Культура кибербезопасности в гражданской авиации

Опубликовано с санкции Генерального секретаря

Январь 2022 г.

Международная организация гражданской авиации

1. Введение

Настоящий инструктивный материал соответствует Стратегии ИКАО в области авиационной кибербезопасности[1] и Плану действий по обеспечению кибербезопасности[2], в пункте действий ПДоК7.1 которого рекомендуется определить и популяризировать культуру кибербезопасности в гражданской авиации.

2. Сфера применения

Настоящий инструктивный материал призван оказать поддержку государствам-членам и заинтересованным сторонам в формировании и внедрении в рамках своих организаций действенной культуры кибербезопасности. Конечной целью является обеспечение безопасности и устойчивости гражданской авиации в отношении киберугроз и рисков.

3. Определение, общие цели и преимущества культуры кибербезопасности

3.1 Для целей настоящего инструктивного материала под культурой кибербезопасности обыкновенно следует понимать набор допущений, установок, убеждений, действий, норм, восприятий и ценностей, которые являются неотъемлемой частью повседневной деятельности организации и отражаются в действиях и принципах поведения всех субъектов и персонала в их взаимодействии с цифровыми активами.

3.2 Позитивная культура кибербезопасности призвана сделать аспекты кибербезопасности частью привычной практики, образа действий и процессов организации путем привнесения их в повседневную деятельность, что отражается в действиях и принципах поведения всего персонала.

3.3 Создание развитой и действенной культуры кибербезопасности в качестве неотъемлемой части организационной культуры помогает организациям в деле повышения их общего уровня эффективности за счет раннего обнаружения потенциальных киберрисков.

3.4 Культура кибербезопасности в гражданской авиации основывается на опыте, усилиях и успешном создании в секторе развитой культуры в сферах авиационной безопасности и безопасности полетов, с которыми у нее имеется много общих основных элементов. Такой межсферный характер культуры кибербезопасности приводит не только к укреплению позиции кибербезопасности, но также оказывает позитивное побочное воздействие в этих трех сферах путем популяризации и укрепления позитивной культуры безопасности полетов, авиационной безопасности и кибербезопасности.

3.5 В итоге, культура кибербезопасности позволяет каждому лицу в организации, независимо от его роли, лучше выполнять свои обязанности в цифровой среде. Примеры преимуществ формирования и внедрения эффективной и действенной культуры кибербезопасности включают:

a) повышение уровня зрелости системы кибербезопасности организации;
b) надлежащая обработка информации всем персоналом;
c) более четкая позиция в отношении кибербезопасности, которая обеспечивает эффективность и действенность организации в деле смягчения киберрисков;
d) повышение осведомленности всего персонала в части киберрисков и роли каждого из них в обнаружении и смягчении указанных рисков;

[1] https://www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx
[2] Письмо государствам ИКАО 2020/114

e) желание сообщать результаты осуществления личного контроля в рамках организационных процессов и процедур обеспечения кибербезопасности, а также сообщать о подозрительной кибердеятельности, что приводит к проактивному и более действенному обнаружению киберрисков.

3.6 Основные элементы эффективной организационной культуры авиационной кибербезопасности изложены в приведенных ниже разделах настоящего инструктивного материала. Тем не менее, хотя эти основные элементы подробно определены, культура кибербезопасности должна формироваться индивидуально в рамках каждой организации. В ней следует учитывать различные аспекты, включая уровень зрелости системы кибербезопасности в организации, существующие культуру и ценности, а также общий ландшафт угроз кибербезопасности.

3.7 Основными элементами развитой и эффективной культуры кибербезопасности в гражданской авиации являются:

a) руководство;
b) межсферные связи;
c) коммуникация;
d) осведомленность, подготовка и образование;
e) системы представления данных;
f) постоянный пересмотр и совершенствование;
g) позитивная рабочая среда.

4. **Руководство**

4.1 Эффективная культура кибербезопасности зависит от приверженности делу каждого лица в организации, начиная со старшего руководства. Старшее руководство должно демонстрировать свою полную приверженность культуре кибербезопасности на постоянной основе и во всех видах деятельности, стратегиях, политике и в организационных целях.

