Информационное письмо
Об участии ГосНИИАС в рабочей группе по кибербезопасности комитета по безопасности Международного Координационного Ассоциации Совета Авиапроизводителей (ICCAIA).

Угрозы, связанные с использованием компьютерной техники, появились вместе с появлением такой техники. При этом до сих пор нет устоявшейся терминологии, связанной с понятиями кибербезопасности и киберугроз. Исторически обеспечение кибербезопасности делится на две составляющие:

- первая из них связана с обеспечением надёжности используемой техники и зависит от её технического совершенства;
- вторая составляющая отражает меры по противодействию угрозам, связанным с воздействием на работоспособность техники, целостность данных и технологических процессов.

В первую очередь нас будут интересовать вопросы обеспечения защищённости от несанкционированного воздействия и разработка нормативно-правовых документов, обеспечивающих подобную деятельность.

Виды киберугроз можно разделить на пассивные и активные.

Пассивные угрозы – доступ к данным без возможности внесения каких-либо изменений.

Активные угрозы делятся по уровню воздействия на подавление (временная потеря работоспособности без потери данных), разрушение (длительное подавление с частичной потерей данных) и уничтожение (полная потеря работоспособности и данных).

Авиационная отрасль отличается повышенными требованиями к обеспечению безопасности и надёжности.

В сентябре 2013 года было принято решение ICAO и International Industry Organizations, включающей в себя ICCAIA, IATA, ACI и CANSO, о начале работ по кибербезопасности.

В ICCAIA, членом которого является САП, была создана рабочая группа по кибербезопасности в рамках Комитета по Безопасности (Security Commettee).

Был разработан и принят план действий по обеспечению кибербезопасности, который одобрили на заседании ICAO и International Industry Organizations, в декабре 2014 года.

Организационно последовательность обеспечения кибербезопасности в России можно представить следующим образом:

09 сентября 2000 года Президентом РФ утверждена Доктрина информационной безопасности РФ (№ Пр-1895).

01 июня 2006 года принят Национальный стандарт РФ «Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий» (ГОСТ Р ИСО/МЭК 13335-1-2006).

29 декабря 2012 года президент РФ подписал указ о составе комиссии по информационной безопасности, которая является рабочим органом Совета безопасности РФ. Комиссия имеет межведомственной принцип формирования, в нее были делегированы 37 руководителей ключевых государственных ведомств из силовых министерств, президентского аппарата, представители Роскомсвязи, Роснефти, Роскомнадзора и др.

15 января 2013 года опубликован и вступил в силу указ Президента РФ о государственном противодействии кибератакам и ответственности ФСБ за его воплощение.

10 марта 2015 года Вице-премьер Дмитрий Рогозин поручил создать при Военно-промышленной комиссии совет по кибербезопасности и межведомственную рабочую группу по информационной защите.

В результате, в рамках предварительной проработки, можно констатировать следующее:

1. В период с 2008 по 2015 такие страны, как США, ЕС, Индия, Южная Корея, Канада и Китай, приняли национальные программы по обеспечению кибербезопасности. В частности от EUROCAE получено руководство по информационной безопасности («Aeronautical Information System Security (ASIS) Framework Guidance»), принятое в декабре 2015 г.
2. В открытой печати не удалось найти национальную программу обеспечения кибербезопасности в РФ;
3. В России отсутствуют нормативные документы по обеспечению кибербезопасности в авиационной отрасли.
4. Под киберугрозами в России, прежде всего, понимается нанесение ущерба информационным ресурсам, биллинговым и банковским системам и нарушение работоспособности информационных и инфраструктурных систем. Нарушению работы различных машин и механизмов уделяется второстепенное внимание, что может привести к массовым жертвам среди населения.
5. Киберугрозы носят межгосударственный, трансграничный характер.
6. Отсутствие национальной программы и узость понимания киберугроз приводит к расхождению терминологии в РФ и за рубежом, что вызовет трудности в коммуникации и при решении межгосударственных задач.
7. В рамках международного сотрудничества, в апреле 2016 года, состоятся Десятый международный форум «Партнёрство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» (Гармиш-Партенкирхен (Германия), с 25 по 28 апреля 2016 г.) и заседание Ассамблеи EUROCAE (Вена (Австрия), с 28 по 29 апреля 2016 г.), где будут обсуждаться вопросы кибербезопасности.

Предварительный план работ по созданию отечественной программы в области кибербезопасности предполагает создание межведомственной рабочей группы, состоящей из 5-7 человек, и разработку дорожной карты по обеспечению кибербезопасности.

Предлагается поручить Д.В. Саульскому:

- подготовить предложения по составу межведомственной рабочей группы;
- подготовить предложения по организации работ по созданию дорожной карты;
- о проделанной работе проинформировать Наблюдательный Совет САП.