ВЫСОКИЕ ТЕХНОЛОГИИ

УДК / UDK 004.056.53

РЕГУЛИРОВАНИЕ КИБЕРБЕЗОПАСНОСТИ ГРАЖДАНСКОЙ АВИАЦИИ: ПЕРСПЕКРТИВЫ ВНЕДРЕНИЯ ПРОГРАММЫ МОДЕРНИЗАЦИИ NEXTGEN В РОССИИ И США

Гончарова Н.А.[1]

С внедрением новых технологий в работу объектов критической инфраструктуры их уязвимости перешли в киберпространство, в связи с чем актуален стал вопрос повышения их уровня кибербезопасности. Не является исключением и гражданская авиация, о выявленных уязвимостях которой в последние годы идет активная дискуссия за рубежом. Однако ввиду исключительной важности критической инфраструктуры для государства и его населения, в большинстве случаев регуляторы склонны устанавливать жесткие меры регулирования, которые зачастую не обоснованы с точки зрения реальной оценки риска. В данной статье автор анализирует и сравнивает обоснованность внедрения программы модернизации гражданской авиации NextGen в части повышения уровня кибербезопасности с точки зрения соотносимости издержек регулирования, возлагаемых на его адресатов, с размером ликвидируемого посредством устанавливаемого регулирования риска в России и США.

Ключевые слова:

Кибербезопасность, критическая инфраструктура, гражданская авиация, NextGen, модернизация, оценка регулирующего воздействия, ОРВ, оценка риска.

[1] **Гончарова Наталия Александровна** – эксперт Научно-учебной лаборатории исследований в области бизнес-коммуникаций Национального исследовательского университета «Высшая школа экономики». Адрес: 101000, Москва, ул. Мясницкая, д. 20. E-mail: nagoncharova@hse.ru.

ВВЕДЕНИЕ

С развитием общества правительства стран сталкивались с различными угрозами критической инфраструктуры государства, имеющей ключевое значение для его функционирования и обеспечения его безопасности. Однако стремительное внедрение новых технологий, автоматизация производственных процессов и компьютеризация процессов управления трансформировали уязвимости жизненно важных объектов инфраструктуры в иную плоскость – в киберпространство. Участившиеся случаи кибератак на критическую инфраструктуру в последнее десятилетие и масштабы их последствий продемонстрировали актуальность данной проблемы. Например, атаки на объекты ядерного производства в Натанзе посредством вируса Stuxnet отбросили ядерную программу Ирана, по экспертным оценкам, на два года назад; вирусы семейства BlackEnergy, поразившие электростанции на Украине, оставили без электричества зимой порядка 1,4 млн жителей [29; 38].

В основном исследования в области кибербезопасности критической инфраструктуры фокусируются на энергетике, оставляя неосвещенными остальные отрасли, имеющие объекты критической инфраструктуры (КИ) [31; 39]. Данное исследование призвано сократить данный пробел, проанализировав возможности повышения кибербезопасности гражданской авиации, также являющейся отраслью КИ и имеющей исключительную важность для государств, располагающихся на крупной по площади территории, в России и США посредством внедрения программы модернизации NextGen.

КИБЕРБЕЗОПАСНОСТЬ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

КЛЮЧЕВЫЕ ТЕНДЕНЦИИ

Масштабная автоматизация и компьютеризация различных каждодневных операций, призванные сократить издержки компаний, стали серьезным вызовом для безопасности жизнедеятельности человека. Обратной стороной развития и внедрения в повседневную жизнь ИКТ стало появление многочисленных уязвимостей в используемых компьютерных системах. Согласно данным Лаборатории Касперского, ежедневно в мире обнаруживается более 250 тысяч новых уязвимостей, из которых более 13,5% фиксируется в России [28]. Изо дня в день ими пытаются воспользоваться в собственных корыстных целях в среднем порядка 13,24 млн злоумышленников по всему миру, при этом на Россию приходится около 5,7% общего числа кибератак [28]. Особый интерес со стороны хакеров проявляется в вопросе безопасности критической инфраструктуры ввиду ее особой важности в рамках обеспечения безопасности государства.

