ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ» (МГТУ ГА)

Кафедра экономики и управления на воздушном транспорте

М.А. Родионов

ОРГАНИЗАЦИЯ БИЗНЕС-ПРОЦЕССОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УПРАВЛЕНИЯ АВИАПРЕДПРИЯТИЯМИ

Учебное пособие

Утверждено редакционно-издательским советом МГТУ ГА в качестве учебного пособия

Москва
ИД Академии Жуковского
2018

УДК 33+004.056+629.7(075.8)
ББК 338:05
Р60

Печатается по решению редакционно-издательского совета
Московского государственного технического университета ГА

Рецензенты:
Большедворская Л.Г. (МГТУ ГА) – д-р техн. наук, доц.;
Кочетков Г.Г. (ЗАО «Лидер») – нач. юр. отдела

Родионов М.А.

Р60 Организация бизнес-процессов обеспечения информационной безопасности управления авиапредприятиями [Текст] : учебное пособие / М.А. Родионов – М. : ИД Академии Жуковского, 2018. – 64 с.

ISBN 978-5-907081-46-8

Данное учебное пособие издается в соответствии с рабочей программой дисциплины «Организация бизнес-процессов обеспечения информационной безопасности управления авиапредприятиями» для студентов направления 25.03.03 «Аэронавигация».

Пособие содержит материалы учебно-методического характера, необходимые для освоения знаний и умений по дисциплине «Организация бизнес-процессов обеспечения информационной безопасности управления авиапредприятиями».

Рассмотрено и одобрено на заседании кафедры 18.10.2018 г. и методического совета 19.10.2018 г.

УДК 33+004.056+629.7(075.8)
ББК 338:05
Св. тем. план 2018 г.
поз. 33

РОДИОНОВ Михаил Александрович
ОРГАНИЗАЦИЯ БИЗНЕС-ПРОЦЕССОВ ОБЕСПЕЧЕНИЯ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УПРАВЛЕНИЯ АВИАПРЕДПРИЯТИЯМИ
Учебное пособие

В авторской редакции

Подписано в печать 29.11.2018 г.
Формат 60x84/16 Печ. л. 4 Усл. печ. л. 3,72
Заказ № 382/1029-УП17 Тираж 30 экз.

Московский государственный технический университет ГА
125993, Москва, Кронштадтский бульвар, д. 20

Издательский дом Академии имени Н. Е. Жуковского
125167, Москва, 8-го Марта 4-я ул., д. 6А
Тел.: (495) 973-45-68 E-mail: zakaz@itsbook.ru

ISBN 978-5-907081-46-8

СОДЕРЖАНИЕ

Введение

В настоящее время человечество вступает в эпоху информационной цивилизации, когда возможности государств, обществ, бизнес - структур во многом определяются уровнем обеспечения их информационной безопасности (ИБ). Стремительная информатизация всех областей жизни позволила наиболее развитым странам за короткий срок значительно оторваться от остального мира, причем данный разрыв может стать исторически необратимым. При этом для Российской Федерации, как наибольшей по площади страны мира, особую актуальность имеют вопросы обеспечения ИБ в транспортной сфере, в том числе в области Гражданской авиации. В современной бизнес-среде конкурентоспособны лишь организации, эффективно обеспечивающие свою информационную безопасность.

При изучении учебного пособия, состоящего из трех глав, студенты могут ознакомиться с концептуальными, правовыми, содержательными, организационными, методическими аспектами информационной безопасности и на базе этих знаний получить возможность планирования, организации и практической реализации мероприятий по обеспечению ИБ на авиапредприятиях. В первой главе «Теоретические положения по бизнес-процессам обеспечения информационной безопасности на авиапредприятиях» рассмотрены значение ИБ в современном мире, понятийный аппарат теории информационной безопасности, сущность и содержание ИБ, роль и место бизнес-процессов обеспечения информационной безопасности в управлении современными авиапредприятиями. Вторая глава «Нормативное правовое обеспечение и стандарты информационной безопасности» посвящена вопросам международного законодательства в сфере ИБ, основным законодательным актам Российской Федерации в данной области, отечественным и зарубежным стандартам ИБ. В третьей главе «Практика бизнес-процессов обеспечения информационной безопасности на авиапредприятиях» описываются основы планирования и организации процессов обеспечения ИБ, особенности обеспечения информационно-технической и информационно-психологической безопасности авиапредприятия.

Пособие предназначено для студентов факультета управления на воздушном транспорте профиля «Организация бизнес-процессов на воздушном транспорте» направления подготовки 25.03.03 «Аэронавигация» - по дисциплине «Организация бизнес-процессов обеспечения информационной безопасности управления авиапредприятиями». Пособие может быть использовано при подготовке студентов по направлению подготовки 38.03.02 «Менеджмент», а также обучающихся по другим направлениям экономического профиля, вопросам государственного и муниципального управления.

Глава 1. Теоретические положения по бизнес-процессам обеспечения информационной безопасности на авиапредприятиях

1.1. Информационная безопасность в современном мире

Глобализация и информатизация всех областей жизнедеятельности, ускоряющееся развитие мирового информационного пространства обусловливают возрастающее влияние информационной сферы на экономические, политические, военные и другие процессы, обостряет информационное соперничество и делает его действенным средством внутри- и внешнеполитической деятельности. Объектами целенаправленного информационного воздействия становятся военно-политическое руководство государства, механизмы выработки и принятия управленческих решений, институты формирования общественного мнения, духовная сфера, мировоззрение и психика граждан, информационная инфраструктура, предприятия оборонно-промышленного комплекса, бизнес-струтуры и другие производства с передовыми технологиями. Транспортная инфраструктура государства также входит число этих критически важных, с точки зрения обеспечения ИБ, объектов. Все это относятся и к авиатранспортной области.

Информационная инфраструктура, информационные ресурсы во все большей степени становятся ареной межгосударственной борьбы за мировое лидерство, достижение противоборствующими сторонами определенных политических, экономических и военных целей. Индивидуальное, групповое и массовое сознание людей все в большей степени зависят от деятельности средств массовой информации (СМИ) и массовой коммуникации. Вошли в обиход, в том числе и в международных отношениях, такие понятия, как “информационная война” (его в 1976 г. впервые использовал американец Томас Рона в отчете для компании Boeing "Системы оружия и информационная война"), “информационное противоборство”, “информационная борьба” и т.п. Все эти положения основываются на том, что достижение информационного доминирования обеспечивает возможность опережать контр-партнера в принятии политических и экономических решений, является основой успеха в силовых действиях.

Необходимым условием для выявления сути любого вопроса, в том числе относящегося к информационной области, является его исторический анализ с последующим творческим преломлением полученных результатов на современную действительность. Так, информационное соперничество не является каким-то совершенно новым явлением. Напротив, оно имеет глубокие исторические корни и велось, в том или ином виде, практически во всех войнах и других конфликтах, которыми богата история человечества[1]. Его

[1] Родионов М.А. Информационное противоборство: история и современность. // Информационный сборник “Безопасность”, № 7-8 (58). М. 2002. С. 156-166.

актуализация в настоящее время обусловлена, прежде всего, скачкообразным развитием информационной техники (прежде всего, компьютеров, средств телекоммуникации и связи) и информационных технологий, которые коренным образом изменили облик современного мира.

Наиболее развитыми зарубежными странами разработаны и реализуются концепции информационных войн, создаются и апробируются отдельные виды информационного оружия. Всё более опасными становятся информационные угрозы со стороны террористических организаций. Изменился характер современного глобального информационного соперничества. В системе геополитической конкуренции ведущее положение занял информационный компонент. Лавинообразно растёт международная компьютерная организованная преступность. В этих условиях информационная сфера российского государства и общества превращается в арену противоборства с иностранными конкурентами, группировками антиконституционной и экстремистской направленности, криминальными структурами и все более остро нуждается в эффективной целенаправленной защите.

Стратегия национальной безопасности РФ среди угроз национальной безопасности называет размывание традиционных российских духовно-нравственных ценностей и ослабление единства многонационального народа России, путем внешней культурной и информационной экспансии, отмечает, необходимость повышения уровня технологической безопасности, в том числе, в информационной сфере, фиксирует, что главными стратегическими угрозами национальной безопасности в области экономики являются, в том числе уязвимость информационной инфраструктуры, отмечает необходимость внедрения современных информационных и коммуникационных технологий, необходимость принятия мер по защите российского общества от внешней идейно-ценностной экспансии и деструктивного информационно-психологического воздействия, осуществления контроля в информационной сфере, отдельно выделяется важность содействия формированию системы международной информационной безопасности. Отмечается, что усилится глобальное информационное противоборство[2]. Это вызывает необходимость принятия для каждого государства соответствующих контрмер в области ИБ.

В информационном обществе информация, знания, информационные услуги и все отрасли, связанные с их производством (телекоммуникационная, компьютерная, телевизионная и др.) растут более быстрыми темпами, являются источником новых рабочих мест, становятся доминирующими в экономическом развитии. В настоящее время сложилась уникальная ситуация, когда развитие информационной сферы общества является неотъемлемым элементом общественного прогресса, однако это развитие породило новые опасности для личности, общества и государства.

---

[2] Указ Президента РФ от 31.12.2015 г. №683 "О Стратегии национальной безопасности Российской Федерации". // ИПС «ГАРАНТ». 2018.

Прогрессивное развитие человека, народов, государств и мира в целом становится существенно зависимым от уровня и степени развитости информационной сферы. Люди и государства слабо защищены от опасностей информационного характера. Данные опасности сравнимы по своим последствиям с оружием массового поражения. Информационная война может затрагивать гражданское население в гораздо большей степени, чем традиционная война. Например, в одном из печатных изданий анализировалась следующая гипотетическая ситуация[3]. Если Китай решит осуществить компьютерную атаку с целью отключения электричества в Чикаго, что приведет к гибели большого числа жителей этого города, будут ли оправданными действия США, если они используют дистанционные системы для подъема ворот плотины в Китае, что приведет к гибели жителей расположенной ниже долины? Является ли юридически, морально и политически приемлемым применение вооруженных сил в ответ на кибератаку?

Вместе с тем без новейших достижений информатизации любое общество будет отсталым, не сможет претендовать на прогрессивное развитие, переход в информационную цивилизацию. Такие общества в будущем неминуемо окажутся в разряде маргинальных, станут информационными колониями.

Информатизация практически всех сторон общественной жизни, деятельности органов государственной власти и управления бизнес-структурами существенно усилили зависимость эффективности функционирования общества и государств от состояния информационной сферы. Развитые страны уже осуществляют практическую реализацию концепции “электронного правительства”. Вместе с тем, движение к информационному обществу является постепенным и очень длительным процессом. Исходные пункты и маршруты этого движения для разных стран различны. Неравномерность мирового экономического развития ведет и к существенным различиям в степени продвижения различных стран к информационному обществу. Именно с ним связывают свое будущее народы и руководители многих стран: в США (национальная информационная инфраструктура), в Совете Европы (информационное общество) и т.д. Не отстают в разработке соответствующих программ и концепций развития информационных и телекоммуникационных технологий другие государства Европейского сообщества, азиатские страны.

Обозначились четкая тенденция: лидирующее значение приобретает всемирная паутина - Интернет**,** неоспоримым лидером которого являются США, которые, за счет своего лидерства в разработке Интернет - технологий сумели заставить мир пропускать весь информационный поток через соответствующие точки доступа к сети, находящиеся на американской территории. Однако уже сегодня рассматриваются пути оптимизации путей глобальных информационных потоков, а некоторые новаторы начинают

[3] “Virtual Defense” by James Adams. “Foreign Affairs”, 2001. Vol. 80. №. 3. May-June, pp. 98-112.

обходить общедоступную сеть с помощью “звездообразных распределительных структур”. А значит, мир стоит на пороге новой схватки за контроль над информационным пространством и “транспортом информации”. Стремительное развитие средств и систем информационного воздействия ведущих держав на информационное пространство других государств ставит проблему ускоренного развития теоретических и практических основ обеспечения информационной безопасности.

Информационный обмен между различными странами и регионами носит неравноправный характер. Информационно развитые страны, стремясь к сохранению своей монополии, используют для этого всевозможные средства, в том числе и информационные. Так, США, продвигая идею “свободы информации”, подразумевают под ней свободное распространение такой информации, которая способствует реализации и защите их национальных интересов, достижению поставленных целей. При этом существенно регламентируется содержание и сроки подачи информации.

Стремительно увеличивается информационная составляющая боевых средств, оружия и техники, то есть того, что, в конечном счете, обеспечивает решение задач непосредственно в вооруженном столкновении. Современные системы оружия по характеру и объему используемой информации, по структуре обеспечивающих информационных компонентов превращаются в системы со значительным территориальным охватом, действующие одновременно во всех сферах: на земле, на море, в воздухе и в космосе.

С накоплением в последней четверти XX века критической массы нового знания, интеллектуального ресурса человечество совершило фазовый переход от существовавшей до этого цивилизации к информационной. При этом появились возможности посредством применения искусственно созданных систем и технологий, получения и использования знаний о высших психических свойствах человека входить в его духовные, интеллектуальные сферы, оказывая позитивное или негативное воздействие. Уже сейчас автоматизация и искусственный интеллект способны изменять экономику динамичнее, чем системы управления государством, обществом, конкретными предприятиями адаптируются к этим изменениям, эта тенденция усиливается

Возрастание информационной зависимости, увеличение мощности привлекаемых для управления информационных ресурсов, повышение открытости государственного, муниципального управления и управления бизнес - структурами являются позитивными моментами эволюции общества и государства. Одновременно они несут в себе негативные явления – проникновение современных информационных технологий в сферу дезорганизации государственного, общественного и коммерческого управления на всех уровнях. Особую роль данные аспекты приобретают в современных условиях разворачивающейся мировой финансово - экономической рецессии и усиливающихся экономических санкций.

1.2. Понятийный аппарат теории информационной безопасности

Разработка научно обоснованного понятийного аппарата является необходимым условием эффективности исследований и практической деятельности в любой области. Рассмотрим проведенную в предыдущих исследованиях автора систематизацию основных понятий и определений теории информационной безопасности.[4,5,6]

Очевидно, что базовым понятием здесь является *информация*. Оно относится к важнейшим системологическим и философским категориям. Человек, как существо разумное, не может существовать вне социума, в котором созданы условия для генерирования и накопления информации различных видов. Слова основателя кибернетики Н.Винера о том, что границей общества являются пределы распространения информации, безусловно, имеют место для любой социально-технической системы[7].

Понятие "информация" (от латинского informatio - разъяснение, изложение) определяется во многих работах. Не останавливаясь на изложенных в них определениях, отметим, что такая совокупность различных мнений, в зависимости от исследуемой области знания, характеризует исключительную многогранность данного понятия. Анализ всего этого многообразия позволяет сделать вывод, что современное содержание понятия информации включает три основных аспекта: обыденный, естественнонаучный и философский.

В обыденном понимании информация - это сведения об окружающем мире и протекающих в нем процессах, воспринимаемые различными потребителями (человеком, другими живыми организмами или специальными техническими устройствами) для обеспечения целенаправленной деятельности. В данном понимании информация - сведения (сообщения, данные) о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления[8].

В естественнонаучном смысле информацию можно определить как свойство материи, состоящее в том, что в результате взаимодействия объектов между их состояниями устанавливается определенное соответствие.[9] Чем сильнее выражено это соответствие, тем полнее состояние одного объекта отражает состояние другого объекта, тем больше информации один объект содержит о другом. Материальными носителями информации являются сигналы, в качестве которых используются состояния физических полей или объектов, а соответствие между сигналом и содержащейся в нем информацией устанавливается по определенным правилам (кодам). Современное

---

[4] Родионов М.А. К вопросу о формах ведения информационной борьбы. // Военная мысль. 1998. № 2. С.67-69.
[5] Родионов М.А. Информационная безопасность (социальные аспекты). М., ВАГШ, 2004.
[6] Родионов М.А. Информационная безопасность социального развития. М., ВАГШ, 2006.
[7] Родионов М.А. Информационная безопасность (социальные аспекты). М., ВАГШ, 2004, стр.73..
[8] Федеральный закон от 27.07.2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации". // ИПС «ГАРАНТ».2018.
[9] Ф.И.Перегудов, Ф.П. Тарасенко. Введение в системный анализ. М., Высшая школа, 1989.

естественнонаучное понятие информации сформировалось из совокупности знаний, полученных разными науками. Отметим, что во многом это было обусловлено установлением тесной взаимосвязи понятия “количества информации” с другим естественнонаучным понятием - “энтропией”.

Огромное значение в развитии понятия информации принадлежит кибернетике, показавшей, что информация имеет непосредственное отношение к процессам управления и развития любых систем. В целом, с помощью теории информации и кибернетики утвердилось понимание того, что информацию можно рассматривать как нечто самостоятельное, что в различных по своей природе системах циркулируют одинаковые потоки информации, что одна и та же информация может храниться на различных физических носителях и передаваться разными по физической природе каналами. Информация стала объективной характеристикой всех материальных систем и их взаимодействия.

