацией.

Анализ предполагает также следующие шаги:

- Получатель должен объединить полученную киберинформацию с имеющимися разведданными (например, сравнить и/или рассмотреть ее в совокупности с другой информацией). Это поможет повысить или понизить уровень доверия к этой информации.
- Получатель должен рассмотреть информацию в контексте своих обязанностей, что позволит оценить значимость информации для получателя в политическом, стратегическом, оперативном, техническом контексте и/или контексте кибербезопасности.

3.5 Доверительные отношения между сторонами

Доверие — это меняющееся с течением времени и многогранное понятие, которое имеет большое значение для безопасного обмена конфиденциальной информацией. Это не абсолютное, а относительное понятие, которое меняется в зависимости от контекста, отношений и поведения.

Установление доверительных отношений между отправляющей и принимающей сторонами имеет решающее значение для эффективного обмена киберинформацией.

[11] См. пп. 3.3.1.1, 3.3.1.2 и добавления B, C и D.

Также могут потребоваться доверительные отношения с непривычными партнерами или заинтересованными сторонами. Важно определить ключевые стороны для упреждающего обмена киберинформацией или обмена ею в порядке реагирования на ситуацию, чтобы обеспечить своевременное и актуальное распространение.

Доверительные отношения могут установиться с различными партнерами и заинтересованными сторонами. Примеры таких доверительных отношений:

- В рамках авиации:
  - между государственными органами (на национальном и/или международном уровне);
  - между государственными органами и авиационными организациями и наоборот;
  - между отраслевыми организациями;
  - между государственными органами или авиационными организациями и международными организациями (например, ИКАО) и наоборот.
- С партнерами и заинтересованными сторонами, не относящимися к авиации:
  - неправительственные организации;
  - некоммерческие организации;
  - международные организации (например, соответствующие учреждения Организации Объединенных Наций);
  - Международная организация уголовной полиции – ИНТЕРПОЛ.

Установление доверительных отношений обычно требует времени. Государства и заинтересованные стороны могут устанавливать, развивать и укреплять доверительные отношения посредством:

- создания альянсов с партнерами-единомышленниками;
- регулярной деятельности: участия в периодических встречах или конференциях;
- соглашений: в следующих двух разделах содержатся рекомендации по типам соглашений, которые могут быть разработаны для обмена киберинформацией.

Государствам и заинтересованным сторонам следует также учитывать преимущества (см. раздел 1.1) и затраты, связанные с установлением и поддержанием доверительных отношений, чтобы обосновать и принять решение об инвестициях, необходимых для таких усилий. К таким соображениям следует отнести:

- время: сколько времени требуется на установление и развитие отношений;
- ресурсы: в том числе кадровые и финансовые;
- преимущества: что получает от отношений каждая из сторон;
- обязательства: потенциальные убытки для каждой из сторон при наличии отношений;
- поддержание: следует также принимать во внимание текущие затраты на поддержание отношений с точки зрения времени и ресурсов.

Поддержание доверительных отношений включает в себя такие действия, как:

- Очные и виртуальные встречи: частота встреч согласовывается между сторонами. Рекомендуется проводить их по мере необходимости, а личные встречи – не реже одного раза в год, с учетом уровня участвующего персонала (старший, средний или технический уровень).
- Упреждающий обмен киберинформацией: частый обмен информацией в зависимости от потребностей и приоритетов. Эта информация может включать:
  - изменения политики и процедур, которые могут коснуться получателя (получателей);
  - продукция: сводки с места событий, стратегический анализ и т. д.;
  - необработанная информация: исходные коды, журналы событий и т. д.
- Обмен киберинформацией при реагировании на события: может включать обмен информацией, связанной с реагированием на киберинцидент:

- во время киберинцидента: обмен информацией в режиме реального времени и последовательность действий по ходу инцидента;
- после киберинцидента: обмен информацией о результатах, первопричинах, накопленном опыте и т. д.

Доверительные отношения могут прекратиться в случае утраты доверия. Примеры действий, которые могут привести к такому результату:

- несанкционированное раскрытие засекреченной информации: случайное или преднамеренное раскрытие засекреченной информации, которая может иметь значение для национальной безопасности или собственников информации, не имеющим на то полномочий лицам или организациям;
- преднамеренный обмен конфиденциальной информацией: намеренный обмен конфиденциальной информацией о безопасности или конфиденциальной служебной информацией с отдельными лицами или организациями в целях выявления уязвимостей или нанесения ущерба репутации, особенно если это происходит публично.

3.5.1 Официальные соглашения

Обмен киберинформацией между сторонами может быть оформлен в виде двусторонних или многосторонних, обязательных или добровольных соглашений.

В таких соглашениях участвуют разные типы сторон. Так, соглашения могут быть разработаны между государствами, государственными учреждениями (например, между ведомством гражданской авиации и национальным органом по кибербезопасности в одном государстве), между государственными учреждениями разных государств (например, между ведомствами гражданской авиации разных государств), между государственным учреждением и заинтересованными сторонами в авиации в рамках одного государства, между государственным учреждением и заинтересованными сторонами в отрасли в другом государстве и/или между заинтересованными сторонами в авиации.

В добавлении E приведен рекомендуемый список разделов, которые должны быть включены в официальное соглашение об обмене киберинформацией, чтобы обеспечить четкое распределение ролей и обязанностей сторон, обменивающихся киберинформацией, что со временем положительно отразится на уровне доверия между сторонами.