КРИТИЧЕСКАЯ ИНФРАСТРУКТУРА. ОБЗОР ЗАКОНОДАТЕЛЬНОЙ БАЗЫ

Термин «критическая инфраструктура» не имеет единого общепринятого определения и разнится от государства к государству. В данном случае следует представить подходы к пониманию КИ, принятые в странах англоязычного блока ОЭСР, которые являются наиболее передовыми в вопросах обеспечения кибербезопасности. В Соединенных Штатах USA PATRIOT Act определяет критическую инфраструктуру в качестве «совокупности физических или виртуальных систем и средств, важных для государства в такой мере, что их вывод из строя или уничтожение могут привести к губительным последствиям в области обороны, экономики, здравоохранения и без-

опасности нации», то есть используется некоторое искаженное разделение объектов по сферам жизнедеятельности человека и функционирования государства [41].

Наиболее доступным для понимания с авторской точки зрения является определение КИ, принятое в Канаде: критическая инфраструктура - это «процессы, системы, объекты, технологии, сети, активы и услуги, необходимые для охраны здоровья, безопасности, экономического благополучия (граждан) и эффективного функционирование правительства», то есть при определении данного термина основываются на интересах экономических акторов [33]. Центр защиты национальной инфраструктуры Великобритании подходит к толкованию термина «национальная критическая инфраструктура» (critical national infrastructure) несколько иначе, определяя его как «объекты, системы, сайты, информация, люди, сети и процессы, необходимые для функционирования государства и лежащие в основе ежедневной жизни, а также сайты и организации, не критичные для предоставления жизненно важных услуг населению, но необходимые для защиты общества от потенциальных угроз».

В России же до сих под законодательно данная дефиниция не определена, однако ключ к ее пониманию косвенно содержится в определении «критически важного объекта», данного в Федеральном законе от 21.12.1994 N 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера», под которым понимается «объект, нарушение или прекращение функционирования которого приведет к потере управления экономикой» государства или его административно-территориальной единицы, «ее необратимому негативному изменению (разрушению) либо существенному снижению безопасности жизнедеятельности населения».

Различается и отраслевой состав объектов КИ, утвержденный законодательно в государственных перечнях. В частности, в США и в России лишь 8 отраслей признаны критическими в обеих странах. Среди них и гражданская авиация, о которой пойдет речь в дальнейшем [19; 10].

Тем не менее, государственные регуляторы осознают исключительную необходимость защиты критической инфраструктуры. Одним инструментов защиты объектов КИ служит установление государственного регулирования в данной области.

ТЕКУЩЕЕ РЕГУЛИРОВАНИЕ КИБЕРБЕЗОПАСНОСТИ

Правовые основы обеспечения безопасности критической инфраструктуры в развитых странах в большинстве своем представлены федеральным регулированием общего характера, не учитывающего отраслевую специфику объектов КИ.

Например, в США большая часть федерального законодательства в области безопасности объектов КИ, принятого в 2000-х гг., являлась реакцией на события 11 сентября 2001 года, продемонстрировавших низкую степень защищенности объектов критической инфраструктуры. Оно представлено следующими основополагающими нормативно-правовыми актами:

- USA PATRIOT Act (октябрь 2001 г.), устанавливающий приоритеты в области обеспечения национальной безопасности;
- Национальная стратегия внутренней безопасности (октябрь 2007 г.), в которой отображены рекомендации по защите ключевой инфраструктуры Соединенных Штатов;

• Национальная стратегия по обеспечению физической безопасности критической инфраструктуры и ключевых активов (февраль 2003 г.), состоящая из указаний по обеспечению безопасности наиболее уязвимых объектов КИ;

• Национальный план защиты критической инфраструктуры (октябрь 2013 г.), содержащего в себе инструменты по взаимодействию в интересах защиты КИ;

• ряд директивных документов по защите объектов КИ.

Тем не менее, узкая направленность ряда угроз, наблюдаемая последнее десятилетие, заставила регуляторов многих стран задуматься о сужении регулирования безопасности не только до отрасли КИ, но и до специфики отдельных видов ее безопасности, что нашло отражение в разрабатываемых отраслевыми ведомствами стандартах для обеспечение различных элементов безопасности.