Стремление дать информации точные определения и количественные измерители наподобие известной формулы Шеннона сужают значение этой категории и оказываются относительно полезными для исследования отдельных определенных типов информации. В настоящее время в учении об информации сложилась ситуация, когда существует сильно развитый формальный аппарат для количественной оценки объемов информации, и в то же время недостаточно развитыми оказываются методы оценки ее качественного содержания. Информация не только является категорией, определяемой жесткими техническими характеристиками, но и обладает интеллектуально - духовным потенциалом, воздействующим на человека, на его внутренний духовный мир и сферы его деятельности.

В философском понимании информация приобрела смысл самостоятельной категории и рассматривается как фундаментальное свойство материи, являющееся аспектом свойства отражения. Рассмотрение эволюции природы и человеческого общества как процессов развития видов информации и накопления разнообразия информационных структур показывает взаимосвязь между различными уровнями организации мира, единство живой и неживой природы, позволяет с системных позиций интегрировать различные научные концепции в единую общенаучную картину мира.[10] Таким образом, естественнонаучное и философское понимание информации диалектически взаимосвязаны, что обусловлено единством их предмета исследования.

Отметим, что современной наукой по-прежнему не решена важная теоретическая и практическая проблема, связанная с количественным измерением уровней организации систем (например, в единицах энтропии). Это бы дало возможность количественно оценивать наиболее существенные свойства функционирования систем, а также понять эволюцию самосовершенствования (структурного и функционального упорядочения) объектов природы, связь живой и неживой ее форм.

---

[10] Абдеев Р.Ф. Философия информационной цивилизации. М., 1994.

Перейдем к рассмотрению других основных понятий и определений, связанных с информатизацией современного общества.

Информатика - область деятельности человеческого общества, связанная с осуществлением информационных процессов.

Информационные процессы - процессы сбора, обработки, накопления, хранения, поиска и распространения информации.

Следующие пять важных понятий и определений приведем на основе Федерального закона Российской Федерации "Об информации, информационных технологиях и о защите информации".[11]

Обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Доступ к информации - возможность получения информации и ее использования.

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

К ключевым понятиям является *информатизация*, под которой целесообразно понимать процесс развития средств информатизации и информационных технологий, а также их внедрения в различные области жизни общества. К *средствам информатизации* целесообразно отнести средства вычислительной техники, связи, управления, а также другие специальные технические средства обеспечения информационных процессов. *Средства вычислительной техники* - электронно-вычислительные машины и комплексы, персональные ЭВМ, периферийное оборудование, устройства телеобработки данных. *Средства телекоммуникации* - средства дистанционной передачи данных.

Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.[12]

Информационные технологии - целостные совокупности приемов, способов и методов применения средств информатизации (прежде всего вычислительной техники) при реализации информационных процессов. Как

[11] Федеральный закон от 27.07.2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации". // ИПС «ГАРАНТ».2018.

[12] Федеральный закон от 27.07.2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации". // ИПС «ГАРАНТ».2018.

видно из данного определения, в отличие от других существующих подходов, здесь средства информатизации не включены в понятие информационной технологии. Это логически вытекает из энциклопедического определения: технология (от греч. techne - искусство, мастерство, умение и ...логия) - это “совокупность приемов и способов получения, обработки или переработки сырья, материалов, полуфабрикатов или изделий, осуществляемых в различных отраслях промышленности, в строительстве и т.д.”. Заметим, что применительно к АСУ говорят об информационной технологии функций управления. Для того чтобы отличить появившиеся относительно недавно специфические компьютерные и сетевые технологии от уже традиционных (к которым в широком смысле можно отнести технологии, относящиеся к широкому диапазону средств информатизации от книгопечатания до телевидения, да и вообще большую часть интеллектуальной человеческой деятельности, которая почти всегда связана со сбором и обработкой информации), их часто называют *новыми информационными технологиями*.

Информационный объект - структурированная по каким-либо признакам совокупность носителей информации.

Следующие постоянно используемые понятия и определения (информационная система, информационно-телекоммуникационная сеть, электронное сообщение, документированная информация, электронный документ, оператор информационной системы, страница сайта в сети "Интернет", страница сайта в сети "Интернет", единая система идентификации и аутентификации, массовая информация, средство массовой информации) также приведены на основе Федерального закона. [13]

Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Электронное сообщение - информация, переданная или полученная пользователем информационно-телекоммуникационной сети.

Документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

Электронный документ - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

---

[13] Федеральный закон от 27.07.2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации". // ИПС «ГАРАНТ».2018.

Оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Сайт в сети "Интернет" - совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет") по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети "Интернет".

Страница сайта в сети "Интернет" - часть сайта в сети "Интернет", доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта в сети "Интернет".

Единая система идентификации и аутентификации - федеральная государственная информационная система, порядок использования которой устанавливается Правительством Российской Федерации и которая обеспечивает в случаях, предусмотренных законодательством Российской Федерации, санкционированный доступ к информации, содержащейся в информационных системах. [14]

Массовая информация - предназначенные для неограниченного круга лиц печатные, аудио-, аудиовизуальные и иные сообщения и материалы.

Средство массовой информации (СМИ) - периодическое печатное издание, сетевое издание, телеканал, радиоканал, телепрограмма, радиопрограмма, видеопрограмма, кинохроникальная программа, иная форма периодического распространения массовой информации под постоянным наименованием (названием).

Под *информационным ресурсом* понимается особый компонент среди других ресурсов государства (экономических, финансовых, социальных, научно-технических и т.д.). Структура данного компонента и функциональные связи между его элементами определяются, прежде всего, спецификой рассмотренного выше его атомарного элемента - информации. Именно уровень использования информационного ресурса обеспечивает необходимые условия для реализации всех направлений современного геополитического соперничества, одним из основных особенностей которого является стремительно идущий процесс изменения соотношения материально-энергетических и информационных ресурсов государств. В отличие от большинства других ресурсов информационные ресурсы способны самовоспроизводиться. При этом скорость появления новой информации пропорциональна уже накопленной информации, находящейся в активной, т.е. общедоступной форме. Это обеспечивает очень быстрый рост информационных ресурсов, которых будет больше в тех странах, где информация уже накоплена и переведена в удобную для использования форму.

---

[14] Федеральный закон от 27.07.2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации". // ИПС «ГАРАНТ».2018.

Таким образом, страны – лидеры в информационной области получают значительные конкурентные преимущества, которые со временем будут все более возрастать.

Отметим, что пока еще не получило достаточно четкого обоснования такое важное понятие теории информационной безопасности как информационный ресурс в авиатранспортной области. Не полностью отражают его суть и имеющиеся более общие определения, касающиеся содержания понятия информационного ресурса в общегосударственном масштабе. Даже нормативно введенное Федеральным законом определение практически сводит понятие информационного ресурса лишь к совокупности массивов документированной информации (документов). Обобщение такого определения на авиатранспортную область сужает смысл исследуемого понятия, так как множество документированной информации является лишь частью всей информации, циркулирующей в органах управления ГА и различных системах. Так, передаваемые распоряжения, команды (сигналы) по линиям связи, сведения с датчиков навигации, метеорологии и многая другая информация явно не укладываются в понятие документа. Кроме того, в этом определении не учтены такие важные аспекты информационного ресурса (обеспечивающие его генерацию и уникальные свойства делимости и воспроизводимости), как сами технические системы, осуществляющие информационные процессы, и использующий эти системы персонал.

В соответствии с изложенным в понятие *информационного ресурса в авиатранспортной области* целесообразно включить информацию, находящуюся на различных физических носителях и циркулирующую между объектами инфраструктуры системы управления, а также сами объекты последней. Такая интерпретация позволяет, в частности, более четко определить цели и объекты обеспечении ИБ собственного информационного ресурса. Так, информационная защита материальных элементов информационного ресурса (физические носители информации и объекты инфраструктуры системы управления) является лишь способом достижения цели. Собственно цель заключается в защите самой информации (ее достоверности, полноты, целостности и др.).

Информационный сектор экономики – включает в себя не все виды информационной деятельности, а только непосредственное производство информационных товаров и услуг.[15] Ядро сектора составляет *информационная индустрия* - производство компьютерной техники, средств информатизации, коммуникации и программных продуктов. Кроме того, в информационный сектор более или менее постоянно включают СМИ, различные информационно - консультационные организации, научные и проектно - конструкторские организации, рекламные и маркетинговые агентства. Новым и самым динамичным сектором информационной индустрии в настоящее время стала

[15] А.Г.Мовсесян, С.Б. Огнивцев. Мировая экономика. М., Финансы и статистика, 2001.

Интернет - экономика. Практически все основные виды экономической и финансовой деятельности используют возможности компьютерных сетей. Интернетовские и другие информационные технологии оказывают мощное воздействие не только на экономику, но и на все общество. Они постепенно формируют новую цивилизационную идентичность людей, населяющих в основном развитые страны и крупные города и повсеместно использующих в производственной деятельности и в быту новые информационные технологии.

Постиндустриальная экономика - экономика, основанная в большей степени на информации и знаниях, чем на традиционной индустрии. Здесь особо подчеркивается преобладающая роль информационного сектора над всеми отраслями материального традиционного индустриального производства.

В Доктрине информационной безопасности используется понятие *информационной сферы***,** рассматриваемой как "совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет"), сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений"[16].

Опасности и угрозы - непременные спутники жизни и деятельности индивидов, обществ, государств, человеческого сообщества на всех этапах его становления и развития. Опасности и угрозы всегда указывают на взаимодействие двух сторон: источника (носителя) опасности и объекта (на которую направлена опасность или угроза).[17]

Источники опасности — это условия и факторы, которые таят в себе и при определенных условиях сами по себе либо в различной совокупности проявляют или обнаруживают враждебные намерения, вредоносные свойства, деструктивную природу, реальные или потенциальные действия. Источники опасности могут иметь естественно - природное, техническое и социальное происхождение.

Объектом угроз и опасностей является целостная система: личность, общество, государство. К этой триаде с позиций комплексного рассмотрения можно добавить и бизнес. Личность является высшей целью общественно-политического и социально-экономического развития страны. Общество - это социальная среда и необходимое условие творчества личности в системе общественных отношений. Государство же представляет собой организационно-политический механизм реализации общественных отношений и обеспечения гарантий прав граждан, творческого развития личности как высшей национальной цели. Объектами угроз в государственном масштабе

[16] Указ Президента РФ от 05.12.2016 г. № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации", Раздел I. // ИПС «ГАРАНТ». 2018.
[17] В.И.Ярочкин. Секьюритология – наука о безопасности жизнедеятельности. М., "Ось-89", 2000.

являются практически все сферы жизни и деятельности общества. И в любой из них существуют специфические особенности опасностей и угроз.

Опасности - это возможные или реальные явления, события и процессы, способные нанести вред человеку, социальной группе, народу, обществу, государству, человеческому сообществу и Земле или даже уничтожить их; нанести ущерб их благополучию, разрушить материальные, духовные или природные ценности, вызвать деградацию, закрыть путь к развитию. Опасность может выступать в различных формах: в виде намерений, планов подготовки действий и самих действий. Разновидностью опасности выступает *риск* - возможная опасность неудачи предпринимаемых действий или сами действия, связанные с такой опасностью. В политике, экономике, финансовой и других видах деятельности обычно имеет место осознанный риск, когда тщательно рассчитываются ожидаемая выгода, цена, которую допустимо заплатить за нее, последствия и т.д. Понятие "опасность" охватывает также явления, процессы и действия, которыми люди наносят вред природе, а природа людям.

Понятие "угроза" родственно понятию "опасность". *Угроза* — это опасность на стадии перехода из возможности в действительность, высказанное намерение или демонстрация готовности одних субъектов нанести ущерб другим. *Угроза национальной безопасности* - совокупность условий и факторов, создающих прямую или косвенную возможность нанесения ущерба национальным интересам.[18]

Национальные интересы Российской Федерации в информационной сфере - объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития в части, касающейся информационной сферы[19].

Угроза информационной безопасности Российской Федерации - совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере[20].

Информационная безопасность Российской Федерации - состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства[21];

---

[18] Указ Президента РФ от 31.12.2015 г. № 683 "О Стратегии национальной безопасности Российской Федерации". // ИПС «ГАРАНТ». 2018.

[19] Указ Президента РФ от 05.12.2016 г. № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации". // ИПС «ГАРАНТ». 2018.

[20] Указ Президента РФ от 05.12.2016 г. № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации". // ИПС «ГАРАНТ». 2018.

[21] Указ Президента РФ от 05.12.2016 г. № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации". // ИПС «ГАРАНТ». 2018.

Обеспечение информационной безопасности - осуществление взаимоувязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления[22].

Многообразие опасностей, угроз и источников их возникновения (образования) требует классификации. Представляется целесообразным группировать опасности и угрозы по следующим признакам: по направленности против определенных субъектов, их интересов и потребностей, а также против тех или иных объектов (в том числе природных); по отношению к объектам воздействия (внутренние и внешние); по сферам действия (экология, экономика, политика, социальная область, духовная сфера, культура и т.д.); по масштабам (глобальные, региональные, государственные, местные и др.); по способам и формам проявления (заявления, конкретные действия, совокупность обстоятельств, которые могут породить опасность в перспективе и требуют защитного реагирования, и т.д.); по источникам и движущим силам (природные, обусловленные деятельностью людей и т.д.); по ожиданию воздействия на объекты (внезапные, неожиданные; ожидаемые, с малым временем задержки; ожидаемые, с большим временем задержки). [23]

Опасности (угрозы) могут быть классифицированы по определенным направлениям или сферам человеческой деятельности. Также угрозы могут быть классифицированы по объектам, направлениям, величине нанесенного ущерба, по вероятности возникновения, по причинам воздействия и целому ряду других признаков. К ним можно отнести и такие показатели классификации: по умыслу - правомерная (вытекающая из реализации правовых норм), противоправная, внеправовая; по форме (прямая, косвенная, завуалированная, манифестированная, латентная, несформировавшаяся); по времени (мгновенная, длящаяся, дискретная, законсервированная); по последствиям (необратимая, обратимая, мутагенная, доминантная, катализирующая); по направлениям (внешняя, внутренняя); по значению (допустимая, недопустимая); по составу (разовая, бинарная, кумулятивная, диффузная); по природе происхождения (социальная, техногенная, природная); по актуализации (вероятная, потенциальная, реальная, осуществленная); по причинности (закономерная, случайная).

Перейдем к рассмотрению понятия *информационной безопасности*. Информационная безопасность обеспечивается устранением информационных угроз данному субъекту (личности, обществу, государству, различным организациям), либо, при наличии информационных угроз, обеспечением достаточной защищенности по отношению к ним. Другая сторона обеспечения

[22] Указ Президента РФ от 05.12.2016 г. № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации". // ИПС «ГАРАНТ». 2018.
[23] В.И. Ярочкин. Секьюритология – наука о безопасности жизнедеятельности. М., “Ось-89”, 2000.

информационной безопасности связана с воздействием на информационные ресурсы (прежде всего, средств и систем информационного воздействия) потенциально опасных конкурентов.

В Доктрине информационной безопасности Российской Федерации под информационной безопасностью понимается "- состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства"[24].

При этом, *интересы личности в информационной сфере* заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества. На основе национальных интересов России в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики по обеспечению информационной безопасности.

Дестабилизирующий фактор информационной безопасности - явление или событие, следствием которого могут быть такие воздействия на информационные ресурсы, которые могут привести к недопустимому снижению их качества. При этом под качеством информационного ресурса понимается совокупность его свойств, обеспечивающих удовлетворение информационных потребностей субъекта в рассматриваемой деятельности.

---

[24] Указ Президента РФ от 05.12.2016 г. № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации". Раздел I. // ИПС «ГАРАНТ». 2018.

Угроза информационной безопасности - совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере[25];

Источники угроз информационной безопасности - это дестабилизирующие факторы, а также социальная, техническая, биологическая, природная и иная среда их появления, системы, средства и люди, общественные и государственные организации. Например, внутренними угрозами информационной безопасности РФ являются: отставание России от ведущих стран мира по уровню информатизации, отсутствие четко сформулированной информационной политики, отвечающей национальным целям, ценностям и интересам и другие.

Главными направлениями обеспечения государственной и общественной безопасности являются усиление роли государства в качестве гаранта безопасности личности и прав собственности, совершенствование правового регулирования предупреждения преступности (в том числе в информационной сфере), коррупции, терроризма и экстремизма, распространения наркотиков и борьбы с такими явлениями, развитие взаимодействия органов обеспечения государственной безопасности и правопорядка с гражданским обществом, повышение доверия граждан к правоохранительной и судебной системам Российской Федерации, эффективности защиты прав и законных интересов российских граждан за рубежом, расширение международного сотрудничества в области государственной и общественной безопасности.[26]

Одной из важнейших форм обеспечения информационной безопасности выступает *информационная борьба* – соперничество в информационной области за достижение превосходства в своевременности, достоверности, полноте получения информации, в скорости и качестве ее переработки.[27] Такая борьба включает следующие направления деятельности: добывание необходимой информации, переработка полученной информации, защита своих информационных ресурсов от противоправного доступа, использование более эффективных средств работы с информацией, воздействие на информационные ресурсы конкурентов и др.

В Соглашение между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (Екатеринбург, 16.06.2009 г.). Термин *"информационная война"* определяется как "противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальных систем, массированной психологической

---

[25] Указ Президента РФ от 05.12.2016 г. № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации". Раздел I. // ИПС «ГАРАНТ». 2018.