3.5.2 Неофициальные соглашения

Неофициальные соглашения часто используются, когда доверительные отношения между обменивающимися информацией сторонами уже установились или подразумеваются по умолчанию. Такие соглашения следует использовать с осторожностью, поскольку они не влекут за собой никаких юридических обязательств для подписавших их сторон. Они не должны быть основным или единственным механизмом обмена киберинформацией.

Такие соглашения содержат ограниченный набор информации, необходимый сторонам для обмена информацией, например:

- технические средства, которые будут использоваться для обмена информацией;
- соответствующие контактные лица (отдельные сотрудники и подразделения в целом).

Строгое и последовательное использование маркировки TLP особенно важно при обмене киберинформацией в рамках неофициальных соглашений для сохранения и укрепления существующего уровня доверия между сторонами.

4. СТРУКТУРИРОВАНИЕ, ПЕРЕДАЧА И АРХИВИРОВАНИЕ КИБЕРИНФОРМАЦИИ

4.1 Структурирование киберинформации перед обменом

Киберинформацию следует упорядочивать на основе определенной классификации или структуры, с тем чтобы при ее распространении обеспечивалось наличие соответствующего контекста, а также полезных и важных для прикладной работы подробностей.

Ниже приведен пример того, как следует структурировать киберинформацию для обмена:

- название: общее описание киберинформации;
- справочный номер: для отслеживания информации отправителем;
- маркировка TLP;
- основные аспекты, в том числе:
    - категория (например, кибершпионаж, киберпреступность, информационные операции);
    - тип (например, уязвимость, ботнет, слежка, личные данные, социальные сети, утечка учетных данных, фишинг, DDoS-атака, вредоносное ПО);
    - уровень киберугрозы (например, критический, высокий, средний, низкий);
    - область/сектор;
    - надежность источника информации и степень доверия к нему (см. п. 3.3.1.1);
- ключевые моменты: перечень, содержащий кратко изложенную пояснительную информацию;
- резюме;
- атрибуция: субъект(ы) угрозы, которые потенциально или фактически могли быть идентифицированы в качестве исполнителей;
- оценка последствий, целей, жертв и т. д.;
- рекомендуемые действия, которые необходимо предпринять получателю(ям);
- прикладная информация:
    - пострадавшие киберактивы;
    - хронология событий;
    - IoC;
    - правила обнаружения;
    - TTP;
- устранение последствий:
    - общие меры по устранению последствий;
    - адресные меры по устранению последствий;
- справочные материалы.

4.2 Передача киберинформации

В данном разделе содержится инструктивный материал по преимуществам и недостаткам использования различных каналов обмена киберинформацией.

4.2.1 Телефон

Такой канал связи подходит для информации, маркированной как **TLP:КРАСНЫЙ**, поскольку обеспечивает связь в режиме реального времени с лицом, которому предполагается передать информацию. Он также помогает передавать важную информацию, требующую немедленных мер.

При использовании телефона для обмена киберинформацией рекомендуется предусмотреть средства контроля, обеспечивающие установление личности обеих сторон (например, во избежание использования аудиозаписей, созданных при помощи искусственного интеллекта).

В целом этот канал связи имеет ограниченное применение (используется в основном для обмена срочной и/или маркированной как **TLP:КРАСНЫЙ** киберинформацией), и поэтому его следует рассматривать в сочетании с другими средствами обмена киберинформацией.

4.2.2 Обычная электронная почта

Киберинформация может быть передана в виде обычного текста в электронном письме.

Использование этого средства для обмена киберинформацией означает, что:

- получатель должен открыть письмо и прочитать информацию;
- необходим анализ содержания письма аналитиком CTI, который сможет оценить его актуальность для получателя;
- первоначально информация будет обрабатываться вручную.

Ниже приведены некоторые ограничения на использование обычной электронной почты для обмена киберинформацией:

- этот канал связи подходит для небольших объемов текстовой информации;
- некоторые системы электронной почты могут заблокировать письмо, поскольку оно может содержать IoC, что приведет к срабатыванию средств контроля информационной безопасности;
- сложно вести актуальные списки адресов электронной почты. Рекомендуется использовать личные и общие адреса электронной почты;
- информация с пометкой **TLP:КРАСНЫЙ** не может быть отправлена на общие адреса электронной почты (например, groupmailbox@company.com), а только на личные (например, someone@company.com);
- некоторые типы адресов электронной почты не могут считаться доверенными получателями (например, неслужебные адреса электронной почты, размещенные на коммерческих почтовых серверах, таких как gmail, hotmail, yahoo и т. д.);
- существует риск подмены пользователя электронной почты. Поэтому для снижения этого риска рекомендуется использовать соответствующие методы подтверждения подлинности, например цифровую подпись электронной почты.

4.2.3 Электронное письмо с вложением

Кибериформация может быть передана в виде документа, приложенного к электронному письму. Вложение может быть зашифровано паролем, который можно отправить получателю по другому надежному каналу (например, в текстовом сообщении, защищенном приложении для обмена сообщениями).

Использование этого средства для обмена киберинформацией означает, что:

- получатель должен открыть вложение и прочитать информацию;
- необходим анализ содержания письма аналитиком CTI, который сможет оценить его актуальность для получателя;
- первоначально информация будет обрабатываться вручную.