Ввиду того, что цифровизация экономики многими государственными деятелями обозначена в качестве ключевого драйвера экономического роста на ближайшие десятилетия, ожидается ускорении темпов внедрения информационных технологий в различные ее отрасти, в том числе, и в отрасли критической инфраструктуры. Вместе с ростом объемов и темпов цифровизации ожидается и увеличение численности компьютерных атак на различные объекты инфраструктуры в связи с отсутствием каких-либо конкретных требований, установленных законодательством именно к кибербезопасности.

В общем понимании под кибербезопасностью понимается безопасность компьютерных систем, однако, как и в случае с критической инфраструктурой, более узкое определение термина «кибербезопасность» также разнится от государства к государству.

Национальный институт стандартов и технологий США (NIST) в своей методике «Framework for Improving Critical Infrastructure Cybersecurity» определяет кибербезопасность как процесс защиты информации путем предупреждения, выявления атак и принятия ответных мер [26]. Следовательно, в данном случае кибербезопасность рассматривается в качестве элемента информационной безопасности.

Зачастую кибербезопасность подменяют термином «информационная безопасность», однако данные дефиниции имеют разное содержание. Под информационной безопасностью понимается защита непосредственно данных, «состояние сохранности информационных ресурсов и защищенности законных прав личности и общества в информационной сфере», в то время как кибербезопасность отвечает за сохранность непосредственно компьютерных систем, она по своей сути не является составной частью информационной безопасности, несмотря на определение, данное NIST [1]. Тем не менее, данные виды безопасности тесно взаимосвязаны, так как в век компьютеризации именно техника отвечает за безопасность информации и операций, проводимых с ней. Таким образом, компьютерная безопасность является ключевым фактором к построению информационной безопасности.

В России актуальность проблемы несовершенной защищенности объектов КИ встает еще острее ввиду популярности в России темы цифровизации экономики и отсутствия понимания, как минимум, определения кибербезопасности, не говоря о подходах к ее обеспечению. Российским законодательством до сих пор не определен сам термин «кибербезопасность». Попытки исправить данный пробел были предприняты

в 2014 году, когда на официальном сайте Совета Федерации был размещен для ознакомления проект «Концепции стратегии кибербезопасности Российской Федерации». В соответствии с представленной концепцией, под кибербезопасностью понимается «совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями» [6]. Любопытно, что целью принятия данной концепции было создание базы для унификации российского регулирования в данной сфере при выстраивании дальнейшей совместной международной деятельности в области кибербезопасности с регуляторами других стран, однако данное Советом Федерации определение не соотносится ни с одним из существующих в развитых странах определений.

Некоторые требования к безопасности компьютерных систем в России присутствуют в законодательстве, регулирующем в целом вопросы безопасности автоматизированных систем управления технологическими процессами (АСУ ТП), однако оно носит общий характер и не учитывает особенности каждой из отраслей, имеющих объекты критической инфраструктуры.

ГРАЖДАНСКАЯ АВИАЦИЯ. НЕОБХОДИМОСТЬ МОДЕРНИЗАЦИИ

ОТРАСЛЕВЫЕ РИСКИ В ОБЛАСТИ КОМПЬЮТЕРНОЙ БЕЗПАСНОСТИ

Сбои в функционировании гражданской авиации способны привести к колоссальным издержкам для многих экономических агентов. Согласно отчету Министерства транспорта США, американская экономика ежегодно теряет более $20 млрд. из-за задержек и простоев рейсов, которые зачастую вызваны сбоями в системе управления воздушным транспортом и инцидентами безопасности на объектах инфраструктуры гражданской авиации [14].

Обеспечение воздушной безопасности является ключевой задачей государства по регулированию отрасли, так как ценой авиационного инцидента могут стать сотни человеческих жизней. Если прежде основной сферой регулирования являлась физическая безопасность системы управления воздушным движением, то после 11 сентября 2001 года приоритеты в области нормотворчества сместились в сферу предупреждения террористических актов на объектах инфраструктуры гражданской авиации и в воздухе [30]. До сих пор защита авиации от атак террористов является одним из основных направлений деятельности государства в рамках обеспечения национальной безопасности.