[26] Указ Президента РФ от 31.12.2015 г. № 683 "О Стратегии национальной безопасности Российской Федерации". // ИПС «ГАРАНТ». 2018.

[27] Родионов М.А. К вопросу о формах ведения информационной борьбы. // Военная мысль. 1998. № 2. С.67-69.

обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны"[28].

Одним из ключевых понятий теории информационной безопасности является информационное оружие. Окончательного законодательного определения информационного оружия пока нет. В ряде источников оно рассматривается как средства уничтожения, искажения или хищения информации; средства преодоления систем защиты; средства ограничения допуска законных пользователей; средства дезорганизации работы технических средств, компьютерных систем[29]. В концепции Конвенции об обеспечении международной информационной безопасности[30] «информационное оружие» определяется, как информационные технологии, средства и методы, предназначенные для ведения информационной войны.

На наш взгляд, необходимо четко различать использование сил и средств, привлекаемых к мероприятиям информационной борьбы, и собственно информационного оружия. К последнему могут быть отнесены: средства радиоэлектронного поражения (подавления), средства специального-программно-математического воздействия (компьютерные вирусы; программные закладные устройства; средства их внедрения в информационные системы, позволяющие управлять ими на расстоянии), средства массовой информации (в том числе синтезаторы аудио- и видеосообщений), голографические изображения в атмосфере, психотронные генераторы, специальные фармакологические средства и др. Основными чертами информационного оружия, объектом воздействия которого является информационный ресурс контр-партнера, являются: универсальность, скрытность, радикальность воздействия, широкий диапазон временных и пространственных характеристик применения, экономичность.

Таким образом, под *информационным оружием* целесообразно понимать технические, программные и иные специальные средства информационной борьбы, воздействующие на информационный ресурс противника. Необходимо отметить, что информационное оружие относится к так называемому *нелетальному (несмертельному) оружию*, под которым понимаются средства воздействия на людей и технику, созданные на основе химических, биологических, физических и иных принципов. Такое оружие выводит контр-партнера из строя в течение определенного времени.

---

[28] Соглашение между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (Екатеринбург, 16 июня 2009 г.). // ИПС «ГАРАНТ». 2018.

[29] Расторгуев С.П. Информационная война. М.: Радио и связь, 1999. С. 56.

[30] Официальный сайт МИД России. Конвенция об обеспечении международной информационной безопасности (концепция). 22.09.2011. // URL: http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/ content/id/191666

1.3. Содержание и принципы информационной безопасности

Важным аспектом теории информационной безопасности является вопрос о ее содержании и, прежде всего, направлениях ее ведения (составных частях). Отметим, что информационные опасности и угрозы не существуют сами по себе, они тесно взаимосвязаны и приводят к определенным конфликтным ситуациям, выражающимся часто в усложнении отношений сторон. Взаимодействие сторон в социально-политических и экономических конфликтах может происходить на разных уровнях, в том числе и на уровне информационной борьбы.

В соответствии с ранее разработанным автором подходом в качестве направлений обеспечения (составных частей) информационной безопасности целесообразно выделить следующие: информационное обеспечение, информационную защиту своего информационного ресурса и информационное воздействие на контр-партнеров[31,32].

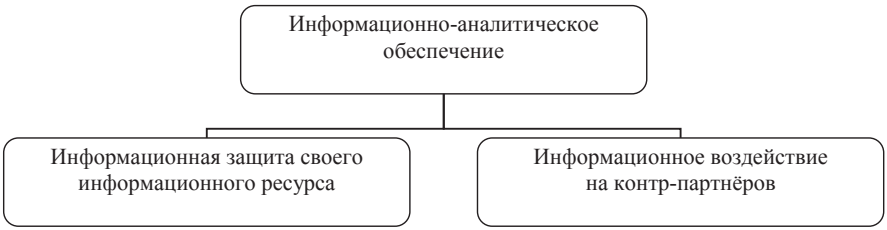

Рис.1. Составные части информационной безопасности

Информационное обеспечение включает сбор, обработку, хранение, передачу информации, прогнозирование изменения обстановки. Информационно-аналитическое обеспечение - это базовая часть системы, предназначенная для разработки стратегии обеспечения информационной безопасности, планирования, организации и обеспечения деятельности двух других подсистем.

Информационная защита объектов своего информационного ресурса предполагает защиту от негативного информационно-технического и информационно - психологического воздействия (как непреднамеренного, так и со стороны контр-партнеров). Информационная защита включает комплекс организационных, технических и психологических мероприятий, направленных на обеспечение эффективности непрерывного функционирования своей информационной системы.

---

[31] Родионов М.А. К вопросу о формах ведения информационной борьбы. // Военная мысль. 1998. № 2. С.67-69.
[32] Родионов М.А. Информационная безопасность (социальные аспекты). М., ВАГШ, 2004. С.132-134.

Информационное воздействие на объекты информационного ресурса контр-партнеров предполагает воздействие на психику должностных лиц, информационно-технические системы различного масштаба и назначения, системы формирования, распространения и использования информационных ресурсов, систему формирования общественного сознания (с помощью пропаганды и СМИ), систему формирования и функционирования общественного мнения, систему принятия управленческих решений. Информационное воздействие на контр-партнёров включает комплекс организационных и технических мероприятий, состоящих в информационном воздействии на информационные ресурсы контрпартнёров (в том числе с целью управление их действиями).

В зависимости от объекта защиты или воздействия информационная безопасность может быть информационно-психологической, для которой объектом выступает общество, большие социальные группы, отдельные должностные лица, личности, и информационно-технической, нацеленной на технические средства и системы.

На авиапредприятии, в качестве средств обеспечения информационной безопасности, используются как информационно-технические средства, так и методы информационно-психологического влияния на персонал и руководство.

Комплексный характер мероприятий по обеспечению информационной безопасности предприятия обусловлен тем, что обеспечение ИБ - это сложная система неразрывно взаимосвязанных и взаимозависимых процессов, каждый из которых, в свою очередь, имеет множество различных взаимосвязанных сторон, свойств, тенденций. Все вышеупомянутые понятия и определения в области информационной безопасности применимы и для любого авиапредприятия. Нередко для авиатранспортной отрасли эти вопросы более актуальны, чем для многих других отраслей, так как приоритетным принципом в сфере гражданской авиации является безопасность.

При обеспечении информационной безопасности, прежде всего, возникают вопросы определения объектов и субъектов, средств и принципов обеспечения ИБ, источников и направленности опасных информационных потоков. Объектами опасного информационного воздействия могут выступать сознание (индивидуальное и общественное), психика отдельных людей и их объединения, информационные системы различного масштаба и назначения. Субъектами информационной безопасности следует, считать те органы и структуры, которые в той или иной мере занимаются ее обеспечением. На государственном уровне ими являются органы исполнительной, законодательной и судебной власти. В отдельных ведомствах созданы органы, специально занимающиеся ИБ. Применительно к конкретным предприятиям это конкретные органы организаций и (или) отдельные должностные лица.

Обеспечение ИБ предполагает разработку и реализацию определенных принципов. Отметим некоторые из них.

Одним из важнейших является принцип баланса интересов личности, общества, государства и бизнеса. Также следует отметить принцип законности и правой обеспеченности. Рост значимости информационной безопасности явно опережает развитие соответствующей сферы права, чем умело пользуются недобросовестные контр-партнеры и просто отдельные злоумышленники.

Принцип экономической эффективности состоит в том, что результаты от мероприятий ИБ должны превышать совокупные затраты на них. На практие это далеко не всегда соблюдается. Создать надежную на 100% систему информационной безопасности организации невозможно. Самая надежная система ИБ не защитит от угроз, которые неизвестны, но кем-то разрабатываются. Необходимым условием эффективности системы ИБ является качество работы обслуживающего ее персонала, который не застрахован от непреднамеренных ошибок. При наличии достаточного количестве времени и необходимых средствах теоретически можно преодолеть любую защиту. Поэтому имеет смысл стоит говорить лишь об обеспечении такого уровня информационной безопасности, при котором стоимость преодоления защиты становится намного больше стоимости получаемой при этом информации или когда за время реализации процесса добывания информации она обесценивается настолько, что усилия злоумышленника по ее получению теряют смысл.

Важен принцип о том, что система ИБ должна быть мобильной, не допускать неоправданных режимных ограничений, так как одновременно с ограничениями государство, организация утрачивает способность создавать и генерировать новые знания. Принцип презумпции несекретности информации означает, что строгому нормированию подлежит конфиденциальность, а не гласность. Принцип системности позволяет увидеть отличие научного понимания ИБ от обыденного. Он предполагает необходимость учета всех взаимосвязанных, взаимодействующих элементов, условий и факторов, критически значимых для обеспечения ИБ в динамике обстановки, программно-целевое планирование развития системы ИБ.

В повседневной жизни ИБ понимается лишь как необходимость борьбы с утечкой конфиденциальной и распространением ложной и информации.

Создание системы информационной безопасности предполагает также выявление источников информационных опасностей.[33] На авиапредприятии очень четко классифицируются эти источники, и в соответствии с ними редактируется стандартная модель системы информационной безопасности предприятия. Эти источники логично классифицировать на естественные и искусственные, на объективные (не зависящие от воли людей) и субъективные (зависящие), на случайные и умышленные. Важно помнить, что естественные информационно-опасные воздействия существуют изначально в природе или возникают в результате аномалий, случайных

[33] Фитисов В. Автоматизация телепроизводства – стратегии современности. // Журнал "Broadcasting. Телевидение и радиовещание" №5, 2008.

факторов, стихийных бедствий и т.д. Искусственные источники создаются людьми. Техносфера являет источником опасностей информационной природы вследствие непреднамеренных ошибок и неисправностей. Умышленные информационно-опасные воздействия осуществляются сознательно и целенаправленно. При этом часто используются специально созданные (искусственные) средства - всем известные средства массовой информации, уникальные программные пакеты для компьютеров и т.п. В целом, по отношению к информационным ресурсам проявляются угрозы целостности надежности, конфиденциальности, полноты и доступности. Информационные технологии должны обладать способностью к недопущению или нейтрализации воздействия как внешних, так и внутренних угроз информации, содержать в себе адекватные методы и способы ее защиты.

1.4. Роль и место бизнес-процессов обеспечения информационной безопасности в управлении современными авиапредприятиями

Все более широкое использование в ГА современных информационных технологий, с одной стороны, способствует более качественному и быстрому предоставлению соответствующих транспортных услуг, с другой стороны, создает угрозы безопасности информационного обмена между субъектами авиатранспортной отрасли, что влечет за собой негативные последствия.

Вторжение в информационную сферу авиатранспортного предприятия несет угрозы несанкционированного доступа к информации о его деятельности, искажения достоверности, целостности, релевантности информации (о пассажиропотоках, персонале организаций, воздушной обстановке, параметрах полетов, метеорологических условиях и т.п.). Данные обстоятельства могут негативно повлиять на процессы планирования, организацию управления воздушным движением, процессы технического обслуживания и ремонта воздушных судов, обслуживания пассажиров, перевозку багажа, почты и грузов и т.д., что, в конечном итоге ведет к снижению уровня безопасности полетов и авиационной безопасности. Выявление и устранение технологических угроз для информационных систем, психологических уязвимостей персонала, является критически важной задачей при решении вопросов обеспечения ИБ авиатранспортных предприятий.

Безопасность объектов ГА представляет собой состояние авиационной транспортной системы, при котором риск причинения вреда лицам или нанесения ущерба имуществу снижен до приемлемого уровня и поддерживается на этом либо более низком уровне посредством непрерывного процесса выявления источников опасности и контроля факторов риска.[34] В соответствии с подходами ИКАО государственная политика обеспечения

[34] Никулин Н.Ф. Обеспечение авиационной безопасности в авиапредприятиях гражданской авиации»: Учебное пособие. – СПб, Академия ГА 1997 г. С.129.

безопасности ГА заключается в комплексе правил и мер, направленных на повышение уровня безопасности пассажиров, работников авиатранспортной отрасли, а также транспортной инфраструктуры. При обеспечении безопасности важно учитывать бурный рост объемов перевозок, развитие транспортной инфраструктуры, качество подготовки авиационных специалистов и др. Управление ИБ авиапредприятия включает планирование организационных мероприятий по выявлению и устранению рисков ИБ, организацию взаимодействия по вопросам предотвращения авиационных происшествий всех участников авиатранспортной системы при осуществлении перевозок, расследование авиационных событий и инцидентов. Затраты на мероприятия по обеспечению ИБ должны окупаться за счет сокращения размеров ущерба от информационных происшествий.

Современный менеджмент базируется на процессном подходе, при котором любая деятельность в организации рассматривается как *процесс,* преобразующий входные ресурсы в выходные (как материальные, так и нематериальные). При этом выходы могут быть непланируемыми и непреднамеренными, например, загрязнение окружающей среды. В такой интерпретации предприятие рассматривается как совокупность *бизнес-систем,* каждая из которых представляет собой взаимодействие бизнес-процессов, конечными целями которых является выпуск продукции или услуги[35]. При этом под *бизнес-процессом* понимается определенная цепочка различных видов деятельности, которые в совокупности создают результат (продукт, услугу, в том числе информационный), имеющий ценность для конечного потребителя, клиента или заказчика. В качестве заказчика может выступать другой бизнес-процесс. В цепочку может входить деятельность подразделений, находящихся на различных уровнях организационной структуры фирмы.

При этом под управлением бизнес-процессами понимается целенаправленное воздействие на них для достижения целей организации посредством их *совершенствования* и *контроля.* Это предполагает практическое осуществление стратегических целей, поставленных на уровне высшего руководства организацией. На уровне конкретного проекта это предполагает создание ценности или извлечение выгоды для фирмы в целом.

Бизнес-процессы организации можно подразделить на четыре группы[36]:

1. Основные бизнес-процессы.
2. Обеспечивающие бизнес-процессы.
3. Бизнес-процессы управления
4. Бизнес-процессы развития.

Основные бизнес-процессы – непосредственно ориентированные на производство продукции, представляющие ценность для клиента и обеспечивающие получение дохода для предприятия.

---

[35] Васильева И.Н. Управление информационной безопасностью. Учебное пособие. СПб.: Изд-во СПбГЭУ, 2014. С. 37-40.

[36] Корягин Н.Д. Бизнес-анализ. Учебное пособие. М., МГТУ ГА, 2017. С.17-18.

Обеспечивающие бизнес-процессы – вспомогательные бизнес-процессы, которые предназначены для обеспечения выполнения основных процессов. Фактически обеспечивающие бизнес-процессы снабжают ресурсами всю деятельность организации.

Бизнес-процессы управления – это бизнес-процессы, охватывающие весь комплекс функций управления на уровне текущих действий и бизнес-системы в целом.

Бизнес-процессы развития – процессы совершенствования, освоения новых направлений и технологий, а также инновации.

Для выработки управленческих решений по всем видам бизнес-процессов разрабатывается соответствующая система показателей и критериев количественной и качественной оценки.

При уточнении роли и места бизнес-процессов обеспечения ИБ в управлении современными авиапредприятиями отметим следующее. Процессы обеспечения ИБ базируются, прежде всего, на обеспечении безопасности и эффективном использовании информационных ресурсов организации. Информационные ресурсы, в свою очередь, обеспечиваются, прежде всего, информационной инфраструктурой авиапредприятия, технически и сервисно сопровождающей бизнес-процессы. Под информационной инфраструктурой можно понимать комплекс различных информационных систем и технологий, с использованием которых предоставляются ресурсы, возможности, услуги, необходимые для функционирования предприятия и выполнения соответствующих бизнес-задач. Все это позволяет осуществить разработку и эффективное использование инфраструктуры системы ИБ в системной взаимосвязи с проектированием и реализацией имеющихся бизнес-процессов. Последнее условие необходимо для повышения эффективности (системности, адаптируемости, сбалансированность, оперативности, управляемости и т.п.) самих бизнес-процессов.

Необходимым условием безопасности функционирования и развития информационной инфраструктуры авиапредприятия является ее ИБ. Только в этом случае можно обеспечить непрерывное эффективное функционирование ИБ инфраструктуры бизнес-процессов предприятия. Таким образом, процессный подход позволяет рассматривать процесс формирования (развития) системы ИБ авиапредприятия как один из *вспомогательных (инфраструктурных) процессов,* обеспечивающих основные бизнес-процессы и другие инфраструктурные процессы авиапредприятия. [37]

[37] Васильева И.Н. Управление информационной безопасностью. Учебное пособие. СПб. : Изд-во СПбГЭУ, 2014. С. 43-44.

Глава 2. Нормативное правовое обеспечение и стандарты информационной безопасности

2.1. Международное законодательство в сфере информационной безопасности

Правовой аспект информационной безопасности, является важным компонентом общей системы обеспечения безопасности авиапредприятия. Использование информационных технологий без увязки с нормативным правовым обеспечением информационной безопасности существенно повышает вероятность возникновения и проявления информационных угроз.