4.2 Старшее руководство должно соблюдать положения политики в области кибербезопасности на личном примере и служить образцом исполнительности для руководителей и персонала организации. Оно должно популяризировать кибербезопасность в качестве организационных и личных ценностей и в то же время аналогичным образом стараться приводить свои принципы поведения в соответствие с такими ценностями.

4.3 В этой связи старшему руководству следует:

a) стремиться повышать свои знания в области кибербезопасности в гражданской авиации;
b) постоянно и на личном примере соблюдать правила, процессы и процедуры кибербезопасности;
c) безоговорочно включить кибербезопасность в качестве приоритетной задачи организации;
d) зафиксировать авиационную кибербезопасность в директивных документах организации, с тем чтобы она стала неотъемлемой частью управленческого плана компании;
e) обеспечить видимую поддержку внедрению культуры кибербезопасности;
f) обеспечить и поддерживать подготовку в области кибербезопасности и наращивания потенциала для всего персонала;
g) обеспечить своевременную обработку донесений о кибербезопасности и обеспечить оперативное принятие любых необходимых корректирующих или превентивных мер;

h) принимать надлежащие меры, когда кибербезопасность подвергается угрозе;
i) следить за развитием позиции организации в области кибербезопасности, культуры кибербезопасности, а также за принятием мер и ресурсами, выделенными в поддержку последовательной активизации принятия культуры кибербезопасности в рамках всей организации.

4.4 Следуя примеру старшего руководящего состава, другие руководящие звенья организации должны также стремиться предпринимать указанные в п. 4.3 действия согласно своим обязанностям и управленческой сфере, с тем чтобы популяризировать приверженность принципам культуры кибербезопасности в рамках всей организации.

5. **Межсферные связи**

5.1. Принимая во внимание многообразие киберрисков и уязвимостей в каждой организации, следует официально установить межсферные связи.

5.2. В качестве механизма координации культуры кибербезопасности в рамках всей организации можно создать подотчетную старшему руководству многодисциплинарную специальную группу.

5.3. Цели данной специальной группы будут включать:

a) периодическую оценку зрелости культуры кибербезопасности в рамках организации;
b) выявление рисков и возможностей в части внедрения культуры кибербезопасности;
c) согласование интересов различных внутренних участвующих сторон в отношении культуры кибербезопасности;
d) поддержка разработки и осуществления межсферных видов деятельности, связанных с укреплением культуры кибербезопасности в организации.

6. **Коммуникация**

6.1. Коммуникация играет важнейшую роль как внутри, так вне организации, в деле обеспечения формирования успешной культуры кибербезопасности. Она является главным средством, с помощью которого можно достичь ожидаемого уровня осведомленности.

6.2. С тем чтобы коммуникация была эффективной, в рамках развитой культуры кибербезопасности следует рассмотреть ряд определенных навыков:

a) *активное слушание* – процесс, с помощью которого воспринимаются вербальные и невербальные сигналы, с тем чтобы распознать ценности и потребности другого лица и способствовать улучшению коллективной коммуникации;
b) *адаптация коммуникационного стиля к различным аудиториям и ситуациям* – понимание того, как осуществляют коммуникацию другие лица, и модификация сообщения, с тем чтобы оно было лучше ими воспринято;
c) *ясность коммуникации* – определение того, что и как сообщать.

6.3. Старшее руководство должно принять меры к тому, чтобы политика и рекомендации, касающиеся кибербезопасности, а также причины их введения, были должным образом доведены до сведения всего персонала. Надежная внутренняя программа обмена информацией способствует принятию и пониманию всем персоналом мер в области кибербезопасности, а также содействует популяризации культуры кибербезопасности в организации.

6.4. Кроме того, программы внутреннего обмена информацией во многом будут способствовать:

a) обеспечению того, что все сотрудники полностью осведомлены о своих обязанностях, правах и действующих в организации механизмах представления данных;
b) популяризации цифрового кодекса поведения в организации, который включает процессы, меры и методы контроля, которые персонал всегда должен соблюдать.