Ниже приведены некоторые ограничения на использование электронного письма с вложением для обмена киберинформацией:

- существует риск открыть вредоносное вложение, поэтому вложение должно сначала пройти проверку;
- некоторые почтовые системы блокируют определенные типы вложений (например, архивированные файлы с расширениями .zip, .rar и .7z);
- некоторые системы электронной почты могут заблокировать доступ к документу, поскольку в нем могут содержаться IoC, что приведет к срабатыванию средств контроля информационной безопасности;
- размер вложения может помешать его передаче по электронной почте;
- сложно вести актуальные списки адресов электронной почты. Рекомендуется использовать личные и общие адреса электронной почты;
- информация с маркировкой **TLP:КРАСНЫЙ** не может быть отправлена на общие адреса электронной почты (например, groupmailbox@company.com), а только на личные (например, someone@company.com).

4.2.4 Частное хранилище данных

Обмен киберинформацией может осуществляться через доступ к частному хранилищу данных, где содержится информация, которой необходимо поделиться.

В таком случае следует предусмотреть методы уведомления получателя (получателей) о появлении новой киберинформации, к которой можно получить доступ.

Процесс передачи уведомлений может быть автоматизирован с помощью электронной почты или других средств (например, текстовых сообщений, защищенных приложений для обмена сообщениями).

Доступ к хранилищу должен быть защищен, а защита – обеспечиваться постоянно:

- средства контроля/обеспечения безопасности должны использоваться в соответствии со степенью секретности информации, совместный доступ к которой предоставляется при помощи хранилища. Средства контроля могут включать место размещение хранилища данных (например, частный/общий сервер, облачный хостинг), контроль доступа/прав, методы установления личности пользователей (например, однократный вход (SSO), двухфакторная/ многофакторная аутентификация (2FA/MFA)) и т. д.;
- необходимо вести и постоянно перепроверять актуальный список организаций/лиц, имеющих право доступа к хранилищу;

- права доступа, например права на *чтение и запись*, должны быть предоставлены отдельным учетным записям и быть защищены;
- все сеансы доступа и действия, происходящие в хранилище, должны фиксироваться и анализироваться;
- киберинформация, размещенная в хранилище, должна быть тщательно разбита по папкам, поскольку не все участники имеют одинаковый доступ к информации. Более того, существует необходимость перемещать информацию между папками по мере того, как категория (например, маркировка TLP) информации меняется со временем (например, она может стать доступной для более широкой аудитории, если категория/уровень TLP-маркировки понижаются). Этот процесс может с течением временем осложниться, поскольку количество участников и объем информации, которой они делятся в хранилище, со временем растут.

4.2.5 Приложения

Для обмена киберинформацией можно использовать различные программные приложения (с открытым исходным кодом или проприетарные) (например, MISP, OpenCTI, CyWare и т. д.).

Не представляется возможным привести общий список соображений относительно использования приложений как таковых, поскольку все зависит от характера приложения (например, идет ли речь о приложении с открытым исходным кодом или о проприетарном приложении), от того, кто отвечает за разработку и обновление средств контроля за обеспечением безопасности, права доступа, каталогизацию информации (например, выполняется ли она вручную или автоматически с помощью правил), хранения конфиденциальной информации (например, на защищенных/частных или открытых серверах) и т. д. Поэтому рекомендуется оценить все эти и другие аспекты при рассмотрении возможности использования приложений для обмена киберинформацией.

Что касается существующих приложений, то в добавлении F представлена информация о MISP – платформе для обмена информацией и разведданными на основе открытого исходного кода, поскольку эта платформа обладает интересными функциональными возможностями, которые могли бы быть полезны при обмене киберинформацией в авиационном секторе.

4.3 Архивирование киберинформации

После обмена киберинформация должна архивироваться как отправителем, так и получателем для целей учета и контроля качества.

При архивировании следует учитывать следующие аспекты:

- Нормативно-правовая база: необходимо учитывать нормативные акты, которыми может регулироваться архивирование информации (например, законы о конфиденциальности и их требования к архивированию определенных типов информации, а также максимально допустимый срок хранения информации в архиве).
- Носители информации: выбор носителя зависит от типа информации. Для архивирования киберинформации могут использоваться различные типы носителей. Например, отчеты о киберинцидентах могут храниться в отдельной базе данных, отчеты о киберугрозах – в виде файла на компьютерном диске и т. д.

- Контроль доступа и права: доступ к архивной киберинформации должен быть определен политикой, определяющей, кто может получить доступ к тому или иному типу информации. Это соответствует маркировке информации в TLP (например, **TLP:ЖЕЛТЫЙ+СТРОГИЙ** означает не всех сотрудников организации, а только тех, кому положено знать информацию исходя из служебной необходимости).
- Локальный и удаленный доступ: к некоторой киберинформации может быть запрещен любой внешний доступ (например, через интрасети), а доступ должен предоставляться только внутри организации. Это предполагает также определение привилегий прав доступа на основе ролей и обязанностей сотрудников, которые могут быть использованы для целей аудита/контроля.
- Средства контроля/защиты: в зависимости от типа информации следует применять различные уровни средств контроля и защиты. Так, для защиты отчетов о киберинцидентах должны применяться более строгие меры контроля, чем для защиты уже исправленных уязвимостей.
- Актуальность: часть киберинформации может устареть в связи с некоторыми изменениями. Например, это уязвимости уже не использующихся организацией систем, стратегические киберугрозы, связанные с уже прошедшими геополитическими событиями, и т. д.
- Удобство использования: необходимо определить различные категории архивов, чтобы поддерживать постоянное удобство использования информации. Например:
    - "горячие": включают последние данные, которые хранятся без сжатия файлов, что обеспечивает максимальную скорость доступа к ним и их обработки;
    - "теплые": включает данные, которые хранятся с небольшим сжатием, что обеспечивает очень высокую производительность при доступе и обработке в случае необходимости;
    - "холодные": включают данные, которые были архивированы и полностью сжаты, и для получения которых требуется ручное извлечение и распаковка.
- Продолжительность: срок хранения киберинформации в архиве должен зависеть от типа информации. Например, можно определить правила архивирования, согласно которым IoC должны храниться не более [X] лет. Кроме того, действия, связанные с удалением устаревшей информации, должны предприниматься в рамках процессов управления архивированием киберинформации.