На саммите руководителей восьми ведущих стран мира в Окинаве 22 июля 2000 г. (Япония) была подписана "Окинавская хартия глобального информационного общества". Таким образом, была сделана попытка перевести вопросы формирования мирового информационного сообщества в плоскость практических решений. В данном документе на декларативном уровне было отмечено стремление к созданию нормативной базы, регулирующей международные информационные отношения. К основным положениям документа можно отнести: призыв ко всем странам и народам ликвидировать международный разрыв в области информации и знаний; общество 21 века – это информационное общество; «Восьмерка» взяла обязательство укреплять нормативную базу и бороться с преступностью в информационной сфере; Были даны основные рекомендации государствам в информационной политике (развитие конкуренции, защита прав интеллектуальной собственности, использование лицензированных продуктов, развитие электронной торговли, защита жизни потребителя, создание безопасного киберпространства); главной политической стратегией определено обеспечение всеобщего доступа к глобальным информационно-телекоммуникационным сетям; Для реализации этой стратегии были определены соответствующие приоритетные области.

Конвенция о международной ГА (Чикаго, 07.12.1944 г.), вступила в силу 04.04.1947 г. Русский текст Конвенции, аутентичный английскому, французскому и испанскому, был принят на Монреальской конференции по воздушному праву 30 сентября 1977 г.[38]

Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23.11.2001 г.), вступила в силу 01.07.2004 г., Россия не участвует в данном международном договоре.

Шанхайская организация сотрудничества (ШОС) в 2006 г. приняла Заявление глав государств-членов по международной информационной безопасности, в котором выражена озабоченность реальной опасностью использования информационных и коммуникационных технологий (ИКТ) в целях, способных нанести серьезный ущерб безопасности человека, общества и

[38] Официальный сайт ИКАО. URL: https://www.icao.int/Pages/default.aspx

государства в нарушение основополагающих принципов равноправия и взаимного уважения, невмешательства во внутренние дела суверенных государств, мирного урегулирования конфликтов, неприменения силы, соблюдения прав человека. В 2007 г. в рамках ШОС утверждён Долгосрочный план действий по ИБ, в котором прописаны необходимые меры для противодействия использования ИКТ в террористических целях, обеспечения безопасного, стабильного функционирования и интернационализации управления глобальной сетью Интернет.[39] Соглашение между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной ИБ (Екатеринбург, 16.06.2009 г.), вступило в силу, для России 02.06.2011 г.[40]

Россия всегда выступала против разрешения межгосударственных противоречий в информационной сфере нецивилизованными способами. Именно по инициативе России была принята резолюция Генеральной Ассамблеи ООН A/RES/65/41 от 08.12.2010 г. «Достижения в сфере информатизации и коммуникаций в контексте международной безопасности».

Позже, Генассамблея ООН на 70-й сессии в 2015 г. приняла российскую резолюцию "Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности". Соавторы резолюции - более 80 государств мира, среди которых страны-участницы БРИКС, ШОС, СНГ, латиноамериканские и азиатские государства, а также впервые - США, Япония и многие члены ЕС, включая Великобританию, Германию, Испанию, Нидерланды и Францию. Указывается, что "удалось достичь консенсуса по целому ряду принципиальных вопросов, связанных с использованием ИКТ, в частности, по поводу того, что: технологии должны использоваться исключительно в мирных целях, а международное сотрудничество необходимо нацелить на предотвращение конфликтов в информационном пространстве; в цифровой сфере действуют такие общепризнанные международно-правовые принципы, как неприменение силы или угрозы силой, уважение суверенитета, невмешательство во внутренние дела государств; государства обладают суверенитетом над информационно-коммуникационной инфраструктурой на своей территории; любые обвинения в адрес государств в причастности к кибератакам должны быть подкреплены доказательствами; государства не должны использовать посредников для осуществления кибератак и не допускать того, чтобы их территории использовались в этих целях; государства должны бороться с использованием скрытых вредоносных функций - так называемых "закладок" - в ИТ-продукции"[41].

---

[39] Официальный сайт ШОС. 27.11.2016. URL: http://rus.sectsco.org/news/20161127/160697.html

[40] Соглашение между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (Екатеринбург, 16.06.2009 г.). // ИПС «ГАРАНТ» 2018.

[41] Официальный сайт МИД РФ. О принятии Первым комитетом Генассамблеи ООН резолюции "Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности" // http://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/cont ent/id/1922990.

Стоит отметить, что Институт проблем информационной безопасности Московского государственного университета совместно и Советом Безопасности и МИД России в 2011 г. разработали Концепцию Конвенции об обеспечении международной информационной безопасности[42]. Конвенция открыта для подписания ее всеми государствами, присоединились к конвенции Китай и Индия, с которыми в 2012 г. были проведены переговоры о методах контроля над распространением информации в сети Интернет.

В качестве основных угроз в информационном пространстве, приводящих к нарушению международной безопасности, рассматриваются следующие:

использование информационных технологий и средств для осуществления враждебных действий и актов агрессии;

целенаправленное деструктивное воздействие в информационном пространстве на критически важные структуры другого государства;

неправомерное использование информационных ресурсов другого государства без согласования с государством, в информационном пространстве которого располагаются эти ресурсы;

действия в информационном пространстве с целью подрыва политической, экономической и социальной систем другого государства, психологическая обработка населения, дестабилизирующая общество;

использование международного информационного пространства структурами, организациями, группами и отдельными лицами в террористических, экстремистских и иных преступных целях;

трансграничное распространение информации, противоречащей принципам и нормам международного права, а также национальным законодательствам государств;

использование информационной инфраструктуры для распространения информации, разжигающей межнациональную, межрасовую и межконфессиональную вражду, расистских и ксенофобских материалов, изображений или других представлений идей, пропагандирующих, способствующих ненависти, дискриминации, насилию, если в качестве предлога к этому используются факторы, основанные на расе, цвете кожи, национальном или этническом происхождении, религии;

манипулирование информационными потоками других государств, дезинформация и сокрытие информации с целью искажения психологической и духовной среды общества, эрозия традиционных культурных, нравственных, этических и эстетических ценностей;

использование ИКТ и средств в ущерб основным информационным правам и свободам человека; противодействие доступу к новейшим ИКТ, создание условий технологической зависимости в сфере информатизации в ущерб другим государствам;

---

[42] Официальный сайт МИД России. Конвенция об обеспечении международной информационной безопасности (концепция). 22.09.2011. // URL: http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/ content/id/191666

информационная экспансия, приобретения контроля над национальными информационными ресурсами другого государства.

Дополнительными факторами, усиливающими опасность перечисленных угроз, являются: неопределенность в идентификации источника враждебных действий, особенно с учетом возрастающей активности отдельных лиц и организаций, включая преступные организации; потенциальная опасность включения в ИКТ недекларируемых деструктивных возможностей; различия в степени оснащенности ИКТ и их безопасности в разных государствах; различия в национальных законодательствах и практике формирования безопасной и быстро восстанавливающейся информационной инфраструктуры[43].

В конвенции отмечается, что информационное пространство является общечеловеческим достоянием, его безопасность является основой обеспечения устойчивого развития цивилизации. Для создания и поддержания атмосферы доверия в информационном пространстве необходимо соблюдение государствами-участниками (далее - государствами) следующих принципов:

деятельность в информационном пространстве должна способствовать социальному и экономическому развитию быть совместимой с задачами поддержания международной безопасности, соответствовать общепризнанным принципам и нормам международного права, неприменения силы, невмешательства во внутренние дела других государств, уважения суверенитета государств, основных прав и свобод человека;

государства в ходе формирования системы международной ИБ будут руководствоваться принципом неделимости безопасности, означающим, что безопасность каждого из них неразрывно связана с безопасностью всех других государств и мирового сообщества в целом, а также не будут укреплять свою безопасность в ущерб безопасности других государств;

государство должно стремиться к преодолению различий в степени оснащенности национальных информационных систем современными ИКТ, сокращению «цифрового разрыва» в целях снижения общего уровня угроз в информационном пространстве;

все государства в информационном пространстве пользуются суверенным равенством, имеют одинаковые права и обязанности и являются равноправными субъектами информационного пространства независимо от различий экономического, социального, политического или иного характера;

государство вправе устанавливать суверенные нормы и управлять в соответствии с национальными законами своим информационным пространством. Суверенитет и законы распространяются на информационную инфраструктуру, расположенную на территории государства-участника или иным образом находящуюся под его юрисдикцией. Государства должны стремиться к гармонизации национальных законодательств, различия в них не

[43] Официальный сайт МИД России. Конвенция об обеспечении международной информационной безопасности (концепция). 22.09.2011. // URL: http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/ content/id/191666

должны создавать барьеры на пути формирования надежной и безопасной информационной среды;

государство должно придерживаться принципа ответственности за собственное информационное пространство, в том числе за его безопасность и за содержание размещаемой в нем информации;

государство имеет право свободно осуществлять без вмешательства извне развитие своего информационного пространства, каждое другое государство обязано уважать это право в соответствии с принципом равноправия и самоопределения народов, закрепленного в Уставе ООН;

государство, учитывая законные интересы безопасности других государств, может самостоятельно определять свои интересы обеспечения ИБ на основе суверенного равенства, а также свободно выбирать способы обеспечения собственной ИБ в соответствии с международным правом;

государства признают, что агрессивная «информационная война» составляет преступление против международного мира и безопасности;

информационное пространство государства не может быть объектом приобретения другой страной в результате угрозы силой или ее применения;

государство имеет неотъемлемое право на самооборону перед лицом агрессивных действий в информационном пространстве при условии достоверного установления источника агрессии и адекватности ответных мер;

государство будет определять свой военный потенциал в информационном пространстве на основе национальных процедур с учетом законных интересов других государств, необходимости содействовать укреплению международной безопасности. Не должно быть попыток добиться господства в информационном пространстве над другими государствами;

государство может размещать свои силы и средства ИБ на территории другой страны в соответствии с соглашением на добровольной основе в ходе переговоров, в соответствии с международным правом;

государство-участник принимает необходимые меры для обеспечения невмешательства в деятельность международных информационных систем управления транспортными, финансовыми потоками, средствами связи, средствами международного информационного, в т.ч. научного и образовательного обмена, исходя из того, что подобное вмешательство может негативно повлиять на информационное пространство в целом;

государства должны поддерживать и стимулировать научно-технические разработки в области освоения информационного пространства, а также образовательно-просветительскую деятельность, направленную на формирование глобальной культуры кибербезопасности;

государство в рамках имеющихся средств обеспечивает в своем информационном пространстве соблюдение основных прав и свобод человека и гражданина, соблюдение прав на интеллектуальную собственность, включая патенты, технологии, коммерческую тайну, торговые марки и авторские права;

государство гарантирует свободу слова, мнений в информационном пространстве, защиту от незаконного вмешательства в частную жизнь граждан;

государство стремится к соблюдению баланса между основными свободами и эффективным противодействием террористическому использованию информационного пространства;

государства не вправе ограничивать или нарушать доступ граждан к информационному пространству, кроме как в целях защиты национальной и общественной безопасности, а также предотвращения неправомерного использования и несанкционированного вмешательства в национальную информационную инфраструктуру;

государства-участники стимулируют партнерство бизнеса и гражданского общества в информационном пространстве;

государства-участники признают свои обязанности по обеспечению осведомленности своих граждан, общественных и государственных органов, других государств и мирового сообщества о новых угрозах в информационном пространстве и об известных путях повышения уровня их безопасности[44].

Против подписания Конвенции выступают США, указывая в качестве аргументов, тот факт, что свободное перемещение информации является основным правом, а конвенция является попыткой России и других стран ввести цензуру в СМИ. Государства, предлагающие конвенцию, преследуют цели создать национальные барьеры в киберпространстве, что будет ограничивать свободу интернет-пространства.

В постсоветский период российские дипломаты неоднократно распространяли среди членов Совета Безопасности ООН разработанные Россией и другими странами проекты договоров о контроле над вооружениями и предотвращении угроз в киберпространстве. Однако США и их союзники отвергали и продолжают игнорировать эти предложения, считая их попыткой страны, проигравшей информационную войну (при этом имеется в виду “холодная война” между США и СССР) , обеспечить свою безопасность.

2.2. Основные законодательные акты Российской Федерации по вопросам информационной безопасности

Основные законы и нормативно-правовые акты Российской Федерации в области информационной безопасности:

1. Конституция РФ принята на всенародном голосовании 12.12.1993 г.
2. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне».
3. Федеральный закон от 29.12.1994 № 77-ФЗ «Об обязательном экземпляре документов».

[44] Официальный сайт МИД России. Конвенция об обеспечении международной информационной безопасности (концепция). 22.09.2011. // URL: http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/ content/id/191666

4. Федеральный закон от 27.12.2002. № 184-ФЗ "О техническом регулировании".

5. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

6. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации".

7. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных".

8. Федеральный закон от 09.02.2007 №16-ФЗ "О транспортной безопасности".

9. Федеральный закон от 06.04.2011 г. № 63-ФЗ "Об электронной подписи".

10. Федеральный закон от 26.07.2017. № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации".

11. Указ Президента РФ от 17.03.2008 № 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена".

12. Указ Президента РФ от 22.05.2015 № 260 "О некоторых вопросах информационной безопасности Российской Федерации".

13. Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации".

14. Указ Президента РФ от 09.05.2017 № 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 гг.".

15. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 г. (утв. Президентом РФ 24.07.2013., № Пр-1753).

16. Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

17. Постановление Правительства РФ от 28.07.2018 № 886 “Об утверждении требований по обеспечению транспортной безопасности, в том числе требований к антитеррористической защищенности объектов (территорий), учитывающих уровни безопасности для различных категорий объектов транспортной инфраструктуры и транспортных средств воздушного транспорта”.

18. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 г., где определены главные угрозы в области международной информационной безопасности, цель, задачи и приоритетные направления государственной

политики Российской Федерации в области международной информационной безопасности, а также механизмы их реализации.[45]

19. Приказ ФСТЭК России от 18.02.2013 № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных";

20. Приказ ФСБ России от 10.07.2014 № 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности";

21. Приказ Минтранса РФ от 18.04.2008 № 62 "Об утверждении Программы авиационной безопасности гражданской авиации Российской Федерации".

Российская Федерация подписала с рядом зарубежных стран Соглашения о сотрудничестве в области обеспечения международной ИБ:

1. Решение о Положении о сотрудничестве государств-членов Организации Договора о коллективной безопасности в сфере обеспечения информационной безопасности (Москва, 10.12.2010 г.).

2. Соглашение между Правительством Российской Федерации и Правительством Федеративной Республики Бразилии о сотрудничестве в области обеспечения международной информационной и коммуникационной безопасности (Москва, 14.05.2010 г.).

3. Распоряжение Правительства РФ от 17.09.2013 № 1672-р "О подписании Соглашения между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности".

4. Распоряжение Правительства РФ от 15.11.2013 № 2120-р "О подписании Соглашения о сотрудничестве государств - участников Содружества Независимых Государств в области обеспечения информационной безопасности".

5. Распоряжение Правительства РФ от 10.07.2014 № 1271-р "О подписании Соглашения между Правительством Российской Федерации и Правительством Республики Куба о сотрудничестве в области обеспечения международной информационной безопасности".

6. Распоряжение Правительства РФ от 30.04.2015 № 788-р "О подписании Соглашения между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности".

---

[45] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утв. Президентом РФ 24.07.2013 г., № Пр-1753). // ИПС «ГАРАНТ» 2018.

7. Распоряжение Правительства РФ от 16.07.2009 № 984-р "Об утверждении Соглашения между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности".

8. Распоряжение Правительства РФ от 04.07.2017 № 1424-р "О подписании Соглашения между Правительством Российской Федерации и Правительством Южно-Африканской Республики о сотрудничестве в области обеспечения международной информационной безопасности".

9. Распоряжение Правительства РФ от 05.09.2018 № 1848-р "О подписании Соглашения между Правительством Российской Федерации и Правительством Социалистической Республики Вьетнам о сотрудничестве в области обеспечения международной информационной безопасности"; и др.

Рассмотрим основные положения наиболее важных законов и нормативных правовых актов.

Конституция РФ[46], обладая высшей юридической силой, устанавливает основные принципы в сфере защиты информации. В статье 23 указывается, что возможность предоставления государственным органам полученной в результате профессиональной деятельности информации о частной жизни граждан допускается только если это прямо предусмотрено федеральным законом. За нарушение неприкосновенности частной жизни предусмотрена уголовная ответственность. Статья 24 предусматривает право на охрану информации, которой люди обмениваются между собой. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Статья 28 Конституции устанавливает, что важнейшими личными правами человека является свобода совести, вероисповедания. Федеральный закон "О свободе совести и о религиозных объединениях" не допускает установления преимуществ либо ограничений в зависимости от отношения человека к религии.[47] Статья 29 Конституции закрепляет свободу мысли. Сама по себе мысль не наносит вреда обществу независимо от ее содержания, пока она не воплотилась в конкретное деяние. Гарантируется свобода массовой информации. Цензура запрещается. В статьях 41 и 42 Конституции отмечается, что в целях обеспечения конституционных прав каждого на жизнь и на охрану здоровья запрещается сокрытие должностными лицами фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, каждый имеет право на благоприятную окружающую среду, достоверную информацию о ее состоянии на возмещение ущерба, причиненного его здоровью или имуществу

[46] Конституция РФ принята на всенародном голосовании 12.12.1993 г. // ИПС «ГАРАНТ» 2018.

[47] Федеральный закон от 26.09.1997 г. № 125-ФЗ "О свободе совести и о религиозных объединениях". // ИПС «ГАРАНТ». 2018.

экологическим правонарушением. Сокрытие этого рода влечет уголовную, административную, гражданско-правовую и другую ответственность.