Тем не менее, с усовершенствованием технологической «начинки» современных воздушных средств, систем управления воздушным движением, информационных систем аэропортов и прочих объектов инфраструктуры гражданской авиации и ее элементов возросло и число уязвимостей киберпространства гражданской авиации, которыми зачастую пытаются воспользоваться злоумышленники. Согласно данным юридической фирмы Cozen O'Connor, представленным на международной конференции по риск-менеджменту в 2016 году, Международный аэропорт Майами в среднем подвергается 20 тыс. попыток кибератак в день, а аэропорты Лос-Анжелеса (7 аэропортов) в год в общей сложности подвергаются 2,9 млн хакерских атак [21].

Новый взгляд на проблемы кибербезопасности гражданской авиации пролило предупреждение ФБР, согласно которому эксперту по безопасности Крису Робертсу удалось воспользоваться взаимосвязанностью бортовой сетью WiFi, раздаваемом на борту самолета авиакомпания United Airlines, с его

бортовыми системами и через свой смартфон перехватить управление полетом воздушного судна [23]. По словам специалиста, с 2011 по 2014 год ему удавалось 15 раз проникнуть в бортовые системы с целью изучения их уязвимостей [9]. Подобные уязвимость существует на многих самолетах, в том числе и на ВС производителей Boeing и Airbus, что делает угрозу кибератаки на бортовые системы актуальной [8]. Особо актуально это для России, где более 85 % авиапарка 10 крупнейших авиаперевозчиков состоит из самолетов данных производителей (табл. 1).

ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ

Зачастую при обнаружении пробелов в системах безопасности, в том числе, кибербезопасности производители оборудования ведут себя оппортунистически и не стремятся предпринять своевременные меры по их устранению, во-первых, в связи с высокими издержками данной процедуры (отзыв оборудования, разработка средств защиты и их тестирования и пр.), и, во-вторых, в целях защиты собственной деловой репутации [20]. Также поступили и в Boeing, выпустив заявление о невозможности кибератаки в разобранном выше кейсе [23].

В целях повышения уровня кибербезопасности индустрии при учете высокой вероятности недобросовестного поведения со стороны производителей оборудования для гражданской авиации, необходимым и обоснованным видится установление жесткого регулирования в отрасли. С другой же стороны, избыточность и жесткость регулирования может и дальше стимулировать недобросовестное поведение стейкхолдеров гражданской авиации по уклонению от исполнения норм.

Во многом установление жесткого регулирования в гражданской авиации является следствием и наличия в отрасли мощного наднационального регулятора, а именно ИКАО. В связи с имеющимися уязвимостям компьютерных систем гражданской авиации, со стороны ИКАО было предпринято много попыток по установлению и развитию сотрудничества между ключевыми стейкхолдерами с целью выявления рисков, связанных с киберпространством, и их минимизации. Например, организация разворачивала дискуссию на тему распределения ответственности за кибербезопасность среди стейкхолдеров отрасли с целью разработки дальнейшего регулирования отрасли на уровне национальных регуляторов.

Помимо этого, ИКАО призывала страны внедрять жесткое управление сферой кибербезопасности гражданской авиации и принимать как можно больше мер по предотвращению кибератак, которые могут привести к негативным последствиям. На основе данной позиции организации можно сделать вывод о том, что в ближайшие годы данная сфера может стать излишне зарегулированной, при этом нормотворчество может стать хаотичным. С другой же стороны, готовность национальных регуляторов разных стран можно проследить на примере России: при направлении официального запроса информации о кибератаках в Росавиацию, агентство ответило, что подобной информацией не располагает, так как она не запрашивается у отраслевых стейкхолдеров.