7. **Осведомленность, подготовка и образование**

7.1 Осведомленность, подготовка и образование – это ключевые области процесса обучения, который должен быть задействован для создания развитой культуры кибербезопасности. Осведомленность предоставляет людям знания, подготовка учит навыкам, а образование предоставляет знания и навыки в рамках теоретической подготовки, объединяя тем самым осведомленность и подготовку.

7.2 Весь персонал гражданской авиации, который взаимодействует с цифровыми активами организации, независимо от своей роли или функции, должен пройти обучение по программе повышения осведомленности, подготовки и образования в области кибербезопасности для получения требуемых знаний и навыков в области рисков, мер и целей авиационной кибербезопасности. По необходимости и возможности эти программы следует адаптировать к соответствующей аудитории.

7.3 Подготовку по программам повышения осведомленности о кибербезопасности должен проходить весь персонал по приему на работу, а также в ходе переподготовки. Временны́е интервалы между проведением повторной программы повышения осведомленности должны быть установлены исходя из уровня зрелости культуры кибербезопасности в организации, и их можно пересматривать по мере повышения уровня зрелости системы.

7.4 Программы повышения осведомленности о кибербезопасности рекомендуется проводить как минимум один раз в очном порядке (в условиях физической или виртуальной аудитории). Кибербезопасность не является знакомой темой для всего персонала, и ее иногда трудно усвоить без наставничества со стороны специалиста. Таким образом, взаимодействие со специалистом в аудитории способствует лучшему пониманию связанных с кибербезопасностью тем. Это позволяет инструктору разъяснить концепцию, процессы, процедуры и меры контроля в упрощенном виде, который понятен технически неискушенному персоналу, а также объяснить преимущества укрепления позиции организации в области кибербезопасности и ее положительное воздействие на общую производительность персонала.

7.5 После проведения начального курса по повышению осведомленности/подготовки в очном порядке организации могут рассмотреть вопрос о применении для целей переподготовки методов электронного обучения (обучения с помощью компьютеров). Такое решение должно учитывать уровень развития культуры кибербезопасности в организации, а также изменения в процессах, мерах контроля и процедурах в области кибербезопасности, которые вводятся в организации в связи с эволюцией ландшафта рисков для кибербезопасности.

7.6 Занятия по программам повышения осведомленности о кибербезопасности должны проводиться специалистами, обладающими требуемым уровнем технических знаний. Однако одной из проблем, связанных с техническими программами повышения осведомленности, является нехватка у преподавателей навыков межличностного общения, и таким образом надлежащие коммуникационные навыки и умение "преподнести" в нужном свете предмет имеют огромное значение для того, чтобы заинтересовать сотрудников и обеспечить принятие и поддержку с их

стороны культуры кибербезопасности. Соответственно, организации должны убедиться в том, что руководители программ по повышению осведомленности в равной степени владеют как техническими знаниями, так и навыками межличностного общения, необходимыми для того, чтобы побудить персонал изменить принципы поведения в поддержку принятия культуры кибербезопасности.

7.7 Типовая программа повышения осведомленности о кибербезопасности должна включать следующие предметы:

a) цель программы повышения осведомленности;
b) существующие в организации механизмы коммуникации;
c) общий обзор киберрисков для гражданской авиации и потенциальные последствия (включая примеры);
d) меры контроля, процессы и процедуры кибербезопасности организации;
e) роль человеческого фактора в защите организации от киберрисков;
f) важность того, чтобы сотрудники напоминали друг другу о принципах кибербезопасности организации, если они замечают несоблюдение своими коллегами соответствующих правил;
g) обзор различных методов эксплуатации уязвимости, которые могут быть нацелены на людей, и их последствия (включая примеры);
h) способы выявления подозрительных видов кибердеятельности;
i) воздействие самоуспокоенности на организацию (включая примеры);
j) принципы киберпрофилактики;
k) надлежащая обработка конфиденциальных данных и информации;
l) механизмы представления данных, способы их использования и механизмы последующих действий.