К основным документам, определяющим стратегические цели, основные понятия и направления обеспечения ИБ относится Доктрина информационной безопасности Российской Федерации[48] (далее – «Доктрина ИБ РФ»). Она определяет стратегические цели и основные направления обеспечения ИБ, анализирует основные информационные угрозы, оценивает состояние ИБ. Отмечается, что некоторые зарубежные страны наращивают возможности информационно-технического воздействия на информационную инфраструктуру в военных целях. Усиливается деятельность организаций, осуществляющих техническую разведку в отношении российских госорганов, научных организаций и предприятий ОПК.

Правовую основу Доктрины ИБ РФ составляют Конституция РФ, общепризнанные принципы и нормы международного права, международные договоры РФ, федеральные конституционные законы, федеральные законы, а также нормативные правовые акты Президента и Правительства РФ.

Доктрина является документом стратегического планирования в сфере обеспечения национальной безопасности РФ, в котором развиваются положения Стратегии национальной безопасности РФ, утвержденной Указом Президента Российской Федерации от 31.12.2015 г. № 683, а также других документов стратегического планирования в указанной сфере.

Доктрина является основой для формирования государственной политики и развития общественных отношений в области обеспечения ИБ, а также для выработки мер по совершенствованию системы обеспечения ИБ.

В Доктрине ИБ РФ, даются основные понятия, оценка состояния ИБ, анализируются основные информационные угрозы. Отмечается, что расширяется деятельность организаций, осуществляющих техническую разведку в отношении российских госорганов, научных организаций и предприятий военно-промышленного комплекса. Отмечается тенденция к увеличению в иностранных медиа-СМИ объема материалов с предвзятой оценкой государственной политики России. Усиливается дискриминация российские СМИ за рубежом. Рост кибер-преступности. Широкое использование механизмов информационного воздействия различными террористическими и экстремистскими организациями.

Указываются основные направления обеспечения ИБ в области обороны, государственной и общественной безопасности, в экономической сфере, в области науки, технологий и образования, стратегической стабильности и равноправного стратегического партнерства. Состав системы обеспечения ИБ определяется Президентом РФ. Совбез России устанавливает перечень приоритетных направлений обеспечения ИБ на среднесрочную перспективу.

---

[48] Указ Президента РФ от 05.12.2016 г. № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации". // ИПС «ГАРАНТ». 2018.

В Доктрине ИБ РФ[49] используются следующие основные понятия:

под *информационной сферой*, понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет"), сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением ИБ, а также совокупность механизмов регулирования соответствующих общественных отношений.

национальные интересы РФ в информационной сфере (далее - национальные интересы в информационной сфере) - объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития в части информационной сферы;

угроза информационной безопасности РФ (далее - информационная угроза) - совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере;

информационная безопасность РФ - состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства;

обеспечение информационной безопасности - осуществление взаимоувязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;

силы обеспечения ИБ - государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством РФ задач по обеспечению ИБ;

средства обеспечения ИБ - правовые, организационные, технические и другие средства, используемые силами обеспечения ИБ;

система обеспечения информационной безопасности - совокупность сил обеспечения ИБ, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения ИБ;

информационная инфраструктура РФ (далее - информационная инфраструктура) - совокупность объектов информатизации, информационных систем, сайтов в сети "Интернет" и сетей связи, расположенных на территории

[49] Указ Президента РФ от 05.12.2016 г. № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации". // ИПС «ГАРАНТ». 2018.

РФ, а также на территориях, находящихся под юрисдикцией РФ или используемых на основании международных договоров РФ.[50]

Доктрина ИБ РФ на основе анализа основных информационных угроз и оценки состояния ИБ определяет стратегические цели и основные направления обеспечения ИБ с учетом стратегических национальных приоритетов РФ.

Федеральный закон от 27.07.2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации", регулирует отношения при осуществлении права на поиск, получение, передачу, производство и распространение информации, при применении информационных технологий, а также при обеспечении защиты информации, за исключением отношений, возникающих при охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации.

Федеральный закон приводит понятийный аппарат и механизмы регулирования в соответствие с практикой применения информационных технологий, определяет правовой статус различных категорий информации, закрепляет положения о регулировании создания и эксплуатации информационных систем, общие требования к использованию информационно-телекоммуникационных сетей, устанавливает принципы регулирования общественных отношений, связанных с использованием информации.

Закон содержит положения, направленные на защиту от недобросовестного использования или злоупотребления возможностями средств распространения информации, при которых пользователям навязывается ненужная информация. В частности, информация должна включать в себя достоверные сведения о ее обладателе или об ином лице - распространителе в форме и в объеме, которые достаточны для идентификации такого лица. При использовании для распространения информации средств, позволяющих определять получателей информации, в том числе почтовых отправлений и электронных сообщений, лицо, распространяющее информацию, обязано обеспечить получателю возможность отказа от такой информации.

Установлены правила и способы защиты прав на информацию, защиты самой информации путем принятия основных правовых, организационных и технических (программно-технических) мер по ее защите. Права обладателя информации, содержащейся в базах данных информационной системы (БД), подлежат охране независимо от авторских и иных прав на такие БД.

Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа). Устанавливается перечень информации, доступ к которой не может быть ограничен (например, о деятельности органов власти и об использовании бюджетных средств), информации, представляемой на безвозмездной основе.

---

[50] Указ Президента РФ от 05.12.2016 г. № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации", Раздел I. // ИПС «ГАРАНТ». 2018.

Закреплен прямой запрет на требование от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и на получение такой информации помимо воли гражданина (физического лица) Исключение могут составлять только случаи, прямо предусмотренные федеральными законами.[51]

Федеральный закон от 26.07.2017 г. № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации", регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак. В законе определяются основные принципы обеспечения безопасности, полномочия госорганов, а также права, обязанности и ответственность лиц, владеющих на праве собственности или ином законном основании объектами инфраструктуры, операторов связи и информационных систем, обеспечивающих взаимодействие этих объектов, определены объекты инфраструктуры: информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры, дано понятия компьютерной атаки, компьютерного инцидента и др. Определен порядок функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы[52].

Федеральный закон от 27.07.2006 г. № 152-ФЗ "О персональных данных" создает правовую основу обращения с персональными данными физических лиц в целях реализации конституционных прав человека, в том числе права на неприкосновенность частной жизни, личную и семейную тайну. Под персональными данными понимаются любые сведения о физическом лице, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и др. Закон определяет принципы и условия обработки персональных данных (ПД), устанавливает общий запрет на обработку персональных данных без согласия субъекта ПД, за исключением отдельных случаев, когда такое согласие не требуется. Регулирует отношения по обработке специальных категорий ПД, обработка которых не допускается без предварительного согласия субъекта ПД, за исключением случаев, когда ПД являются общедоступными, обработка данных необходима для обеспечения жизни и здоровья лица; обработка производится в связи с осуществлением правосудия, а также иных обстоятельств. Важнейшей гарантией прав субъекта ПД является обязанность операторов и третьих лиц, получивших доступ к ПД, обеспечивать их конфиденциальность (кроме случаев их обезличивания и

[51] Справка к Федеральному закону от 27.07.2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации". // ИПС «ГАРАНТ» 2018.
[52] Справка к Федеральному закону от 26.07.2017 г. № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации". // ИПС «ГАРАНТ» 2018.

общедоступных ПД), а также право субъекта ПД на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке. Контроль и надзор за обработкой ПД возложен на федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи, который наделяется соответствующими правами и обязанностями.[53]

Федеральный закон от 06.04.2011 г. № 63-ФЗ "Об электронной подписи", расширяет сферу использования и допустимые виды ЭП, ранее разрешалось применять только сертифицированные средства ЭП в гражданско-правовых отношениях. Выделяются 2 вида ЭП: простая и усиленная. Усиленная ЭП может быть квалифицированной либо неквалифицированной. Простая ЭП подтверждает, что данное электронное сообщение отправлено конкретным лицом. Усиленная неквалифицированная ЭП позволяет не только однозначно идентифицировать отправителя, но и подтвердить, что с момента подписания документа его никто не изменял. Сообщение с простой или неквалифицированной ЭП может быть приравнено к бумажному документу, подписанному собственноручно, если стороны заранее об этом договорились, а также в специально предусмотренных законом случаях. Усиленная квалифицированная ЭП дополнительно подтверждается сертификатом, выданным аккредитованным удостоверяющим центром. Сообщение с такой ЭП во всех случаях приравнивается к бумажному документу с собственноручной подписью. Уполномоченный в сфере ЭП орган определяет Правительство РФ. Он проводит аккредитацию удостоверяющих центров.[54]

Указ Президента РФ от 22.05.2015 г. № 260 "О некоторых вопросах информационной безопасности Российской Федерации", принято решение преобразовать сегмент международной компьютерной сети "Интернет" для федеральных и региональных органов власти, подведомственных ФСО России, в российский государственный сегмент информационно-телекоммуникационной сети "Интернет", являющийся элементом российской части данной сети.

2.3. Международные и российские стандарты информационной безопасности

Конкретные формы планирования, организации и осуществления мероприятий ИБ в организации и их содержание зависят от решаемых при этом целей, задач, условий обстановки и др. Все это нашло отражение в подходах по стандартизации процессов обеспечения ИБ. Первоначально данные подходы акцентировались на технологических вопросах (криптозащите, управлении доступом, сетевой безопасности и др.), впоследствии область их применения

[53] Справка к Федеральному закону от 27.07.2006. № 152-ФЗ "О персональных данных". // ИПС «ГАРАНТ» 2018.
[54] Справка к Федеральному закону от 06.04.2011. № 63-ФЗ "Об электронной подписи". // ИПС «ГАРАНТ» 2018.

расширилась. К технологическим стандартам, например, относятся криптографические стандарты (КОЛЕС 18033, FIPS 140, ГОСТ 28147-89, ГОСТ Р 34.10-2001, ГОСТ Р 34.11-94 и др.), стандарты на средства и методы аутентификации (ISO/IEC 9798, ГОСТ Р 52633-2006) и т.д.

В начале нулевых годов появились международные стандарты по критериям оценки компьютерных систем требованиям безопасности (ISO/IEC 15408 и др.). Следующим этапом стал переход к вопросам управления ИБ (серия ISO/IEC 27000). Здесь рассматривались следующие аспекты: разработка СМИБ компании, управление информационными рисками, управление информационными инцидентами, аудит ИБ. К данной группе относятся и «лучшие практики» обеспечения ИБ: BS 7799 - ISO/IEC, 17799 - ISO/IEC 27002, библиотеки мер контроля из серии стандартов NIST 800, германский стандарт BSI. Следующим шагом стало создание корпоративного управления ИБ (например,ISM3, Cobit 5 и т.п.).

Современная версия германского стандарта BSI 100 базируется на методике базовой защиты ИТ, позволяющей разрабатывать СМИБ по стандарту ISO/IEC 27001, включающей каталоги стандартизации подходов к анализу рисков. Прародителем серии международных стандартов управления ИБ КОЛЕС 27000 является британский стандарт BS 7799, который, в основном, предназначался для обеспечения безопасности в коммерческой деятельности. Стандарт КОЛЕС 27001 и его последующие версии содержат жесткие требования к разработке, внедрению и совершенствованию СМИБ.

Стандарт BS 7799-3:2006 «СМИБ. Руководство по управлению рисками ИБ» регламентирует оценку и управление рисками ИБ. Разработанный на его базе международный стандарт ISO/IEC 27005:2008 (Менеджмент рисков ИБ) настроен на риск-ориентированный подход к управлению ИБ в соответствии с базовыми положениями ISO/IEC 27001. Впоследствии ISO/IEC 27005 был приведен в соответствие с новыми стандартами управления рисками (ISO 31000:2009 «Менеджмент рисков. Принципы и руководства», ISO/IEC 31010:2009 «Менеджмент рисков. Методики оценки рисков», ISO Guide73:2009 «Менеджмент риска. Словарь»).

Основной целью принятия стандартов серии ISO/IEC 27000 является обеспечение совместимости с другими современными стандартами управления. В настоящее время практически оформилась сиситема стандартов СМИБ - серия 27000 «Информационная технология. Методы и средства обеспечения безопасности» (рис. 2)[55]. Данные международные стандарты не являются обязательными для государств-участников. При этом, в соответствии с регламентом ISO/IEC 21:2004 возможно как прямое, так и косвенное применение стандартов.

[55] Васильева И.Н. Управление информационной безопасностью. Учебное пособие. СПб. : Изд-во СПбГЭУ, 2014. С. 22-24.

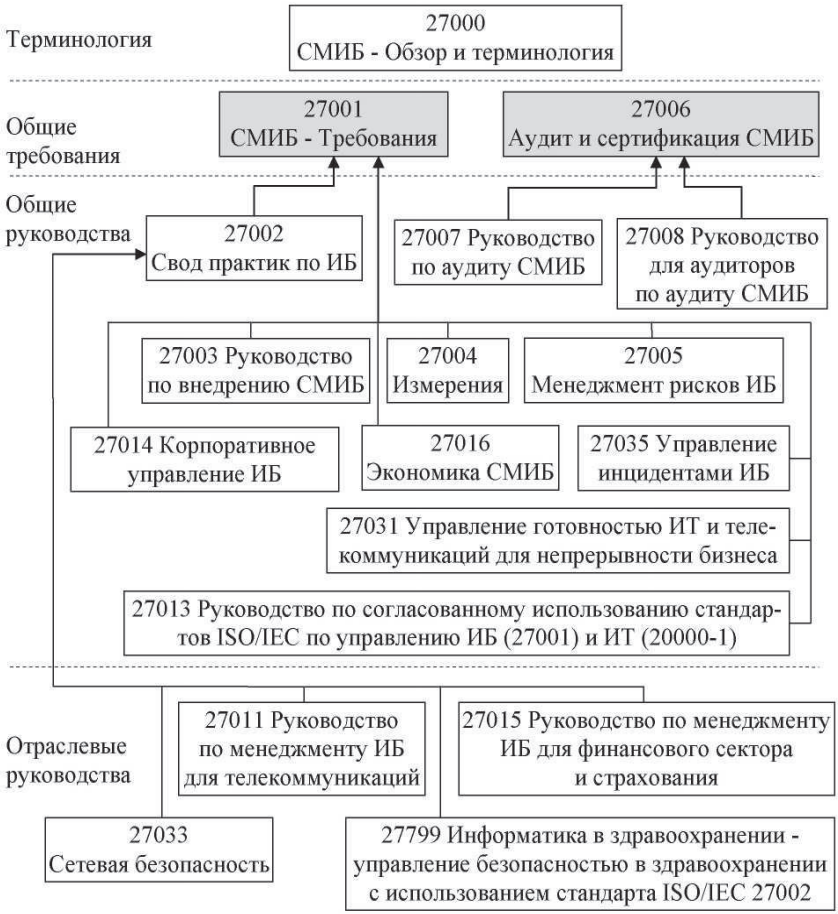

Рис. 2. Система международных стандартов СМИБ

Американские стандарты ИБ объединены в серию NIST 800, включающую более 100 документов: руководства, рекомендации, схемы менеджмента, технические спецификации, каталоги мер контроля и другие документы по разным уровням организации деятельности и аспектам ИБ, а также по разным предметным областям ЗИ и типам ИТ. [56]

Важно учитывать не только национальные стандарты, но и стандарты саморегулируемых профессиональных организаций в сфере ИБ, такие,

[56] NIST. Computer Security Resource Center. Special Publications (800 Series), [электронный ресурс]. - URL: http://csrc.nist.gov/publications/ PubsSPs.html (дата обращения: 27.08.2012).

например, как Information Security Management Maturity Model (ISM3, Модель зрелости менеджмента ИБ) консорциума ISM3 и Cobit 5 for Information Security международной ассоциации ИТ-аудиторов ISACA. Эти стандарты ориентированы на менеджмент компании и владельцев бизнес-процессов, делают упор на достижении бизнес-целей, в отличие от ISO/IEC 27001, делающегоакцент на внедрение защитных мер. Вместе с тем, эти стандарты совместимы с ISO/IEC 27001, осуществляют процессный подход, используют модифицированную модель непрерывного совершенствования PDCA.

Cobit - стандарт корпоративного управлению ИТ сферой, которая включает и процессы ИБ. Управление и контроль над информацией являются основой методологии Cobit и помогают соответствовать целям бизнеса. Среди процессов, описываемых Cobit 4.1, - обеспечение непрерывности ИТ-сервисов, обеспечение безопасности систем, управление проблемами (инцидентами), управление физической безопасностью и защитой от воздействия окружающей среды. Обеспечение целостности информации и защита ИТ активов требуют процесса управления безопасностью. Этот процесс включает определение и поддержку ролей и ответственности в сфере ИТ-безопасности, политики, стандарты и процедуры. [57]

Cobit 5 содержит серию документов, в том числе 2012 г. вышло руководство Cobit 5 for Information Security.[58] При разработке Cobit 5 учитывались стандарты КОЛЕС 27001/27002 и NIST SP800-53 revl.

С точки зрения практического использования следует отметить, что Международные стандарты ISO и британские стандарты BS распространяются фирмами-разработчиками на коммерческой основе по лицензии, также как коммерческое лицензионное программное обеспечение.

