Приложение 2

к приказу Генерального директора

АО «Авиационная администрация Казахстана»

от \_\_\_ \_\_\_\_\_\_\_\_ 20\_\_г. № \_\_\_\_

**Проверочный лист мероприятий по авиационной безопасности**

**По внедрению мер защиты критических авиационных систем информационных и связных технологий от киберугроз в гражданской авиации Республики Казахстан**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Нормативная ссылка** | **Оценка соответствия**  **(+/-)** | **Номер позиции несоответствия** | **Примечание** |
| 1 | Определены ли критически важные авиационные информационные системы; |  |  |  |
| 2 | Внедрены ли меры защитыавиационных информационных систем; |  |  |  |
| 3 | Определение угрозы и факторов риска, представляемые возможными киберинцидентами в отношении полётов и критически важных систем гражданской авиации, а также серьёзные последствия, к которым могут привести такие инциденты; |  |  |  |
| 4 | Имеются ли, выработаны ли стратегии, политики и планы обеспечения кибербезопасности; |  |  |  |
| 5 | Внедрена ли система управления кибербезопасностью; |  |  |  |
| 6 | Проводится ли обмен информацией в области киберугроз с заинтересованными сторонами; |  |  |  |
| 7 | Определены ли юридические последствия действий, ставящих под угрозу безопасность полётов воздушных судов путём использования киберуязвимых мест; |  |  |  |
| 8 | Внедрены ли методы мониторинга систем и выявления инцидентов; |  |  |  |
| 9 | Проводится ли координация действий по предоставлению отчётности об инцидентах между подразделениями организации гражданской авиации в области авиационной безопасности и безопасности полётов и национальными группами быстрого реагирования на компьютерные угрозы (CERT); |  |  |  |
| 10 | При определении критически важных систем дополнительно указано ли программное обеспечение и оборудование для критически важных информационных систем и систем данных, используемых в их деятельности гражданской авиации; |  |  |  |
| 11 | Защита критических авиационных систем информационных и связных технологий (в том числе их оборудования и программного обеспечения) и данных включённая в процессы оценки риска для каждой критически важной авиационной системы; |  |  |  |
| 12 | Концепция, задача, масштаб и стратегия обеспечения безопасности в организации в соответствии с национальными законодательными актами, нормативными положениями, политикой и инструктивным материалом, определённое подразделением организации гражданской авиации, отвечающее за обеспечение кибербезопасности; |  |  |  |
| 13 | Включили ли организации гражданской авиации в свои программы безопасности соответствующие положения, касающиеся защиты критических систем информационных и связных технологий (включая их программное обеспечение и оборудование) и данных от кибератак и вмешательства; |  |  |  |
| 14 | Эксплуатанты (организации гражданской авиации) учитывают соображения безопасности на протяжении всего цикла работы авиационных систем информационных и связных технологий, начиная с проектирования и разработки до завершения срока эксплуатации и обслуживания систем, вплоть до безопасной и надлежащей утилизации оборудования и программного обеспечения, также и при модификации, пересмотре, обновлении и модернизации существующих систем, при хранении и управление данными в этих системах; |  |  |  |
| 15 | Ответственность за обеспечение защиты критически важных информационных систем лежит на должном образе подобранном, нанятом и подготовленном персонал; |  |  |  |
| 16 | Разработка четких инструктивных указании эксплуатантами авиационной отрасли для подготовки всех сотрудников, использующих или устанавливающих критически важные информационные системы, занимающихся их обслуживанием, а также для определенных летных экипажей и систем, и для персонала по техническому обслуживанию воздушных судов; |  |  |  |
| 17 | Регулярная подготовка своих пользователей в части передовой практики, касающейся обеспечения кибербезопасности в целом и в частности того, как кибербезопасность соотносится с системами и данными информационных и связных технологий, использующимися в авиационной отрасли; |  |  |  |