7.8 Кампании по повышению осведомленности о кибербезопасности следует также проводить периодически в качестве напоминания, с тем чтобы закрепить знания и навыки персонала. Для этой цели имеются различные средства, в том числе:

a) *средства на бумажных носителях* – такие, как плакаты, брошюры, буклеты и т. д. Такой тип информации можно легко распространить и усвоить. Однако это пассивные средства, которые требуют постоянного обновления (и при каждом обновлении новый тираж);
b) *онлайновые средства* – такие, как электронная почта, бюллетени, сообщения на заставке экрана, интранет, короткие видеоролики, страницы с часто задаваемыми вопросами, электронное обучение (обучение с помощью компьютеров) и т. д. Основное преимущество этих средств по сравнению со средствами на бумажных носителях заключается в их способности охватить всю организацию. Их относительно легко обновлять в плане ресурсов, и они являются низкозатратными.

8. **Система представления данных**

8.1 Краеугольным камнем культуры кибербезопасности является разработка и внедрение внутренней системы представления данных о кибербезопасности. Такая система позволяет организации проактивно управлять своими киберрисками, оценивать развитие позиции организации в области кибербезопасности, определять потребности сотрудников в повышении осведомленности и подготовки и планировать соответствующие действия, а также адаптировать свои внутренние процессы, меры контроля и действия в соответствии с развитием тенденций в области кибербезопасности и согласно зрелости культуры кибербезопасности.

8.2 Системы представления данных о кибербезопасности собирают элементы информации как из систем представления данных о безопасности полетов, так и систем представления данных об авиационной безопасности. Тем самым они затрагивают две области: первая область – это донесения о собственных действиях/ошибках, которые не соответствуют политике и процессам организации в области информационной безопасности, а вторая область – это донесения о подозрительных/неправильных действиях других сотрудников.

8.3 При разработке своего механизма представления данных о кибербезопасности организациям рекомендуется воспользоваться опытом, полученным при разработке и внедрении систем представления данных о безопасности полетов и авиационной безопасности.

8.4 При внедрении системы представления данных о кибербезопасности следует принимать во внимание следующие элементы:

a) конфиденциальность личной информации, в силу чего личные данные не собираются и/или не сохраняются. Если личные данные собираются, их следует использовать исключительно для того, чтобы получить разъяснения, дополнительную информацию о сообщаемом событии или для обратной связи с лицом, представившем данные;
b) с тем чтобы обеспечить конфиденциальность личной информации, следует разработать политику, которая четко определяет лицо (лица), несущее(ие) за это ответственность, которым поручается обеспечить, поддерживать, гарантировать конфиденциальность, а также анализировать собранную информацию и принимать по ней последующие меры;
c) проведение надлежащей подготовки всего персонала по методам использования системы представления данных;
d) внедрение справедливой культуры в представлении данных о кибербезопасности и обеспечение надлежащей осведомленности всего персонала о порядке функционирования справедливой культуры, с тем чтобы сотрудники чувствовали себя более уверенно при предоставлении информации;
e) в соответствующих случаях внедрение программы мотивации, направленной на поощрение персонала сообщать о собственных ошибках, а также о любом замеченным ими подозрительном поведении в части кибербезопасности.

Справедливая культура

8.5 Организациям следует побуждать своих сотрудников к тому, чтобы они сообщали о связанных с кибербезопасностью инцидентах в рамках принятия справедливой культуры. Справедливая культура – это концепция, применяемая в системе представления данных о безопасности полетов, которая может иметь большое значение в деле популяризации культуры кибербезопасности.