Таким образом, российское отраслевое агентство не обладает данными для разработки мер по регулированию компьютерной безопасности в гражданской авиации, что позволяет сделать вывод о том, что, во-первых, у органа нет представления о текущей ситуации в сфере, во-вторых, регулирование в данной отрасли будет приниматься во многом вслепую и, в-третьих, при разработке мер регулятор не будет обращаться к оценке риска для их обоснования, что может привести, в свою очередь, к излишнему ре-

гулированию и подтверждает тезис, выдвинутый ранее в данной работе.

Желание как можно быстрее зарегулировать сферу кибербезопасности в отрасли с такими высокими рисками, как в гражданской авиации, уже отмеченное выше, усиленное популярностью данной темы приводит к хаотичному нагромождению регуляторных норм и запрещающего характера, ошибочно относимых регуляторами к сфере кибербезопасности.

Наиболее ярким примером является введение в марте 2017 года в США, а затем и в Великобритании запрета на провоз ноутбуков и крупногабаритных гаджетов в ручной клади для путешественников из ряда стран Среднего Востока [43; 15]. Данная мера была призвана усилить антитеррористическую защиту в таких критически значимых объектах инфраструктуры как аэропорты, а также на борту самолетов.

Необходимость в данном запрете возникла в связи с данными ФРБ, согласно которым террористы Исламского государства и подобных ему экстремистских группировок разработали способы обхода существующих систем проверки безопасности аэропорта, устанавливая снаряды со взрывчатым веществом в ноутбуки и мобильные телефоны. Данная версия была подтверждена рядом тестов, по итогам которых сотрудники Бюро обнаружили, что взрывчатка действительно может быть спрятана в деталях батареи ноутбука с помощью подручных средств при сохранении его рабочего состояния и невидимости взрывчатки для систем безопасности [12].

Поводом для экспериментов ФБР и прецедентом дальнейшего ограничения проноса ноутбуков стал взрыв 2 февраля 2016 года на борту самолета, следовавшего из Могадишо в Джибути. Террористический акт был организован группировкой «Аш-Шабааб», входящей в состав Аль-Каиды и действующей на территории Сомали. Террористы-смертники поместили взрывчатку в ноутбук вместо дисковода, в результате чего перед взлетом в ходе проверки она не была обнаружена [12].

С одной стороны, представленная мера напрямую связана с использованием электронных устройств, однако, несмотря на заявления представителей власти, она не относится к сфере кибербезопасности, так как гаджеты в данном случае являются лишь «оболочкой», средством проноса взрывчатки на борт самолета. В связи с этим описанный случай не может быть отнесен к инцидентам кибербезопасности, как и сам запрет не регулирует эксплуатацию компьютерных систем, а является в чистом виде мерой по предупреждению террористической угрозы в гражданской авиации. Этот случай демонстрирует, помимо прочего, отсутствие у регуляторов единого понимания предмета кибербезопасности.

В то же время скептически стоит относится и к эффективности самой меры. Во-первых, запрет проноса электронных устройств распространяется лишь на ручную кладь, в то время как они свободно могут быть провезены на борту того же самолета в грузовом отсеке в багаже, подлежащем к сдаче, а детонатор самой взрывчатки может быть активизирован дистанционно. Во-вторых, запрет распространяется лишь на пассажиров прямых рейсов из ряда аэропортов стран Среднего Востока и рейсы с промежуточной посадкой в Канаде, что дает возможность потенциальным террористам совершить пересадку в другой стране, где системы безопасности также не в состоянии отследить наличие взрывчатки, содержащейся в гаджете, и провести его в ручной клади на борту самолета, держащего курс в Соединенные Штаты.

Табл. 1. Авиапарк топ-10 крупнейших российских компаний на конец 2017 года и стоимость суточной задержки рейса среднего по вместительности пассажиров ВС авиакомпаний.