5. ДАЛЬНЕЙШИЙ ОБМЕН КИБЕРИНФОРМАЦИЕЙ

5.1 Зачем нужен дальнейший обмен киберинформацией

Дальнейший обмен киберинформацией, полученной из внешнего источника, может потребоваться для того, чтобы обеспечить доступ к информации максимально широкой аудитории, для которой она востребована. Однако перед дальнейшим обменом киберинформацией следует тщательно взвесить все обстоятельства.

В качестве примера можно привести ситуацию, когда государственное ведомство получает информацию от ее автора, который разрешает дальнейший обмен ею только с организациями, с которыми у него есть официальное соглашение. По оценке государственного ведомства, другим государственным ведомствам, которые не имеют официального соглашения с автором информации, необходимо ознакомиться с этой информацией. В этом случае получатель информации должен связаться с ее автором и запросить его согласие на дальнейший обмен информацией с другими ведомствами, которым необходимо знать ее.

Для выяснения того, стоит ли и с кем стоит в дальнейшем делиться киберинформацией, получатель информации должен учитывать следующие факторы:

- Ограничения дальнейшего распространения: можно ли и нужно ли распространять эту информацию дальше? В случае сомнений (например, сомнений по поводу возможно неправильной маркировки TLP) получатель может запросить разрешение отправителя на дальнейший обмен информацией.
- Цель дальнейшего распространения информации и роль предполагаемого получателя.

Цель дальнейшего обмена киберинформацией связана с тем, какие действия ожидаются от получателя:

- Информирование/повышение осведомленности: у предполагаемого получателя есть служебная необходимость, и информация предоставляется только в информационных целях.
- Действия: у предполагаемого получателя есть служебная необходимость, и киберинформация передается для выполнения получателем конкретных действий. К таким действиям могут относиться:
  - Выделение или привлечение ресурсов для решения конкретной проблемы.
  - Выделение или привлечение ресурсов для смягчения последствий конкретной киберугрозы или уязвимости.
  - Выделение или привлечение ресурсов для оказания помощи при реагировании.

Роль предполагаемого получателя может учитываться при принятии решения о дальнейшем обмене киберинформацией. К числу получателей, которым может потребоваться информация, относятся, например:

- **Технические специалисты**: эксперт или специалист, отвечающий за обеспечение защиты сетей, систем, сервисов, приложений, IT/OT-инфраструктуры и т. д. от несанкционированного доступа.
- **Руководители профильных органов**: лица, разрабатывающие стратегии, политику, процедуры и/или процессы обеспечения кибербезопасности в авиации или для соответствующих неавиационных компаний, которые должны быть реализованы заинтересованными сторонами в авиации.
- **Высшее руководство**: высокопоставленные сотрудники, утверждающие ход реализации стратегий, политики, процедур и/или процессов обеспечения кибербезопасности в авиации или в соответствующих неавиационных отраслях.

- **Координатор**: эксперт или специалист по кибербезопасности, которому поручено должным образом направлять потоки полученной при обмене информации нужным сотрудникам.
- **Сотрудник по обеспечению безопасности полетов**: эксперт по безопасности полетов, который может также определить возможные последствия для безопасности, эффективности и/или пропускной способности авиации.
- **Сотрудник по авиационной безопасности**: эксперт по авиационной безопасности, который может также определить возможные последствия для авиационной безопасности.

5.2 Правила дальнейшего обмена киберинформацией

Правила дальнейшего обмена киберинформацией охватывают множество областей, которые следует тщательно изучить:

- Организация, которой в дальнейшем будет передана информация (например, государство/ авиационная заинтересованная сторона/ неавиационная заинтересованная сторона, национальный орган/международная организация).
- Роль получателя, которому в дальнейшем будет передана киберинформация.
- Передаваемая информация: весь объем киберинформации или ее часть (например, документ целиком или только соответствующие пункты).
- При каких обстоятельствах будет осуществляться обмен информацией: с упреждением или в порядке реагирования.
- Частота обмена информацией: регулярно или по мере необходимости.
- Причина обмена киберинформацией (например, для информирования или принятия мер).
- Обращение с киберинформацией: все первоначальные ограничения секретности и оговорки должны сохраняться при передаче по соответствующим каналам связи (т. е. по секретным и несекретным каналам связи).
- TLP-маркировка киберинформации не может изменяться при ее дальнейшем распространении.