Применительно к Российской Федерации не предусмотрено прямого действия международных стандартов. В нашей стране они начинают действовать лишь после принятия их в качестве национальных стандартов (ГОСТ). Также отметим, в РФ не признаются полученные в других странах сертификаты. Кроме того, отечественные варианты международных стандартов ГОСТ Р ИСО/МЭК не признаются другими государствами. В соответствии с Федеральным Законом «О техническом регулировании» № 184-ФЗ от 27.12.2002 использование национальных стандартов (ГОСТ), в том числе и совместимых с ISO/IEC стандартов в области ИБ, является добровольным.

Таким образом, процессы управления информационной безопасностью и инцидентами ИБ регулируются международными общими, специализированными и отраслевыми стандартами (ISO/IEC 27035:2011, ISO/IEC 20000-1:2011, ISO/IEC27001:2013, ISO/IEC 27002:2013 и др.). Российские ГОСТы и стандарты, зачастую, являются переводом зарубежных

[57]CobiT 4.1. Российское издание. - М.: Аудит и контроль информационных систем, 2008.
[58] Cobit 5 for Information Security Introduction, [электронный ресурс]. - URL: http://www.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf (дата обращения: 29.08.2012).

стандартов. В значительной степени международные стандарты в сфере информационной безопасности разрабатывались и охватывают финансовую и банковскую сферы. Контроль и оценка состояния безопасности информационной инфраструктуры организации осуществляется путем проверки их соответствия международным (ISO, Common criteris for IT security) стандартам и российским государственным (ГОСТ).

Российские национальные стандарты

1. Национальный стандарт РФ ГОСТ Р ИСО/МЭК 27002-2012 "Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности" (утв. приказом Федерального агентства по техническому регулированию и метрологии от 24.09.2012 г. №423-ст);
2. Национальный стандарт РФ ГОСТ Р ИСО/МЭК 13335-1-2006 "Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий" (утв. приказом Федерального агентства по техническому регулированию и метрологии от 19.12.2006 г. № 317-ст);
3. Национальный стандарт РФ ГОСТ Р 53114-2008 "Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения" (утв. Приказом Федерального агентства по техническому регулированию и метрологии от 18.12. 2008 г. № 532-ст);
4. Национальный стандарт РФ ГОСТ Р 53131-2008 (ИСО/МЭК ТО 24762:2008) "Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения" (утв. Приказом Федерального агентства по техническому регулированию и метрологии от 18.12.2008 г. № 533-ст);
5. Национальный стандарт РФ ГОСТ Р 54582-2011/ISO/IEC/TR 15443-2:2005 "Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 2. Методы доверия" (утв. Приказом Федерального агентства по техническому регулированию и метрологии от 01.12.2011 г. № 690-ст);
6. Национальный стандарт РФ ГОСТ Р ИСО/МЭК 27005-2010 "Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности" (утв. Приказом Федерального агентства по техническому регулированию и метрологии от 30.11.2010 г. № 632-ст);
7. Национальный стандарт РФ ГОСТ Р ИСО/МЭК ТО 19791-2008 "Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем" (утв. Приказом Федерального агентства по техническому регулированию и метрологии от 18.12.2008 г. № 525-ст);

8. Национальный стандарт РФ ГОСТ Р ИСО/МЭК ТО 13335-5-2006 "Информационная технология. Методы и средства обеспечения безопасности. Часть 5 "Руководство по менеджменту безопасности сети" (утв. приказом Федерального агентства по техническому регулированию и метрологии от 19.12. 2006 г. № 317-ст);

9. Национальный стандарт РФ ГОСТ Р 54080-2010 "Воздушный транспорт. Система технического обслуживания и ремонта авиационной техники. Информационно-аналитическая система мониторинга лентой годности воздушных судов. Общие требования". (утв. Приказом Федерального агентства по техническому регулированию и метрологии от 30.11.2010 г. № 734-ст);

10. Национальный стандарт РФ ГОСТ Р 55860-2013 "Воздушный транспорт. Система менеджмента безопасности авиационной деятельности. Общие принципы построения СМБ на всех этапах жизненного цикла авиационной техники. Структурная схема и функции модулей типовой СМБ. Общие положения" (утв. Приказом Федерального агентства по техническому регулированию и метрологии от 22.11.2013 г. № 1932-ст);

11. Стандарт Банка России СТО БР ИББС-1.0-2014 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения" (принят и введен в действие распоряжением Банка России от 17.05.2014 г. № Р-399)

12. Рекомендации в области стандартизации Банка России РС БР ИББС-2.5-2014 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности" (приняты и введены в действие распоряжением Банка России от 17.05.2014 г. № Р-400).

13. Стандарт Банка России СТО БР ИББС-1.3-2016 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств" (принят и введен в действие приказом ЦБР от 30.11.2016 г. № ОД-4234).

14. Стандарт Банка России СТО БР ИББС-1.4-2018 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Управление риском нарушения информационной безопасности при аутсорсинге" (принят и введен в действие приказом Банка России от 06.03.2018 г. № ОД-568)

Глава 3. Практика бизнес-процессов обеспечения информационной безопасности на авиапредприятиях

3.1. Планирование и организация процессов обеспечения информационной безопасности

Государства-члены ИКАО обязаны приводить национальные программы безопасности ГА в соответствие со стандартами ИКАО, контролирует этот процесс, взаимодействуя с местными авиационными властями.

В качестве основы ИБ авиапредприятия должны быть сформулированы цели, стратегии и политика ИБ. Комплекс перечисленных аспектов содействует эффективности и непрерывности процессов деятельности авиапредприятия и обеспечивает взаимоувязанность всех мер по ИБ. В целях обеспечения такого рода согласованности, особенно важно, корреляцию стратегии и политики безопасности авиапредприятия, а также интеграцию в программы обучения и повышения квалификации в области безопасности. Цели (чего необходимо достичь), стратегии (способы достижения цели), политика (правила, которые следует соблюдать при реализации стратегий) и процедуры (методы, способы, конкретные приемы осуществления политики) конкретизируются в конкретных бизнес-процессах, осуществляемых подразделениями авиапредприятия на соответствующих уровнях.

В целом, практическая деятельность по планированию и организации бизнес-процессов обеспечения ИБ управления авиапредприятий должна соответствовать определенным принципам, к числе наиболее важных из которых можно отнести следующие.

1. Принцип законности. Развитие и совершенствования системы ИБ авивпредприятия должно осуществляться в строгом соответствии с нормативными правовыми актами РФ, в том числе с учетом международных договоров (соглашений), требований организационно-распорядительных и нормативно-методических документов соответствующих уполномоченных органов, органов власти в пределах их компетенции, требований соответствующих отраслевых и внутриорганизационных документов.

2. Принцип первого лица. СМИБ будет эффективно реализована, только если будет создаваться, внедряться и управляться “сверху – вниз”. Руководство определяет политику ИБ, требуемую организационную структуру, устанавливает должностную иерархию, соответствующие функционалы, контролирует выполнение мероприятий по обеспечению ИБ.

3. Принцип разграничения полномочий. Органы управления предприятия, структурные подразделения создают условия для обеспечения требуемого уровня ИБ на подведомственных им объектах защиты.

4. Принцип своевременности реакции. Превентивная разработка мер по ИБ, их непосредственная реализация, обеспечивает адекватную реакцию на

возникающие и прогнозируемые угрозы, оперативную быструю ликвидацию их последствий.

5. Принцип непрерывности. Характер информационных угроз и особенности защищаемых информационных объектов требуют постоянного их мониторинга во всех условиях обстановки.

6. Принцип подконтрольности и подотчетности. Органы управления всех уровней, все должностные лица в установленном порядке отчитываются и несут ответственность перед вышестоящими органами управления за состояние ИБ в подведомственных им подразделениях (на объектах защиты), а вышестоящие органы управления осуществляют контроль состояния системы ИБ в подчиненных им подразделениях.

7. Принцип соответствия предполагает, что уровень развития системы ИБ должен соответствовать задачам обеспечения безопасности организации в целом, ее эффективного функционирования с учётом реальных возможностей. Средства и способы обеспечения ИБ применяются в соответствии с реальными угрозами и экономическим возможностям организации.

8. Принцип прозрачности и гласности состоит в том, что важно участие в процессах разработки, внедрения и функционирования СМИБ всех сотрудников авиапредприятия, в части касающейся каждого в плане работы с информационными ресурсами фирмы.

9. Принцип эволюционности: СМИБ рационально создавать и внедрять постепенно, по мере практической необходимости и целесообразности планирования, организации и практической реализации тех или иных процессов обеспечения ИБ.

10. Принцип необходимости непрерывного риск-менеджмента ИБ. Именно постоянная эффективная оценка информационных рисков составляет теоретическую и практическую основу всей СМИБ.

Также можно отметить принципы разделения функций, гибкости управления, открытости алгоритмов и механизмов защиты, простота применения защитных мер и средств, а также другие.

В соответствии с рассмотренным ранее походом стандарта ISO/IEC 27001, СМИБ является составной частью системы менеджмента предприятия в целом, акцентирующейся на оценке рисков в области ИБ. Проектирование, разработка, создание, эксплуатация СМИБ требует универсального подхода как к любой системе менеджмента. В связи с этим процедуры стандарта управления качеством ISO 9001 обязательны и для стандарта ISO 27001. Как известно, Документное обеспечение ISO/IEC 27001 соответствует положениям ISO 9001, поэтому использование СМИБ по ISO/IEC 27001 на основе ранее практически реализованной системы менеджмента качества ISO 9001 может способствовать существенному снижению уровня затрат авиапредприятия.

В целом, применение ISO/IEC 27001 для разработки и использования СМИБ в рамках процессной модели PDCA подразумевает непрерывную

циклическую систему мероприятий по планированию, организации, практической реализации, контролю, совершенствованию процессов обеспечения ИБ.

При планировании СМИБ, включающем традиционные в менеджменте вопросы, в стандарте ISO/IEC 27001 уделяется особое внимание следующим аспектам: разграничение зоны ответственности создаваемой СМИБ предприятия, разработка политики СМИБ в соответствии со спецификой бизнес-процессов организации, определение методических и технологических подходов к процессам риск-менеджмента на предприятии (непрерывный мониторинг, диагностирование и контроль информационных рисков, разработка показателей и критериев, количественная и качественная оценка рисков, управление информационными рисками и др.), получение разрешения руководства предприятия на разработку, внедрение и эксплуатацию СМИБ, разработка и практическое применение требований по перечню мер контроля из каталога стандарта. Следует также отметить специфику планирования по ISO/IEC 27001. В отличии от требований к аттестации автоматизированных систем, данный стандарт предназначен для сертификации процесса, а не предприятия или системы ИБ.

Неоправданное расширение перечня объектов обеспечения ИБ, стремление охватить все бизнес-процессы на авиапредприятии (существенно акцентироваться, прежде всего, на критически важных бизнес-процессах) будут существенно увеличивать стоимость мероприятий по ИБ, что может существенно уменьшить шансы на эффективное решение вопросов разработки, внедрения и сертификации СМИБ. Также важно адекватно отобразить взаимосвязь СМИБ с остальными СУ и процессами в организации.

Разработка политики ИБ авиапредприятия должна осуществляться с учетом специфики организации, реализуемых в ней бизнес-процессов внешнего и внутреннего нормативного правового поля фирмы, методологии и практики риск-менеджмента фирмы. Крайне существенные требования накладывает содержание карты рисков организации. При этом планируются вопросы управления не только рисками, но и активами, мерами контроля, документооборотом, изменениями, мероприятиями в случае происшествий в области ИБ, персоналом и т.п.

При необходимости в дальнейшем прохождения предприятием аудита СМИБ и сертификации, итогом планирования должна быть также разработка и представление руководству (при необходимости – внешним аудиторам) соответствующего «Положения о применимости», в котором фиксируются требования из каталога мер контроля, реализованные в СМИБ организации, а также нереализованные с обоснованием причин невыполнения. Данные материалы должны непрерывно актуализироваться.

Можно выделить следующие основные виды аудита ИБ: экспертный аудит безопасности (в процессе его выявляются недостатки в системе мер защиты информации на основе имеющегося опыта экспертов, участвующих в процедуре

обследования); оценка соответствия рекомендациям отечественных и международных стандартов, а также требованиям руководящих документов; инструментальный анализ защищенности информационной системы предприятия, направленный на выявление и устранение уязвимостей программно-аппаратного обеспечения системы; системный или комплексный аудит, включающий в себя все вышеперечисленные формы проведения обследования. В зависимости от решаемых предприятием задач, каждый из вышеперечисленных видов аудита может проводиться по отдельности или в комплексе. В качестве объекта аудита может выступать как информационная система компании в целом, так и ее отдельные сегменты, в которых проводится обработка информации, подлежащей защите[59].

После планирования идет процесс организации мероприятий ИБ, который в излагаемом контексте, предполагает внедрение ISO 27001/27002(17799) на предприятии. Соответствующий ISO/IEC 27001 вариант оргструктуры системы управления ИБ предприятия представлен на рис.3.[60]

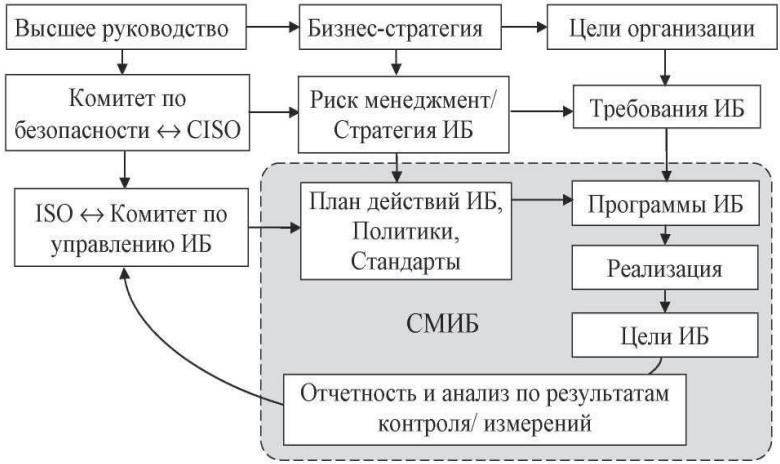

Рис. 3. Организационная структура системы управления ИБ

Топ-менеджер по ИБ, возглавляющий коллегиальный орган управления по решению стратегических вопросов ИБ - комитет по информационной безопасности, обычно подчиняется Генеральному директору или непосредственно Совету директоров компании. Линейный руководитель (например, начальник службы ИБ) отвечает за все вопросы управления,

[59] Родионов М.А. Методологические аспекты информационного аудита в менеджменте предприятия. // Научный вестник МГТУ ГА, № 156. М. 2010. С. 68-75.
[60] Васильева И.Н. Управление информационной безопасностью. Учебное пособие. СПб. : Изд-во СПбГЭУ, 2014. С. 54.

связанные с обеспечением ИБ организации. Важно разграничивать уровень операционной деятельности по обеспечению ИБ и уровень управления ИБ предприятия в целом. В ведущих зарубежных компаниях работу координирует топ-менеджер CISO (административный и методологический центр управления ИБ). За операционные риски отвечают руководители подразделений (линейные менеджеры), они же делегируют функции управления ИБ подразделениям ИТ и другим, входящим в состав системы ИБ, подразделениям. Это позволяет создавать более эффективную систему ИБ, с четкими и понятными полномочиями и обязанностями [8]. [61]

Внедрение СМИБ целесообразно осуществлять на предприятии в виде проекта, что достаточно подробно изложено в стандарте ISO/IEC 27003:2010 «Руководство по внедрению СМИБ».

Практическая реализация СМИБ неразрывна от процессов соответствующего контроля, включающего непрерывный мониторинг и проверку реализации мероприятий по ИБ с точки зрения эффективности СМИБ, с учетом результатов внутренних и внешних аудитов ИБ, переоценку остаточных информационных рисков при изменении условия обстановки и другие мероприятия. Для определения и мониторинга показателей эффективности СМИБ разрабатывается Программа измерения информационной безопасности, приведенная в стандарте ISO/IEC 27004:2009 «Менеджмент ИБ. Измерения».

В целом, система обеспечения ИБ авиапредприятий является составной частью системы обеспечения информационной безопасности авиатранспортной отрасли и РФ в целом. Она планируется, организуется и ведется с учётом всех критически важных для защищаемых объектов угроз, комплексности правовых, организационных, технических и специальных методов обеспечения ИБ, преемственности и непрерывности мероприятий по обеспечению ИБ.

3.2. Особенности обеспечения информационно-технической безопасности авиапредприятий

Практика обеспечения информационно-технической безопасности (ИТБ) авиапредприятия основывается на действующих международных и российских стандартах. Для эффективного обеспечения бизнес-процессов управления ИБ авиапредприятия, в организациях авиаотрасли должны быть сформулированы цели, стратегии и политика ИТБ для обеспечения согласованности всех аспектов безопасности авиапредприятия. Эффективность ГА, безопасность полетов (БП) и авиационная безопасность (АБ) в определяющей степени зависят от наличия систем информационных и связных технологий (ICT), а также от точности и конфиденциальности данных.

[61] Лукацкий А. В. Кто такие CISO и есть ли они в России? // Inside. Защита информации. - 2007. - № 3. - С. 18-20.