Серия ВС	Модель ВС	Кол-во пассажиров	*Авиаперевозчик*										*Срвз значение*
			Аэрофлот	Россия	S7-Airlines	Уральские авиалинии	UTair	Победа	Глобус	Azur Air	NordWind	ВИМ-авиа	
Boeing	B777-300	402	16	4	-	-	-	-	-	-	2	1	
	B777-200	364	-	-	-	-	-	-	-	-	4	11	
	B767-300	336	-	-	-	-	-	-	-	7	-	1	
	B767-200	249	-	-	-	-	3	-	-	-	-	-	
	B757-200	238	-	-	-	-	-	-	-	8	-	3	
	B747-400	485	-	4	-	-	-	-	-		-	-	
	B737-800	160	40	15	21	-	9	12	19	6	6	-	
	B737-500	126	-	-	-	-	32	-	-	-	-	-	
	B737-400	159	-	-	-	-	6	-	-	-	-	-	
AirBus	A330	330	22	-	-	-	-	-	-	-	1	1	
	A321	185	37	-	7	14	-	-	-	-	7	-	
	A320neo	164	-	-	4	-	-	-	-	-	-	-	
	A320	180	78	5	18	24	-	-	-	-	-	-	
	A319	144	-	27	19	7	-	-	-	-	-	3	
Sukhoi	SSJ100	98	42	-	-	-	-	-	-	-	-	-	
Embraer	170	78	-	-	17	-	-	-	-	-	-	-	
ATR	72-500	70	-	-	-	-	15	-	-	-	-	-	
АН	74	52	-	-	-	-	5	-	-	-	-	-	
	2	12	-	-	-	-	4	-	-	-	-	-	
Численность авиапарка			235	55	86	45	74	12	19	21	20	20	
Средняя вместимость ВС авиакомпании			190	195	147	176	115	160	160	110	242	310	164
*Стоимость суточной задержки рейса среднего ВС для авиакомпании, €**			439375	450938	339937	407000	265937	370000	370000	254375	559625	716875	380406

*из расчета 1 дня простоя самолета AirBus A380, общей вместимостью до 400 человек [3].

Таким образом, обнаруженная уязвимость систем безопасности не была ликвидирована посредством регулирования, а дополнительные переплаты в связи с увеличением веса провозимого багажа упали на плечи пассажиров.

Если говорить о системе регулирования кибербезопасности гражданской авиации в целом, то в большинстве стран данная область до сих пор регулируется в основном не отраслевым, а межотраслевым законодательством в рамках обеспечения кибербезопасности критической инфраструктуры или транспортной системы.

В Соединенных Штатах для решения данной проблемы был избран путь стандартизации. В 2013 году Правительство США занялось разработкой стандартов обеспечения информационной и кибербезопасности объектов КИ, в том числе и гражданской авиации в рамках указа Б. Обамы по повышению кибербезопасности критической инфраструктуры. Результатом данной деятельности стал стандарт NIST «Framework for Improving Critical Infrastructure Cybersecurity», выпущенный в 2014 году [26]. Данный стандарт призван послужить основой для разработки отраслевых стандартов кибербезопасности, которой сейчас занимаются такие отраслевые регуляторы, как Transportation Security Administration of the U.S. Department of Homeland Security и Federal Aviation Administration of the U.S. Department of Transportation [40].

Осознают власти и необходимость качественно нового технического обновления существующих принципов выстраивания компьютерной архитектуры различных систем гражданской авиации, в результате чего особое внимание было уделено перспективам модернизации отрасли.

В России же не раз выдвигались инициативы по государственному регулированию безопасности авиационной отрасли в целом еще во второй половине 1990-х годов, однако они не получили дальнейшего хода. На данный момент, в соответствии с Воздушным Кодексом РФ, ключевым показателем воздушной безопасности является степень защищенности авиации от незаконного вмешательства [2]. Однако данного рода вмешательство может быть осуществлено и нетипичным для истории гражданской авиации способом при помощи использования уязвимостей в киберпространстве ее систем. Эта сфера до сих пор выпадает из государственного регулирования в России. Фактически первым нормативным правовым актом, затрагивающим данную область, является Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации», который лишь обязывает бизнес сообщать властям об инцидентах в области информационной (де-факто кибер-) безопасности. Таким образом, данный закон абсолютно не учитывает специфики анализируемой отрасли.