8.6 В контексте представления данных о кибербезопасности справедливая культура побуждает всех сотрудников к тому, чтобы сообщать о связанных с кибербезопасностью инцидентах и ошибках. Эта среда, в которой все понимают, что с ними будут обращаться справедливо исходя из их действий, а не из результатов их действий. В условиях справедливой культуры все сотрудники четко понимают, что наказывать за все шибки, независимо от их последствий, несправедливо, но в то же время они понимают, что полная безнаказанность является также неприемлемой, поскольку некоторые действия могут иметь злой умысел или могут быть результатом явной халатности и/или беспечности. Таким образом, при формировании справедливой культуры важно провести черту между приемлемыми и неприемлемыми действиями.

8.7 Справедливая культура определяет не только ответственность персонала перед своими организациями, но также и ответственность руководства перед персоналом. Такую ответственность следует включить в политику, в которой старшее руководство организации должно:

a) побуждать сотрудников практиковать гиперпрофилактику и обязательно отмечать их усилия, направленные на поддержку организации в деле управления киберрисками;
b) обязательно предоставлять всем сотрудникам надлежащие процедуры обеспечения кибербезопасности, повышать их осведомленность, проводить подготовку и образовательные мероприятия для оказания им поддержки в исполнении их обязанностей;
c) брать на себя ответственность, если причиной какого-либо инцидента является недостаточная осведомленность или оперативность в устранении определенного киберриска;
d) побуждать сотрудников сообщать о киберинцидентах, опасностях, ошибках или любом подозрительном поведении, которые они заметят, без страха понести за это наказание.

Контроль качества

8.8 Организации должны внедрять программы контроля качества, предназначенные для мониторинга эффективного принятия мер кибербезопасности. Программы контроля качества могут служить эффективным средством в поддержании бдительности сотрудников и их приверженности принципам культуры кибербезопасности. Периодичность и тщательность принятия мер по контролю качества могут оказать положительное влияние на сотрудников тем, что они демонстрируют приверженность руководства целям кибербезопасности и соблюдению соответствующих требований.

8.9 В рамках программ контроля качества следует проводить регулярные проверки качества работы действующих механизмов представления данных.

9. Постоянный пересмотр и совершенствование

9.1 Организациям следует разработать систему показателей эффективности, предназначенную для оценки влияния принимаемых мер на культуру кибербезопасности, а также для определения существующих пробелов между желаемыми и фактическими результатами, связанными с культурой кибербезопасности.

9.2 Поскольку некоторые элементы культуры кибербезопасности могут непосредственно не проявляться, для оценки эффективности культуры кибербезопасности можно использовать ряд возможных показателей. Такие меры могут включать:

a) статистические данные по сообщаемым инцидентам (рассматриваемые в сравнении с данными, полученными из технических реестров организации) для оценки эффективности деятельности сотрудников в области кибербезопасности, их уровня осведомленности и достигнутых результатов в содействии представлению данных о кибербезопасности;
b) результаты курсов по переподготовке персонала;
c) результаты моделирования злонамеренных действий для проверки ответной реакции персонала;
d) вопросники и собеседования.

10. **Позитивная рабочая среда**

10.1 Общая позитивная рабочая среда может также оказать большое влияние на приверженность персонала культуре кибербезопасности и повысить эффективность обеспечения кибербезопасности.

10.2 Позитивная рабочая среда должна как минимум включать:

a) участие персонала в процессе принятия решений (например, предложения по совершенствованию программ подготовки по повышению осведомленности о кибербезопасности);
b) выделение достаточного количества времени на прохождение персоналом подготовки по надлежащей киберпрофилактике;
c) механизм оценки и признания хороших результатов работы (т. е. стимулирование и/или программы поощрения);
d) предоставление информации персоналу по линии обратной связи о предложениях и о донесениях о кибербезопасности;
e) постановку четких, достижимых и поддающихся измерению целей в части связанных с кибербезопасностью инцидентов, а также периодическое предоставление персоналу информации по линии обратной связи о достигнутом прогрессе организации в этом направлении;
f) предоставление необходимых процедур, повышение осведомленности, проведение подготовки и предоставление средств, позволяющих персоналу выполнять свои обязанности;
g) предоставление персоналу надлежащей степени самостоятельности и ответственности.

— КОНЕЦ —