5.3 Методы и носители для дальнейшего обмена информацией

Методы/носители, в определенных ситуациях используемые при дальнейшем обмене киберинформацией, должны быть безопасными и простыми в использования.

Физическая информация: информация, предоставляемая в печатном виде. Информация должна быть надлежащим образом упакована (например, в папку) и защищена (например, в папку, закрывающуюся на молнию или защелку) на время транспортировки к месту встречи и вплоть до передачи печатной копии (копий). Любые напоминания или оговорки, касающиеся обращения с информацией, должны быть отмечены на самих материалах или на титульном листе (например, порядок обращения с конфиденциальной информацией по авиационной безопасности (SSI) обычно помещается на титульный лист вместе с инструкциями)[12].

Информация в электронном виде: к дальнейшему обмену информацией применимы те же средства обмена киберинформацией, что упоминаются в разделе 4.2. При этом следует учитывать тот факт, что адресат, которому передается киберинформация, может не иметь доступа к некоторым электронным средствам, к которым имеет доступ

[12] В инструктивном материале по работе с конфиденциальной информацией по авиационной безопасности в разделе 2.3 *Руководства по авиационной безопасности ИКАО* (Doc 8973 - Restricted) содержится полезная информация, которая может быть использована в контексте обмена киберинформацией.

отправитель (например, внесенная в белый список электронная почта, портал/ хранилище, где находится информация).

Существуют дополнительные правила работы с секретной информацией, принятые в конкретном государстве или организации. Эти правила должны строго соблюдаться в соответствии с действующими правилами и процедурами.

— — — — — — — —

Добавление A

Рекомендуемая для обмена авиационная киберинформация в разбивке по типам данных

КИБЕРРАЗВЕДДАННЫЕ

- **Разведданные о киберугрозах (CTI):**
  - **Стратегическая информация:**
    - От государственных органов (национальный центр кибербезопасности, ВГА и т. д.) заинтересованным сторонам в авиации в пределах государства
    - От национального центра кибербезопасности авиационным CERT/ISAC
    - От авиационных CERT/ISAC заинтересованным сторонам в авиации
    - Между проверенными национальными центрами кибербезопасности
    - Между заслуживающими доверия государствами
  - **Оперативная информация**:
    - От одних заинтересованных сторон в авиации другим
    - От авиационных CERT/ISAC заинтересованным сторонам в авиации
    - От заинтересованных сторон в авиации государственным органам (национальный центр кибербезопасности, ВГА и т. д.) в пределах государства
  - **Тактическая информация:**
    - От одних заинтересованных сторон в авиации другим
    - От авиационных CERT/ISAC заинтересованным сторонам в авиации
    - От национального центра кибербезопасности авиационным CERT/ISAC
    - От национального центра кибербезопасности заинтересованным сторонам в авиации в пределах государства
    - От заинтересованных сторон в авиации государственным органам (национальный центр кибербезопасности, ВГА и т. д.)

- **IOC:**
  - От одних заинтересованных сторон в авиации другим
  - От авиационных CERT/ISAC заинтересованным сторонам в авиации
  - От национального центра кибербезопасности авиационным CERT/ISAC
  - От национального центра кибербезопасности заинтересованным сторонам в авиации в пределах государства
  - От заинтересованных сторон в авиации национальному центру кибербезопасности

- **TTP:**
  - От одних заинтересованных сторон в авиации другим
  - От авиационных CERT/ISAC заинтересованным сторонам в авиации

- От национального центра кибербезопасности авиационным CERT/ISAC
- От национального центра кибербезопасности заинтересованным сторонам в авиации в государстве
- От заинтересованных сторон в авиации национальному центру кибербезопасности

- **Уязвимости:**
  - От одних заинтересованных сторон в авиации другим
  - От заинтересованных сторон в авиации смежным предприятиям цепочки поставок
  - От исследовательских учреждений авиационным CERT/ISAC
  - От исследовательских учреждений государственным органам (национальный центр кибербезопасности, ВГА и т. д.)
  - От исследовательских учреждений заинтересованным сторонам в авиации
  - От исследовательских учреждений участникам цепочки поставок
  - От авиационных CERT/ISAC заинтересованным сторонам в авиации
  - От национального центра кибербезопасности авиационным CERT/ISAC
  - От национального центра кибербезопасности заинтересованным сторонам в авиации в государстве
  - От заинтересованных сторон в авиации профильным государственным органам (национальный центр кибербезопасности, ВГА и т. д.)

ОТЧЕТ О КИБЕРИНЦИДЕНТЕ

- Обязательные отчеты о киберинцидентах (в соответствии с действующим национальным законодательством и/или нормативными актами):
  - От заинтересованных сторон в авиации профильным государственным органам (национальный центр кибербезопасности, ВГА и т. д.) – в случае инцидентов, имеющих отношение к безопасности полетов и/или авиационной безопасности
  - От заинтересованных сторон в авиации правоохранительным органам (в случае конкретных типов инцидентов, связанных с киберпреступностью, например, мошенничеством, или с конкретными законами, например, законами о неприкосновенности частной жизни)
  - От государства в адрес ИКАО (в случае киберинцидентов, связанных с актами незаконного вмешательства)

- Добровольные отчеты о киберинцидентах:
  - От заинтересованных сторон в авиации национальному центру кибербезопасности
  - От одних заинтересованных сторон в авиации другим (особенно если между ними налажено взаимодействие)
  - От заинтересованных сторон в авиации авиационным CERT/ISAC

— — — — — — — —

Добавление B

Пример механизма оценки и ранжирования достоверности и надежности источника киберинформации/разведданных

1. Репутация и прошлый опыт взаимодействия:
   - Оцените историю взаимодействия и репутацию источника среди специалистов по кибербезопасности.
   - Узнайте о прошлом опыте успешного взаимодействий, вкладе и участии в работе отраслевых организаций.
   - Оцените опыт работы по предоставлению точной и своевременной информации/разведданных о киберугрозах.