В связи с неохваченностью данной сферы государственным регулированием в России и во избежание хаотичного и излишнего нормотворчества в данной области становится актуальным обращение к международному опыту регулирования кибербезопасности в области гражданской авиации и оценка перспектив его внедрения в российских реалиях. В частности, в рамках данной работы будут сравнены перспективы внедрения модернизационной программы NextGen в части повышения уровня кибербезопасности путем оценки регулирующего воздействия программы в США и в России посредством вычисления регуляторных балансов для ключевых стейкхолдеров регулирования (регулятора, адресатов регулирования и пр.).

МЕТОДОЛОГИЯ

ОЦЕНКА РЕГУЛИРУЮЩЕГО ВОЗДЕЙСТВИЯ

Последствия государственного вмешательства в общественные отношения путем установления государственного регулирования в отрасли или изменения отраслевого законодательства в сторону установления новых требований, в данном случае к безопасности полетов, для ключевых стейкхолдеров (как адресатов регулирования, там и для самого регулятора) в рамках данной работы проанализированы посредством упрощенной процедуры оценки регулирующего воздействия (ОРВ, regulatory impact assessment). Данная процедура широко используется в западной практике для обоснования регулирования тех или иных общественных отношений на основе анализа возможных положительных и отрицательных последствий регулирования.

В данной статье в основу ОРВ лег анализ выгод и издержек (cost-benefit analysis) с элементами мультикритериального анализа.

COST-BENEFIT ANALYSIS

Для оценки выгод и издержек регулирования для стейкхолдеров использованы исключительно монетизируемые выходы, тем не менее в работе обозначены и немонетизируемые (квантифицируемые и качественные) выходы, а также предпринята попытка приведения некоторых из них к косвенным экономическим величинам, в частности, в денежном выражении.

Все группы стейкхолдеров разбиты на 3 крупные категории: государство, бизнес и общество (потребители, население) - для обобщенной оценки регуляторной нагрузки на 3 ключевых экономических акторов. Важно отметить, что государство в рамках анализа выступает исключительно в качестве регулятора, в связи с чем госкорпорации, госкомпании и акционерные общества с государственным участием отнесены к категории «бизнес».

Для каждой из идентифицированных групп и категорий стейкхолдеров в рамках проведенного анализа определены ключевые выгоды и издержки регулирования для оценки влияния на них планируемых изменений законодательства и обоснования возлагаемого экономического бремени. По итогам анализа на основе проведенных расчетов сформированы регуляторные балансы как для групп, так и для категорий, позволяющие провести сравнительный анализ регуляторной воздействия при внедрении программы NextGen в США и в России.

RISK ASSESSMENT

В большинстве своем нарушение/прекращение работы объектов критической инфраструктуры влечет за собой возникновение различных негативных последствий, колоссальных по степени ущерба и масштабу, в связи с чем, с одной стороны, установление жесткого регулирования с целью повышения уровня безопасности вполне обосновано, чем регулярно пользуются российские законодатели (стоит вспомнить «пакет Яровой»). С другой же стороны, исполнение жестких норм регулирования нередко ложится тяжелым бременем, в первую очередь, на бизнес, владеющий и управляющий объектами КИ, а также на государство и население. В то время как вероятность неблагоприятного события, в частности, проведения успешной кибератаки (cyberattack likelihood) не столь велика. Таким образом, при более детальном рассмотрении необходимость установления жесткого регулирования может заметно снизиться и выйти за рамки обоснованного.

Для учета данной особенности в исследовании при расчете выгод регулирования (они же экономические потери при

наступлении рискового события, вероятность которого, как подразумевается, будет сведена к нулю при установлении регулирования) используется процедура оценки риска (risk assessment). Согласно рекомендациям Совета ОЭСР, анализ риска (risk assessment) или анализ возникновения рисковых ситуаций – это «методология определения характера и степени риска путем анализа потенциальных опасностей и оценки существующих условий уязвимости, которые вместе могут потенциально нанести вред людям, имуществу, услугам, средствам к существованию и окружающей среде» [36]. Привлечение данного инструмента позволяет скорректировать экономический ущерб от нарушения работы критической инфраструктуры путем учета годовой частотности (annual rate of occurrence) наступления рискового события.