Защита авиационных систем от киберугроз, понижение степени их уязвимости и обеспечение способности систем к восстановлению функций могут быть достигнуты исключительно за счет применения подхода, основанного на сотрудничестве и включающего коллективную экспертную работу в области авиационной безопасности, аэронавигации, безопасности систем ICT и участие специалистов из других соответствующих областей.[62]

В Рабочем документе ИКАО "Решение проблем кибербезопасности в гражданской авиации" отмечается, что кибербезопасность в ГА является приоритетной задачей, отрасль все больше зависит от наличия систем информационных и связных технологий, а также от целостности и конфиденциальности данных, возрастает актуальность защиты критически важных систем инфраструктуры ГА от киберугроз. Обозначена необходимость совместной работы над разработкой эффективной и координированной глобальной программы для заинтересованных сторон в области ГА по решению проблем кибербезопасности наряду с краткосрочными мероприятиями по повышению устойчивости глобальной системы авиации к киберугрозам, которые могут представлять угрозу БП ГА.

Для эффективного выстраивания бизнес-процессов обеспечения ИБ авиапредприятия необходимо принять следующие меры по противодействию киберугрозам в сфере ГА: определить угрозы и факторы риска, представляемые возможными киберинцидентами в отношении полетов и критически важных систем; определить круг обязанностей органов и заинтересованных сторон отрасли по отношению к кибербезопасности в ГА; поощрять выработку общего понимания государствами-членами киберугроз и факторов риска и общих критериев для определения важности объектов и систем, требующих защиты; поощрять координацию действий между государственными органами и отраслью по отношению к выработке стратегии, политики и планов обеспечения кибербезопасности; обмен информацией, необходимой для выявления критических уязвимых мер, которые требуется устранить; создавать государственно-отраслевые партнерства и механизмы на национальном и международном уровнях и участвовать в их деятельности по обмену информацией в области киберугроз, инцидентов, тенденций и мер противодействия; основываясь на едином понимании киберугроз и факторов риска, использовать гибкий подход к защите критически важных авиационных систем путем внедрения систем управления кибербезопасностью; поощрять развитие в национальных органах и в авиационной отрасли устойчивой культуры кибербезопасности на всех уровнях; определить юридические последствия действий, ставящих под угрозу БП воздушных судов путем использования киберуязвимых мест; способствовать разработке и внедрению международных стандартов, стратегии и передовой практики в сфере защиты применяемых для целей ГА критически важных систем информации и связи от

[62] Официальный сайт ИКАО. Решение проблем кибербезопасности в гражданской авиации. 30.05.2016. URL: https://www.icao.int/Meetings/a39/Documents/WP/wp_017_ru.pdf

актов вмешательства, которые могут угрожать БП ГА; разработать политику и по необходимости выделять ресурсы для обеспечения соответствующих требований для критически важных авиационных систем (должна быть обеспечена безопасность архитектуры систем на уровне конструкции; системы должны располагать запасом прочности; способы передачи данных должны быть безопасными, обеспечивающими целостность и конфиденциальность данных; должны быть внедрены методы мониторинга систем и выявления инцидентов и представления сообщений о них; необходимо осуществлять ретроспективный анализ киберинцидентов; сотрудничать в разработке программы ИКАО в сфере кибербезопасности согласно комплексному подходу, включающему области аэронавигации, связи, наблюдения, эксплуатации воздушных судов, летной годности и др).[63]

Важными мерами по обеспечению ИТБ организации являются: политики и процедуры; механизмы контроля доступа; антивирусное программное обеспечение; шифрование; цифровая подпись; инструменты мониторинга и анализа; резервный источник питания; резервные копии информации.[64]

Необходимо сформировать и поддерживать базу инцидентов ИБ в актуальном состоянии, структуру записей рекомендуется осуществлять на основе классификатора инцидентов по следующим признакам: степени тяжести последствий для бизнес-процессов обеспечения управления ИБ авиапредприятия (в денежном выражении, в балльной шкале); степени вероятности повторного возникновения инцидента ИБ; видам источников угроз ИБ, вызывающих инциденты ИБ; по преднамеренности возникновения инцидента ИБ - случайный, намеренный, ошибочный; по видам объектов информационной инфраструктуры, задействованных при реализации инцидента ИБ; по уровню информационной инфраструктуры, на котором происходит инцидент ИБ; по нарушенным свойствам ИБ - конфиденциальность, целостность, доступность; по типу инцидента ИБ - свершившийся инцидент ИБ, попытка осуществления инцидента ИБ, подозрение на инцидент ИБ; по области распространения и действия инцидента ИБ; по сложности обнаружения инцидента ИБ; по сложности закрытия инцидента ИБ и др. При этом целесообразно установить состав атрибутов инцидентов ИБ, возможных для заполнения на каждом из этапов реагирования на инцидент ИБ.

К конкретным методам обеспечения ИТБ организации относятся вопросы, связанные со способами несанкционированного доступа (НСД) к ресурсам и объектам ИБ. Так НСД к программам включает: проникновение в программу,. деструктивные функции закладок и работа прикладных программ, способы реализации функций закладок, НСД в базы данных и др. Другим важным

---

[63] Официальный сайт ИКАО. Решение проблем кибербезопасности в гражданской авиации. 30.05.2016. URL: https://www.icao.int/Meetings/a39/Documents/WP/wp_017_ru.pdf

[64] Национальный стандарт РФ ГОСТ Р ИСО/МЭК 13335-1-2006 "Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий" (утв. приказом Федерального агентства по техническому регулированию и метрологии от 19 декабря 2006 г. N 317-ст). // ИПС «ГАРАНТ». 2018.

аспектам ИТБ является вопрос о защитных механизмах, используемых в информационных системах (ИС), к которым относятся идентификация и аутентификация, разграничение доступа к ресурсам ИС Критически важен в ИТБ вопрос защиты информации от утечки по техническим каналам, включающий понимание модели технического канала утечки информации, порядка определения границы контролируемой зоны, а также источников возникновения опасных сигналов. Следующий необходимый для обеспечения ИТБ аспект: управление целостностью данных, их восстановлением и хранением. Это включает: разработку стратегии хранения данных, резервирование, архивирование и управление восстановлением данных (обеспечение целостности данных, резервирование и архивирование - raid и hsm, технология теневого копирования данных, архивация данных, создание отказоустойчивых томов для хранения данных). Важным разделом теории и практики обеспечения ИТБ является криптографическая защита. Здесь применяются симметричные и асимметричные криптосистемы. Широко используются архивация, алгоритмы Хаффмана и Лемпеля-Зива, хеширование паролей, транспортное кодирование и т.д. Практически важное значение имеют Windows-хуки (обработка ОС сообщений от клавиатуры, обработка ОС сообщений от "мыши", программирование Windows-хуков). Перечисленные аспекты ИТБ нашли свое отражение в соответствующей литературе, в том числе в учебной литературе МГТУ ГА[65].

На основе Рекомендаций в области стандартизации Банка России РС БР ИББС-2.5-2014 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности"[66], применяя метод аналогии, рассмотрим возможный перечень типов и событий ИБ.

Физический уровень информационной инфраструктуры включает: физический доступ работников организации БС РФ и иных лиц в здания и помещения организации; физический доступ работников предприятия и иных лиц к средствам вычислительной техники (ВТ) и использование указанными субъектами средств ВТ; использование работниками фирмы и иными лицами устройств копирования и многофункциональных устройств; использование работниками организации и иными лица аппаратов факсимильной связи; изменение параметров настроек средств ВТ, телекоммуникационного оборудования; изменение параметров настроек оборудования, обеспечивающего функционирование средств ВТ; сбои и отказы в работе средств ВТ, телекоммуникационного оборудования; сбои и отказы в работе оборудования, обеспечивающего функционирование средств ВТ; сбои и отказы

[65] В.И. Петров, К. Г.Апарина. Основы информационной безопасности. Учебное пособие. М., МГТУ ГА, 2014.

[66] Рекомендаций в области стандартизации Банка России РС БР ИББС-2.5-2014 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности" (приняты и введены в действие распоряжением Банка России от 17.05.2014 г. № Р-400). // ИПС «ГАРАНТ».2018.

в работе средств защиты информации; сбои и отказы в работе сети телефонной связи; отказы в работе сетей передачи данных; физическое воздействие на средства ВТ, телекоммуникационное оборудование, средства защиты информации и сети передачи данных; изменения климатических режимов помещений, в которых расположены средства ВТ, телекоммуникационное оборудование; изменения параметров функционирования сетей передачи данных; замена и (или) модификация программных и (или) аппаратных частей средств ВТ, телекоммуникационного оборудования; осуществление действий с носителями информации, в том числе вынос за пределы территории объектов авиапредприятия носителей информации; вынос за пределы фирмы переносных средств ВТ; использование переносных средств ВТ на территории объектов организации; передача средств ВТ между подразделениями предприятия; передача средств ВТ во внешние организации; проведение работниками организации и иными лицами фото- и (или) видеосъемки в зданиях или помещениях авиапредприятия; проведение мероприятий по доступу к телевизионным системам охранного наблюдения, охранной сигнализации, системам контроля и управления доступом; события, формируемые телевизионными системами охранного наблюдения, охранной сигнализации, системами контроля и управления доступом; осуществление действий с носителями информации и системами, позволяющими осуществить физический доступ в здания и помещения организации.

Уровень сетевого оборудования: изменение параметров настроек сетевого оборудования и программного обеспечения (ПО) сетевого оборудования; изменение состава и версий ПО сетевого оборудования; обнаружение аномальной сетевой активности; аутентификация и завершение сеанса работы на сетевом оборудовании; обнаружение вредоносного кода и его проявлений; изменение топологии вычислительных сетей; подключение оборудования к вычислительным сетям; сбои в работе ПО сетевого оборудования; обновление ПО сетевого оборудования; выполнение операций по техническому обслуживанию сетевого оборудования; использование средств анализа уязвимостей сетевого оборудования; отключение/перезагрузка сетевого оборудования; обнаружение атак типа "отказ в обслуживании"; смена и (или) компрометация аутентификационных данных, используемых для доступа к сетевому оборудованию; сбои в работе средств защиты информации; изменение параметров работы средств защиты информации; запуск средств анализа топологии вычислительной сети.

Уровень сетевых приложений и сервисов: идентификация, аутентификация, авторизация и завершение сеанса работников организации и иных лиц; изменение параметров настроек, состава и версий ПО; обнаружение вредоносного кода и его проявлений; установление соединений и обработка запросов, в том числе удаленных, на уровне сетевых приложений и сервисов; сбои и отказы в работе сетевых приложений и сервисов; выполнение операций, связанных с эксплуатацией и администрированием сетевых приложений и

сервисов; обнаружение нетипичных (аномальных) запросов на уровне сетевых приложений и сервисов; отключение/перезагрузка или приостановление работы сетевых приложений и сервисов; выполнение операций по предоставлению доступа к использованию сетевых приложений и сервисов, в том числе использованию электронной почты и сети Интернет; выполнение операции по архивированию данных сетевых приложений и сервисов, в том числе данных электронной почты; осуществление операций по обмену сообщениями, в том числе обмену платежными сообщениями; сбои в осуществлении обменом сообщениями, в том числе в обмене платежными сообщениями; искажение, модификация сообщений, в том числе платежных сообщений; аутентификация сообщений, в том числе платежных сообщений; аутентификация АРМ - участников обмена сообщениями, в том числе платежными сообщениями; завершение/приостановка выполнения сетевых приложений и сервисов по ошибке; распространение и (или) сбор информации с использованием сетевых приложений и сервисов; выполнение операций со списками рассылки и адресными книгами; наделение работников организации БС РФ и (или) иных лиц правами пользователя конкретного пакета сервисов, в том числе сервисов и ресурсов сети Интернет; использование средств анализа уязвимостей сетевых приложений и сервисов; смена и (или) компрометация аутентификационных данных, используемых для осуществления доступа к сетевым приложениям и сервисам; сбои в работе средств защиты информации; переадресация сообщений, в том числе платежных сообщений; распространение информации, побуждающей клиента сообщать информацию, необходимую для осуществления действий от его имени; внешние воздействия из сети Интернет, в том числе сетевые атаки; выполнение операций со средствами криптографической защиты информации и ключевой информацией.

Уровень операционных систем (ОС): - аутентификация и завершение работы работников организации и иных лиц, в том числе на уровне системного ПО, систем управления БД и прикладного ПО; изменение параметров конфигурации, состава и версий ПО уровня ОС; запуск, остановка и (или) отключение/перезагрузка ПО уровня ОС; обнаружение вредоносного кода и его проявлений; установление соединений и обработка запросов с использованием ПО уровня ОС; сбои в работе ПО уровня ОС; выполнение операций, связанных с эксплуатацией и администрированием ПО уровня ОС; обнаружение нетипичных запросов с использованием ПО уровня ОС; сбои и отказы в работе средств защиты информации; изменение параметров конфигурации средств защиты информации; выполнение операций по предоставлению доступа к ПО уровня ОС и информационным ресурсам, обрабатываемым с использованием ПО уровня ОС; выполнение операций по архивированию, резервированию и восстановлению информации; завершение/приостановка работы ПО уровня ОС по ошибке; использование средств анализа уязвимостей ПО уровня ОС; смена и (или) компрометация аутентификационных данных, используемых для доступа к ПО уровня ОС и информационным ресурсам, обрабатываемым с

использованием ПО уровня ОС; изменение параметров конфигурации средств защиты информации; внешнее воздействие из сети Интернет на ПО уровня ОС; создание, авторизация, уничтожение или изменение платежной информации; создание, уничтожение или изменение информационных ресурсов, баз данных и (или) иных массивов информации; компрометация аутентификационных данных и ключевой информации; выполнение операций со средствами криптографической защиты информации и ключевой информацией.

Уровень технологических процессов и приложений и уровень бизнес-процессов организации: выполнение отдельных операций или процедур в рамках платежных и информационных технологических процессов; контроль выполнения операций или процедур в рамках платежных и информационных технологических процессов; осуществление операций или процедур в рамках платежных и информационных технологических процессов с использованием средств криптографической защиты информации; выделение и назначение ролей, в том числе ролей, связанных с обеспечением ИБ.

Для эффективной разработки и эксплуатации системы ИТБ авиапредприятия необходимо также обеспечить выполнение следующих требований: простота защиты информационных ресурсов; приемлемость мероприятий для пользователей; подконтрольность системы ИБ; постоянный контроль за наиболее важной информацией; дробление конфиденциальной информации на составляющие элементы, доступ к которым имеют разные пользователи; минимизация привилегий по доступу к информации; установка ловушек для провоцирования НСД; устойчивость защиты во времени и при неблагоприятных условиях обстановки; требуемый уровень обеспечения ИБ, дублирование и перекрытие при проведении конкретных информационно-технических мероприятий по защите информации.

3.3. Информационно-психологическая безопасность на авиапредприятиях

Самым ценным ресурсом любого авиапредприятия являются люди. Именно от квалификации персонала, степени его использования зависит конкурентоспособность организации. Персонал предприятия представляет собой совокупность работников определенных категорий и профессий, занятых единой производственной деятельностью, направленной на получение прибыли или дохода и удовлетворение своих материальных потребностей. Эффективная реализация человеческого ресурса во много определяется психологическим состоянием как всего коллектива, так и каждого конкретного работника. Управление этими процессами предполагает использование методов обеспечения информационно-психологической безопасности организации.

Информационные воздействия - необходимая предпосылка и условие формирования и существования общественного и индивидуального сознания. Они могут изменять, реструктурировать психологические свойства, состояния и

модели поведения и деятельности общества и отдельной личности в нужном направлении. Информационно-психологические воздействия могут оказывать влияние на все компоненты сознания - психические процессы (восприятие, память, воображение, мышление, внимание), психологические состояния и психические свойства личности. Специально организованные воздействия на психику человека могут носить как конструктивный, так и деструктивный характер. Негативные информационно-психологические воздействия на человека могут привести к двум видам взаимодействующих изменений[67]:

изменения психики, психологического здоровья человека (нарушающие адекватное отражение мира и своего места в нем, отношения человека к миру);

сдвигам в ценностях, жизненных позициях, ориентирах, мировоззрении личности, т.е. в том, что определяет личность как гражданина.

Человек как личность-индивид обладает сознанием, подверженным различного рода манипулятивным воздействиям, информационным по своей природе, результаты которых могут как способствовать положительным изменениям в жизнедеятельности человека, так и угрожать его физическому или психологическому здоровью, выполнению им своих служебных обязанностей. С другой стороны, постоянно имеют место информационные воздействия на организованные или неорганизованные группы и массы людей. Наряду с возможным положительным влияний таких воздействий нередко они носят и деструктивный характер (например, инициация паники на воздушном судне, мобилизация митингующих к активным действиям и т.п.).

Наиболее распространенным в общении должностных лиц методом информационно-психологического воздействия является манипуляция - это скрытое управление человеком, вид психологического воздействия, искусное исполнение которым ведет к скрытому возбуждению у другого человека намерений, не совпадающих с его актуально существующими желаниями.

Отличительные черты манипуляции: осознанность манипулятором своих целей и средств; скрытость целей и средств манипулятора; принятие адресатом на себя ответственности за происходящее. Основной признак - наличие «жертвы» манипуляции. Субъективное ощущение жертвы манипуляции - некомфортное состояние, ощущение одиночества, покинутости, суженного сознания и т.п.