2. Достоверность и компетентность:
   - Оцените квалификацию, сертификаты и компетентность людей или групп, ответственных за источник.
   - Учитывайте их опыт работы с конкретными видами информации/разведданных о киберугрозах.

3. Источники информации и методы ее сбора:
   - Изучите методы сбора и источники информации.
   - Установите наличие доступа к разнообразным и надежным источникам информации.
   - Оцените строгость процессов сбора данных.

4. Обмен данными и сотрудничество:
   - Определите, делится ли источник информацией/разведданными о киберугрозах с доверенными организациями или коллегами по отрасли.
   - Сотрудничество с другими организациями, занимающимися вопросами кибербезопасности, может повысить доверие к ним.

5. Транспарентность:
   - Оцените уровень прозрачности их отчетности и методологии.
   - Оцените, раскрывают ли они источники, методы анализа и частоту обновления данных.

6. Своевременность и точность:
   - Оцените способность источника своевременно и точно предоставлять информацию/разведданные о киберугрозах.
   - Изучите точность их прошлых прогнозов и эффективность обнаружения киберугроз.

7. Анализ и контекст:
   - Проанализируйте глубину и качество анализа киберугроз.
   - Оцените способность проанализировать контекст киберугроз, включая вопросы атрибуции и возможных последствий.

8. Соответствие отраслевым стандартам:
   - Определите, соответствует ли источник отраслевым стандартам и передовой практике в части работы с информацией/разведданными о киберугрозах, например, соблюдает ли требования рамочных механизмов, таких как STIX/TAXII, и общих форматов данных.

9. Соблюдение правовых и этических норм:
    - Убедитесь, что источник соблюдает правовые и этические нормы, касающиеся сбора и передачи данных.

Для оценки уровня доверия к источнику киберинформации/разведданных можно использовать схему оценок, основанную на вышеуказанных критериях.

Ниже приводится пример схемы оценки.

1. Присвойте каждому критерию весовой коэффициент в зависимости от его важности с точки зрения конкретных потребностей организации и параметров риска.
2. Оцените источник по шкале (например, от 1 до 5) по каждому критерию, где 5 – это наивысший уровень доверия.
3. Рассчитайте общий балл доверия, суммировав взвешенные оценки по каждому критерию. Более высокий балл указывает на источник, заслуживающий большего доверия.

Вот упрощенный пример того, как рассчитать общий балл доверия:

- Репутация и прошлый опыт взаимодействия: 4/5
- Достоверность и компетентность: 5/5
- Источники информации и методы ее сбора: 3/5
- Обмен данными и сотрудничество: 4/5
- Транспарентность: 4/5
- Своевременность и точность: 4/5
- Анализ и контекст: 5/5
- Соответствие отраслевым стандартам: 4/5
- Соблюдение правовых и этических норм: 5/5

Общий показатель доверия к источнику может быть таким:

(4*0,1) + (5*0,15) + (3*0,1) + (4*0,1) + (4*0,1) + (4*0,1) + (5*0,15) + (4*0,1) + (5*0,1) = **4,30**

— — — — — — — —

Добавление C

Пример механизма оценки правдоподобности и достоверности источника киберинформации/разведданных

1. Подтверждение из нескольких источников:
   - Оцените, подтверждаются ли информация/разведданные о киберугрозе несколькими независимыми источниками: например, несколько источников, сообщающих одну и ту же информацию, могут повысить ее правдоподобность.

2. Соответствие известным угрозам и тактике:
   - Определите, соответствуют ли информация/разведданные о киберугрозах известным киберугрозам, методам и тактике атак, поскольку несоответствия могут указывать на более низкий уровень правдоподобности.

3. Технические подробности и доказательства:
   - Проверьте наличие технических подробностей и доказательств, подтверждающих информацию/разведданные о киберугрозе, поскольку убедительные технические доказательства повышают правдоподобность.

4. Атрибуция и мотивация:
   - Оцените возможность атрибуции (установления ответственности за киберугрозу конкретных субъектов или групп).
   - Изучите мотивы этих субъектов и их соответствие заявленной киберугрозе.

5. Выбор времени и контекст:
   - Проанализируйте время и контекст возникновения киберугрозы в системе кибербезопасности.
   - Рассмотрите, согласуется ли киберугроза с текущими событиями или тенденциями.

6. Историческая точность:
   - Оцените историческую точность источника при составлении отчетов о киберугрозах, поскольку стабильно высокая точность отчетов в прошлом повышает степень доверия к ним.

7. Проверка коллегами и круг доверенных лиц:
   - Определите, были ли информация/разведданные о киберугрозе подтверждены или одобрены коллегами или отраслевыми группами, поскольку подтверждение со стороны коллег может повысить правдоподобность.

8. Тревожные сигналы и аномалии:
   - Выявляйте тревожные сигналы, аномалии или подозрительные элементы в информации/разведданных о киберугрозах; разбор и прояснение таких вопросов может повысить степень доверия.