| 18 | Предоставление уполномоченной организации списка всех ответственных лиц за контроль и обеспечение кибербезопасности, авиационной безопасности и контроль качества; |  |  |  |
| 19 | Проектирование сетей и управление ими с учётом соблюдения требований кибербезопасности; |  |  |  |
| 20 | Включение положений, касающихся информационной и кибербезопасности при поставке и обслуживании новых и имеющихся авиационных систем, информационных и связных технологий и данных; |  |  |  |
| 21 | Организация контроля доступа. Меры ограничения доступа к критически важным системам; |  |  |  |
| 22 | Непрерывный мониторинг информационной безопасности (ISCM); |  |  |  |
| 23 | Обнаружение. Разработка режима непрерывного мониторинга информационной безопасности (ISCM); |  |  |  |
| 24 | Планирование мер реагирования. Готовность к реагированию. Реагирование на инциденты. Уведомления об инцидентах; |  |  |  |
| 25 | Создание и использование плана связи в кризисной ситуации; |  |  |  |
| 26 | Проведение последующего анализа произошедших инцидентов информационной и кибербезопасности; |  |  |  |
| 27 | Ответные действия в связи с актами незаконного вмешательства (кибератаки, ставящие под угрозу безопасность авиации); |  |  |  |
| 28 | Соблюдение конфиденциальности информации по авиационной безопасности. Идентификация, обращение, обмен, уничтожение; |  |  |  |
| 29 | Предоставление информации об угрозе; |  |  |  |
| 30 | Соблюдение полномочий инспектора уполномоченной организации; |  |  |  |
| 31 | Проведение мероприятий по контролю качества; |  |  |  |
| 32 | Меры безопасности аэронавигационной службы. Оценка уязвимостей. Определение диапазона возможных нападений; |  |  |  |
| 33 | Меры безопасности аэродромного диспетчерского пункта; |  |  |  |
| 34 | Меры безопасности аэронавигационных средств и аэронавигационных систем; |  |  |  |
| 35 | Безопасность электропитания; |  |  |  |
| 36 | Меры безопасности объектов технического обслуживания; |  |  |  |
|  | Исполнение Единых требований Постановления Правительства Республики Казахстан от 20 декабря 2016 года № 832 и других законодательных актов Республики Казахстан регулирующие вопросы информационной и кибербезопасности; |  |  |  |
| 37 | Соблюдение требований мер информатизации организации; |  |  |  |
| 38 | Соблюдение организации информационной безопасности; |  |  |  |
| 39 | Соблюдение требований к электронным информационным ресурсам и интернет-ресурсам; |  |  |  |
| 40 | Соблюдение требований к разрабатываемому или приобретаемому прикладному программному обеспечению; |  |  |  |
| 41 | Соблюдение требований к информационно-коммуникационной инфраструктуре; |  |  |  |
| 42 | Соблюдение требований к информационной системе; |  |  |  |
| 43 | Соблюдение требований к технологической платформе; |  |  |  |
| 44 | Соблюдение требований к аппаратно-программному комплексу; |  |  |  |
| 45 | Соблюдение требований к сетям телекоммуникаций; |  |  |  |
| 46 | Соблюдение требований к системам бесперебойного функционирования технических средств и информационной безопасности. |  |  |  |

Расшифровка аббревиатур:

(-1) – несоответствие критическое, представляющее угрозу авиационной безопасности и препятствующее дальнейшей деятельности;

(-2) – несоответствия, не препятствующие дальнейшей деятельности, при условии устранения в согласованные сроки или введении ограничений;

(-3) – несоответствия, не препятствующие дальнейшей деятельности и подлежащие устранению при совершенствовании производства и системы качества;

(\*) – не обязательно для данной организации;

(+) – отвечает требованиям;

NA (не применимо) – меры или процедуры не применяется или не используются в данной организации (к примеру, отсутствие рейсов, требующих повышенной бдительности, и т.д.);

NС (не подтверждено) – меры или процедуры, в отношении которых инспекторы не смогли установить соответствие требованиям нормативных правовых актов (отсутствие времени, противоречивая информация или по иным причинам).