Типовые приемы манипуляции: уход от темы разговора, ссылка на других, искажение смысла, лесть, намеки, ирония, шутка-высмеивание, запугивание, предсказывание негативных последствий, имитация решения проблемы, оттягивание решения под всевозможными предлогами и др.

Некоторые типовые приемы противодействия манипуляции: раскрыть цель манипулятора и открыто заявить ему об этом; встречная манипуляция - раскрыть манипуляцию, но не заявлять об этом, а пытаться добиться своих собственных скрытых целей; противостояние манипуляции - если адресат

[67] Родионов М.А. Информационная безопасность (социальные аспекты). М., ВАГШ, 2004.

понял, что им манипулируют и начинает выяснять или нейтрализовывать действия оппонента; капитуляция - если адресат решает отдаться на волю манипулятора (например, ему приятны действия манипулятора или он согласен с целью); психологическая игра - бессознательно совершаемая манипуляция, чаще всего взаимная.

Рассматривая авиатранспортную область, приведем в качестве примера сводки авиационных происшествий, которые свидетельствуют о большом разнообразии факторов, отрицательно влияющих на эффективность деятельности человека в процессе выполнения полетов. Содержание некоторых заключений из отчетов о причинах авиационных происшествий:

"обязанности не были распределены должным образом, и весь экипаж был занят наблюдением за индикатором положения шасси ";

"командир воздушного судна как руководитель неправильно использовал все ресурсы, имеющиеся в его распоряжении ";

"зрительная иллюзия, связанная с явлением " черной дыры " ... ";

"сбой в нормальных процедурах связи и неправильное понимание речевых сообщений ...";

"ошибки при передаче информации и вводе данных ...".[68]

Эти примеры свидетельствуют о том, что рационализация действий людей в сложной высокотехнологической рабочей среде охватывает все аспекты человеческой деятельности, а именно: принятие решений и другие познавательные процессы, конструирование дисплеев и органов управления, компоновку кабин, связи и программное обеспечение, карты схемы, и документацию, такую как руководства по летной эксплуатации, стандартные эксплуатационные процедуры и контрольные перечни операций. Учет человеческого фактора играет важную роль при отборе персонала, его подготовке и во время проверок, а также для предотвращения и при расследовании авиационных происшествий. [69]

Учет информационно-психологических факторов охватывает много дисциплин. На индивидуальном уровне информация, взятая из психологии, используется для того, чтобы понять, как люди обрабатывают информацию и принимают решения. Психология и физиология дают понимание сенсорных процессов как средства восприятия и передачи информации об окружающем нас мире. Антропометрия и биомеханика призваны помочь в понимании измерений и движений человеческого тела, это важно для оптимизации конструкции и компоновки органов управления и других характеристик рабочих мест в кабине экипажа и салоне воздушного судна. Биология и ее область хронобиология необходимы для правильного понимания природы биоритмов и их влияния на человека во время посменной работы, ночных

[68] Основные принципы учета человеческого фактора в руководстве по проведению проверок безопасности полетов. ИКАО Doc9806 AN 763. 2002. С.2-2.

[69] Основные принципы учета человеческого фактора в руководстве по проведению проверок безопасности полетов. ИКАО Doc9806 AN 763. 2002. С.2-3.

полетов и пересечения временных поясов. Знания о человеческом факторе постоянно углубляются благодаря научным исследованиям.[70]

В модели человеческого фактора SHEL 1 используются блоки для представления различных его компонентов. Название модели на английском языке образуется из начальных букв ее четырех компонентов: субъект – LIVEWARE (человек), объект – HARDWARE (машина), процедуры – SOFTWARE (правила, руководства, символы и т. д.) и окружающая среда – NVIRONMENT (ситуация, в которой должны функционировать остальные составляющие системы L-H-S). Это представляет собой дальнейшее развитие традиционной системы " человек – машина – среда". SHEL заостряет внимание на человеке и на его интерфейсах с другими компонентами системы авиации.[71]

Психологические факторы оказывают влияние на психологическую готовность к действиям в любых обстоятельствах, которые могут сложиться в ходе полета. Среди них: надлежащая подготовка, знания и опыт, зрительные или вестибулярные иллюзии и рабочая нагрузка. Индивидуальная психологическая подготовленность к выполнению профессиональных задач включает мотивацию, отношение к вызывающему риск поведению, уверенность в себе, стресс и т. д. Каждый из этих аспектов влияет на эффективность мышления, на коммуникабельность и умение принимать решения, на способность правильно действовать в экстренных ситуациях. Существует разница в допустимых отклонениях с учетом таких физиологических факторов, как скука, стресс и неопределенность.

Психосоциальные факторы включают в себя все внешние факторы социальной системы индивидуума, действующие как в производственной, так и в нерабочей среде, которые вызывают дополнительную нагрузку, например ссора с начальником, смерть члена семьи, личные финансовые и другие семейные проблемы и др. Эти психосоциальные факторы могут влиять на подход к рабочей ситуации, способность преодолевать стресс, действовать в случае возникновения форс-мажорных обстоятельств.[72] Они формируют обстановку, в котором нормальный, здоровый, квалифицированный и опытный персонал может работать хуже, чем от него ожидается. Чтобы избежать напряженных ситуаций, негативно влияющих на деятельность человека, необходимо правильно понимать последствия несоответствий на границах между различными блоками SHEL и центральным блоком "человек ".[73]

Прежде чем человек может отреагировать на информацию, он должен ее прочувствовать. Здесь существует возможность возникновения ошибок,

---

[70] Основные принципы учета человеческого фактора в руководстве по проведению проверок безопасности полетов. ИКАО Doc9806 AN 763. 2002. С. 2-3.

[71] Основные принципы учета человеческого фактора в руководстве по проведению проверок безопасности полетов. ИКАО Doc9806 AN 763. 2002. С. 2-4.

[72] Основные принципы учета человеческого фактора в руководстве по проведению проверок безопасности полетов. ИКАО Doc9806 AN 763. 2002. С. 2-5.

[73] Основные принципы учета человеческого фактора в руководстве по проведению проверок безопасности полетов. ИКАО Doc9806 AN 763. 2002. С. 2-5.

поскольку сенсорные системы функционируют только в пределах узких диапазонов. Затем информация попадает в мозг, где подвергается обработке, после чего делается вывод о значении этой информации. Такая интерпретационная деятельность, называемая восприятием, является благодатной почвой для ошибок. Ожидания, опыт, установки, мотивация и возбуждение – все это оказывает определенное влияние на восприятие и является возможными источниками ошибок. После формирования выводов относительно значения информации начинается процесс принятия решений. Многие факторы могут приводить к неправильным решениям: подготовка или прошлый опыт; эмоциональные или коммерческие соображения; усталость, прием медикаментов, мотивация, физические или психологические расстройства. Действие (или бездействие) следует за решением, создавая дальнейший потенциал для совершения ошибок. Как только предпринимается действие, начинает работать механизм обратной связи. Недостатки этого механизма могут также приводить к ошибкам.[74]

Стресс создает особые проблемы для экипажа, поскольку его последствия часто бывают трудноуловимыми и их часто бывает тяжело оценить. Хотя любая аварийная ситуация неизбежно порождает стресс, также существуют привносимые в текущую ситуацию каким - либо членом экипажа физический и умственный стрессы, которые другие члены экипажа могут быть не в состоянии обнаружить. Общая годность члена экипажа к полетам может ухудшаться из-за усталости, умственных и эмоциональных проблем и т. д. до такой степени, что другие члены экипажа могут рассматривать его как утратившего эту годность. Умения, связанные с преодолением стресса, касаются не только способности замечать и улаживать стрессы других, но и способности предчувствовать, распознавать и справляться со своим собственным стрессом. Это включает психологические стрессы, связанные с расписанием полетов и графиком смен, волнением, связанным с проверками, а также стрессы, связанные с карьерой и личными достижениями, проблемами межличностных отношений, как внутри самого экипажа, так и с членами других экипажей, с взаимоотношениями в семье и на работе, включая привычные семейные проблемы. Некоторые из ведущих авиакомпаний пытаются снизить проблематичность этих стрессов путем поощрения открытого и искреннего общения между руководством компании и членами летных экипажей, посредством рассмотрения стресса как части концепции годности к полетам. Необходимым условием для этого является признание руководством того факта, что стресс может быть легитимной проблемой летных экипажей.[75]

---

[74] Основные принципы учета человеческого фактора в руководстве по проведению проверок безопасности полетов. ИКАО Doc9806 AN 763. 2002. С. 2-18.

[75] Основные принципы учета человеческого фактора в руководстве по проведению проверок безопасности полетов. ИКАО Doc9806 AN 763. 2002. С. 2-27.

В процессе взаимодействия работников авиационной отрасли на их действия влияет фактор культуры. Различные культуры предполагают разные способы решения общих проблем, с которыми все мы сталкиваемся[76].

Логику суждения можно считать основой для принятия правильных решений. Принимая решение, авиадиспетчер должен учесть все факторы, которые должны повлиять на последствия решения. Если авиадиспетчеры правильно определяют и оценивают все факторы, принимают рациональные решения, то тем самым они демонстрируют хорошую логику суждений. Однако многие из факторов, такие как стресс, скука и усталость, могут влиять на логику суждений и таким образом способствовать ошибкам в суждении. Это включает: что – то делать, чего не следует делать или не делать того, что следует делать; не делать в полном объеме того, что следует делать или делать слишком много из того, что не требуется делать; действия предпринимаются слишком рано, когда еще следует подождать или с задержкой, хотя необходимо действовать без промедления.

Обратная связь играет важную роль для обнаружения ошибок в суждении и инициировании действий по смягчению их последствий. Неспособность обнаружить ошибки повышает вероятность совершения дополнительных ошибок в суждении в связи с получением неправильной информации в результате первой ошибки. Однако распознавание первой ошибки может зависеть от психологической установки авиадиспетчера. Некоторые авиадиспетчеры постоянно демонстрируют такой стиль мышления, который затрудняет выявление ошибок, и они должны понять, что у них такой образ поведения и им следует избавиться от него[77].

Управление воздушным движением часто считается профессией, которая связана с воздействием сильных стрессов вследствие жестких требований к решению задач, дефицита времени и ответственности за возможное последствие ошибок, которые усугубляются вследствие использования непригодного оборудования, а также по причине нехватки квалифицированных авиадиспетчеров. С другой стороны, существует мнение, что благодаря профессиональному отбору, подготовке и опыту, авиадиспетчеры лучше подготовлены, чем многие другие профессии, к действиям в стрессовой обстановке. По статистике в ряде государств значительно увеличилось количество заболеваний, связанных со стрессом.[78] Там существуют дополнительные проблемы, связанные с отсутствием необходимых ресурсов, включая надлежащим образом подготовленных психологов, физиологов, эргономистов, авиационных специалистов, руководителей и законодателей.

---

[76] Основные принципы учета человеческого фактора в руководстве по проведению проверок безопасности полетов. ИКАО Doc9806 AN 763. 2002. С. 4-2.

[77] Основные принципы учета человеческого фактора в руководстве по проведению проверок безопасности полетов. ИКАО Doc9806 AN 763. 2002. С. 7-7.

[78] Основные принципы учета человеческого фактора в руководстве по проведению проверок безопасности полетов. ИКАО Doc9806 AN 763. 2002. С. 7-7.

Заключение

В настоящее время значительно актуализировалось значение вопросов, связанных с выявлением и нейтрализацией угроз в информационной области, необходимость постоянного совершенствования процессов обеспечения ИБ в соответствии с национальными и корпоративными интересами, в том числе в авиатранспортной области. В современной бизнес-среде конкурентоспособны лишь организации, способные эффективно обеспечивать свою информационную безопасность. Теория и практика обеспечения информационной безопасности на российских авиапредприятиях требует более глубокого осмысления и развития с использованием лучших достижений зарубежного опыта. Специалисты ГА Российской Федерации должны соответствовать постоянно возрастающим требованиям в этой области.

В пособии изложены необходимые теоретические сведения о содержании процессов обеспечения информационной безопасности, современных подходах к обеспечению информационной безопасности, организационном, нормативно-правовом, методологическом и технологическом обеспечении данных процессов, их специфики для авиатранспортной отрасли.

Изучение изложенных в учебном пособии теоретических положений и практических вопросов по обеспечению информационной безопасности, с учетом специфики авиатранспортной отрасли, поможет обучаемым овладеть соответствующими профессиональными компетенциями, позволит их обладателю повысить свою конкурентоспособность на рынке труда. Пособие нацелено на выработку у студентов знаний, практических навыков и умений принятия эффективных управленческих решений в области обеспечения информационной безопасности, использования современных подходов при планировании, организации и проведении мероприятий по обеспечению ИБ в условиях обострения критически опасных информационных угроз современной турбулентной бизнес-среды.

Список литературы

1. Васильева И.Н. Управление информационной безопасностью. Учебное пособие. СПб.: Изд-во СПбГЭУ, 2014.
2. Корягин Н.Д. Бизнес-анализ. Учебное пособие. М., МГТУ ГА, 2017.
3. Лукацкий А. В. Кто такие CISO и есть ли они в России? // Inside. Защита информации. - 2007. - № 3. - С. 18-20.
4. Петров В.И., К. Г.Апарина. Основы информационной безопасности. Учебное пособие. М., МГТУ ГА, 2014.
5. Репин В.В., Елиферов В.Г. Процессный подход к управлению. Моделирование бизнес-процессов. –М.: Издательство Манн, Иванов и Фербер, 2013.
6. Родионов М.А. Методологические аспекты информационного аудита в менеджменте предприятия. // Научный вестник МГТУ ГА, № 156 (6). М. 2010.
7. Родионов М.А., Волкова Т.А. Политические коммуникации и властные элиты. // Коммуникология. 2014. Т. 6. № 4, С. 78-87.
8. Родионов М.А. Проблемы информационно-аналитического обеспечения современного стратегического менеджмента. // Научный вестник МГТУ ГА, № 202. М. 2014. С. 65-69.
9. Родионов М.А. К вопросу о формах ведения информационной борьбы. // Военная мысль. 1998. № 2. С.67-69.
10. Родионов М.А. Информационная безопасность (социальные аспекты). М., ВАГШ, 2004.
11. Родионов М.А. Информационная безопасность социального развития. М., ВАГШ, 2006.
12. Родионов М.А. Информационное противоборство: история и современность. // Информационный сборник “Безопасность”, № 7-8 (58). М. 2002. С. 156-166.
13. Родионов М.А. Антикризисное управление. Часть 1. Теоретические положения антикризисного управления. М., МГТУ, 2012.
14. Родионов М.А. Антикризисное управление. Часть 2. Практика антикризисного управления. М., МГТУ, 2014.
15. Родионов М.А. Информационно-аналитическая поддержка принятия решений в антикризисном менеджменте. // Научный вестник МГТУ ГА, № 131 (7), серия Менеджмент, экономика, финансы. М., 2008. С. 126-130.
16. Родионов М.А. Информационная безопасность политических элит. // Социально-Гуманитарные знания. № 1. 2016. С. 107-119.
17. Рекомендации в области стандартизации Банка России РС БР ИББС-2.5-2014 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности" (приняты и введены в действие

распоряжением Банка России от 17.05.2014 г. № Р-400). // ИПС «ГАРАНТ».2018.
18. Родионов М.А. Информационные технологии принятия управленческих решений в современном стратегическом менеджменте. // Научный вестник МГТУ ГА, № 214 (4). М. 2015. С. 105-109.
19. Родионов М.А. Методы защиты информации в современном менеджменте. // Научный вестник МГТУ ГА, № 167. М. 2011. С. 72-78.
20. Свод знаний по управлению бизнес-процессами (BPM CBOK 3.0). – Перевод с английского под редакцией Белайчука А.А., Елифёрова В.Г. – М.: АПУБП, 2015.
21. Ярочкин В.И. Секьюритология – наука о безопасности жизнедеятельности. М., “Ось-89”, 2000.
22. “Virtual Defense” by James Adams. “Foreign Affairs”, 2001. Vol. 80. №. 3. May-June, pp. 98-112.
23. CobiT 4.1. Российское издание. - М.: Аудит и контроль информационных систем, 2008.

ИНТЕРНЕТ-РЕСУРСЫ:

1. Официальный сайт ИКАО. URL: https://www.icao.int/Pages/default.aspx
2. Официальный сайт ШОС. 27.11.2016. URL: http://rus.sectsco.org/news/20161127/160697.html
3. Официальный сайт ИКАО. Решение проблем кибербезопасности в гражданской авиации. 30.05.2016. URL: https://www.icao.int/Meetings/a39/Documents/WP/wp_017_ru.pdf
4. Официальный сайт МИД России. Конвенция об обеспечении международной информационной безопасности (концепция). 22.09.2011. // URL: http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/ CptICkB6BZ29/ content/id/191666
5. Официальный сайт МИД России. Конвенция об обеспечении международной информационной безопасности (концепция). 22.09.2011. // URL: http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/ content/id/191666
6. Cobit 5 for Information Security Introduction, [электронный ресурс]. - URL: http://www.isaca.org/COBIT/ Documents/COBIT-5-for-Information-Security-Introduction.pdf (дата обращения: 29.08.2012).
7. NIST. Computer Security Resource Center. Special Publications (800 Series), URL: http://csrc.nist.gov/publications/ PubsSPs.html.