Для измерения уровня правдоподобности/достоверности источника киберинформации/разведданных можно использовать систему оценок, основанную на вышеуказанных критериях.

Ниже приводится пример схемы оценки.

1. Присвойте каждому критерию весовой коэффициент в зависимости от его важности и актуальности для оценки киберриска.
2. Оцените разведданные об угрозе по шкале (например, от 1 до 5) по каждому критерию, где 5 – это наивысший уровень правдоподобности.
3. Рассчитайте общий балл правдоподобности, суммировав взвешенные оценки по каждому критерию. Более высокий балл указывает на более правдоподобный отчет об угрозе.

Вот упрощенный пример того, как рассчитать общий балл правдоподобности/ достоверности:

- Подтверждение из нескольких источников: 4/5
- Соответствие известным угрозам и тактике: 3/5
- Технические подробности и доказательства: 5/5
- Атрибуция и мотивация: 4/5
- Выбор времени и контекст: 4/5
- Историческая точность: 4/5
- Проверка коллегами и круг доверенных лиц: 4/5
- Тревожные сигналы и аномалии: 3/5

Общий балл правдоподобности/достоверности может быть следующим:

(4*0,15) + (3*0,15) + (5*0,15) + (4*0,1) + (4*0,15) + (4*0,1) + (4*0,1) + (3*0,1) = **3,90**

— — — — — — — —

Добавление D

Пример схемы оценки уровня доверия к киберинформации

В этом добавлении описывается "кодекс Адмиралтейства"[13] как еще один пример метода оценки собранных разведданных.

Шкала может использоваться при обмене информацией, чтобы дать представление о надежности источника и достоверности информации. В рамках данного метода используются два символа (буква и цифра), где буква оценивает надежность источника, а цифра отражает уровень доверия к информации.

Надежность источника

Надежность источника оценивается на основе технической оценки его возможностей, а в случае с агентурными данным – на основе их истории. В этой системе обозначения используется алфавитная кодировка от A до F для оценки надежности источника следующим образом.

Код надежности	Надежность	Пояснение
A	Абсолютно надежен	Нет никаких сомнений в подлинности, благонадежности или компетентности; в прошлом зарекомендовал себя абсолютно надежным.
B	Обычно надежен	Имеются небольшие сомнения в подлинности, благонадежности или компетентности; в прошлом в большинстве случаев предоставлял достоверную информацию.
C	Относительно надежен	Имеются сомнения в подлинности, благонадежности или компетентности, но в прошлом предоставлял достоверную информацию.
D	Обычно ненадежен	Имеются серьезные сомнения в подлинности, благонадежности или компетентности, но в прошлом предоставлял достоверную информацию.
E	Ненадежен	Не хватает подлинности, благонадежности и компетентности; в прошлом предоставлял недостоверную информацию.
F	Невозможно оценить надежность	Не на что опереться для оценки надежности источника.

[13] Подробное описание методики можно найти на страницах 59 – 60 публикации Joint Doctrine Publication 2-00, Intelligence, Counter-intelligence and Security Support to Joint Operations (Fourth Edition) (Объединенная доктрина 2-00 "Обеспечение разведки, контрразведки и безопасности в совместных операциях" (четвертое издание)), доступной по следующей ссылке: https://www.gov.uk/government/publications/jdp-2-00-understanding-and-intelligence-support-to-joint-operations.

Достоверность информации

Достоверность оценивается с учетом вероятности и уровня подтверждения другими источниками. В этой системе обозначения используется следующая числовая кодировка от 1 до 6 для оценки достоверности источника.

Оценка досто-верности	Достоверность	Пояснение
1	Подтверждено другими источниками	Подтверждено другими независимыми источниками; логично само по себе; согласуется с другой информацией по этому вопросу.
2	Вероятно, соответствует действительности	Не подтверждено; логично само по себе; согласуется с другой информацией по этому вопросу.
3	Возможно, соответствует действительности	Не подтверждено; довольно логично само по себе; частично согласуется с другой информацией по этому вопросу.
4	Сомнительно	Не подтверждено; возможно, но не логично; другая информация по этому вопросу отсутствует.
5	Неправдоподобно	Не подтверждено; нелогично само по себе; противоречит другой информации по этому вопросу.
6	Невозможно оценить правдоподобность	Не на что опереться для оценки достоверности информации.

Приведенные выше таблицы можно свести в следующую таблицу.

Надежность источника	Достоверность киберинформации
A Абсолютно надежен	1 Подтверждено другими источниками
B Обычно надежен	2 Вероятно, соответствует действительности
C Относительно надежен	3 Возможно, соответствует действительности
D Обычно ненадежен	4 Сомнительно
E Ненадежен	5 Неправдоподобно
F Невозможно оценить надежность	6 Невозможно оценить правдоподобность

Вот два примера ранжирования киберинформации:

- *C4, что трактуется следующим образом: относительно надежный источник и вызывающая сомнения информация.*
- *A1, что трактуется следующим образом: источник абсолютно надежен, информация подтверждена другими источниками.*

Несмотря на субъективность оценки, ранжирование является полезным инструментом, который помогает получателю киберинформации провести собственную оценку и анализ киберинформации.

— — — — — — — —

Добавление E

Рекомендуемая структура официального соглашения об обмене киберинформацией

Официальное соглашение об обмене киберинформацией должно включать следующие разделы:

- ✓ Преамбула, включающая названия и описание сторон.
- ✓ Определения и сокращения.
- ✓ Сфера применения: описание сферы применения документа и ссылка на добавление 1, в котором описывается тип киберинформации, подлежащей обмену.
- ✓ Права и обязанности получателя информации (реципиента).
- ✓ Источники информации: кто и кому будет предоставлять информацию, на основании каких источников, потребуется ли делиться информацией об источнике.
- ✓ Ограничения на то, какой информацией и с кем можно делиться, с учетом действующего законодательства, прав интеллектуальной собственности, конфиденциальности коммерческой информации, определения маркировки TLP и т. д.
- ✓ Формат и периодичность обмена информацией.
- ✓ Средства передачи информации (например, письма, телефон, текстовые сообщения, электронная почта, репозиторий и т. д.), включая средства защиты и обеспечения конфиденциальности, неприкосновенности и доступности информации, передаваемой в цифровом виде.
- ✓ Требования к качеству: описание действий, которые отправителю необходимо совершить перед передачей информации. Здесь же описываются средства обеспечения целостности и качества информации, передаваемой в общий доступ, включая, например, ее анонимизацию и/или обезличивание.
- ✓ Хранение и учет: описание политики и процедур архивирования подлежащей обмену информации. Здесь же описывается минимальный срок, в течение которого отправленная/полученная информация должна архивироваться для предусмотренных соглашением и отношениями между сторонами целей контроля качества.
- ✓ Стоимость: описание того, какая из сторон принимает на себя расходы по обмену информацией. Каждой из сторон рекомендуется нести собственные расходы по выполнению соглашения.
- ✓ Административные процессы и процедуры управления изменениями, прописанные в соглашении.
- ✓ Переписка и уведомления, связанные с соглашением.
- ✓ Материальная ответственность: здесь описываются соответствующие обязательства. Рекомендуется возмещать отправляющей стороне расходы, связанные с передачей информации.
- ✓ Обработка персональных данных: описание того, как будут обрабатываться персональные данные, включая применимые законы и правила.
- ✓ Разрешение споров: как и в соответствии с какими законами будут рассматриваться споры, связанные с соглашением. Сторонам рекомендуется прежде всего попытаться урегулировать споры мирным путем, а в случае неудачи – прибегнуть к услугам посредников в оговоренной ими юрисдикции.

- ✓ Соглашение целиком и поправки к нему: здесь описывается приоритетность тех или иных частей соглашения.
- ✓ Дата вступления соглашения в силу, срок его действия, процедуры продления и прекращения действия.
- ✓ Назначение: подписи уполномоченных лиц от каждой стороны.
- ✓ Добавления:
  - Добавление 1. Необходимая информация: описание типов информации, которую передает каждая из сторон.
  - Добавление 2. Определение маркировки TLP, включая ссылку на стандарт FIRST TLP.

— — — — — — — —

Добавление F

MISP – платформа с открытым исходным кодом для сбора информации об угрозах и обмена ею

MISP[14] – это платформа для совместного использования, хранения и сопоставления информации о признаках несанкционированного доступа (IoC) в результате целенаправленных кибератак, а также таких разведданных о киберугрозах, как информация об исполнителях угроз, финансовых махинациях и т. д.

Это бесплатная платформа с открытым исходным кодом для сбора информации о киберугрозах и обмена ею, которая позволяет организациям создавать сообщества для обмена информацией, например разведданными о киберугрозах, показателях несанкционированного доступа, информацией о субъектах угроз и любых видах киберугроз, которые могут быть структурированы в рамках MISP.

Пользователи MISP совместно используют информацию о существующих вредоносных программах и киберугрозах. MISP используется для создания "сообществ". Обмен информацией происходит внутри сообщества пользователей. Цель этой платформы, основанной на доверительных отношениях, – помочь повысить эффективность мер противодействия целенаправленным кибератакам, а также превентивных действий и обнаружения.

Государствам и заинтересованным сторонам в авиации рекомендуется изучить возможности MISP, а также любых аналогичных платформ в качестве средства/метода обмена киберинформацией:

- помогает автоматизировать использование полученной информации для обновления различных систем безопасности, таких как системы управления информацией о безопасности и соответствующими процессами/ центры обеспечения безопасности (SIEM/SOC), межсетевые экраны, антивирусное программное обеспечение и системы обнаружения и предотвращения вторжений (IDPS/IPS);
- позволяет быстро обмениваться киберинформацией, так как время может быть критическим фактором при обмене информацией, связанной с оперативным реагированием на киберинцидент;
- позволяет обновлять киберинформацию в связи с киберинцидентами и добавлять к ней дополнительную информацию по мере ее поступления;
- через MISP могут передаваться все типы информации, маркированной согласно TLP. Однако информация, помеченная как **TLP:КРАСНЫЙ**, распространяется через MISP только в том случае, если сообщество состоит из ограниченного числа лиц, которые согласны делиться такой информацией. Как правило, информация, маркированная **TLP:КРАСНЫЙ**, передается не по MISP, а с помощью альтернативных средств (например, по телефону, посредством текстовых сообщений и по электронной почте).

— КОНЕЦ —

[14] Дополнительная информация об использовании MISP: https://www.circl.lu/services/misp-malware-information-sharing-platform/.