Стоит обратить отдельное внимание на тот факт, что в расчетах использована годовая частотность не самого инцидента (нарушения в работе объекта КИ), которая обычно используется в процедуре оценки риска, а именно случаев успешной кибератаки, то есть несанкционированного проникновения в компьютерную систему в обход систем безопасности при использовании конкретных уязвимостей даже при отсутствии непосредственно негативных последствий. Данная оговорка допустима и значима в связи со спецификой сферы кибербезопасности и, в частности, такой угрозы, как кибератака: в подавляющем большинстве случаев хакеры изначально проникают в компьютерные системы с целью их изучения и тестирования их уязвимостей, при этом имея возможность нанести ущерб работе компьютерной системы и связанным производственным или бизнес-процессам, но не нанося его. Таким образом, наступление неблагоприятного последствия зависит исключительно от целей и намерений конкретно взятого хакера или хакерской группировки. В связи с этим, на взгляд автора, необходим учет зафиксированных случаев кибератак, не приведших к негативным последствиям, но потенциально имеющих такую возможность.

В рамках данного исследования оценка риска выполнена в соответствии с европейским стандартом ISO/IEC 27005:2008, разработанным специально для оценки рисков в сфере IT-безопасности и сфокусированным, в отличие от американского аналога NIST, именно на оценке последствий наступления рискового события без детального анализа сторонних факторов [27; 34].

Алгоритм процедуры оценки риска состоит из трех ключевых этапов:

- Определение риска (Risk Identification);
- расчет риска (Risk Estimation);
- постаналитическая оценка риска (Risk Evaluation).

Определение риска. В основу определения риска легло сценарное планирование. На данном этапе формируются сценарии последствий наступления неблагоприятного события, характерные для IT-отрасли. Для этого необходимо, во-первых, выявить ключевые уязвимости киберсистемы и угрозы, связанные с ними, во-вторых, на основе выявленных угроз идентифицировать связанные бизнес-процессы, а затем сформировать сценарии наступления рискового события и определить его последствии для каждой группы/категории стейкхолдеров в рамках соответствующего сценария.

По своей сути большинство кибератак не способно нанести физический урон непосредственно компьютерным системам, за исключением компьютерного червя Stuxnet, способного физически разрушить

инфраструктуру и предназначенного для приостановки ядерной программы в Иране. В связи низкой распространенностью и узостью применения, Stuxnet не будет учитываться в данной работе. Следовательно, необходимость определения первичных активов (компьютерных систем) для последующей оценки нанесенного непосредственно им ущерба, предусмотренная указанным выше стандартом для оценки нанесения им ущерба в ходе последующих этапов анализа риска, в рамках данной работы перестает быть актуальной.

Таким образом, в качестве результата на данном этапе должны быть сформированы таблицы со сценариями последствий успешной кибератаки (табл. 2).

Табл. 2. Форма представления информации по угрозам в соответствии с методикой исследования.

Уязвимость, цель кибератаки (комп. система)	Угроза	Связанные бизнес-процессы	Сценарий последствий	Последствия успешной кибератаки

Расчет риска. На стадии оценки риска непосредственно производится экономическая оценка последствий наступления неблагоприятного исхода. Различают два подхода к оценке риска: качественный и количественный. В данном исследовании используется количественная оценка риска, так как она основана на использовании статистических данных и подразумевает более точную (при наличии соответствующих данных) экономическую оценку ущерба, в отличие от качественного подхода, в основе которого в качестве источника информации лежит интервьюирование.

В рамках использования risk assessment в качестве убытка от возникновения риска рассчитывается годовой ожидаемый убыток, основанный на данных о количестве случаев неблагоприятного исхода (успешных кибератак) в год и ущерба от одного случая наступления рискового события и описываемый следующей формулой:

$$ALE=ARO \times SLE \quad (1),$$

где ALE (Annualized Loss Expectancy) – годовой ожидаемый убыток, ARO (Annual Rate of Occurrence) – годовая интенсивность потока событий, а SLE (Single Loss Expectancy) – ожидание единичной потери.

Ввиду того, что непосредственно самому активу, то есть компьютерной системе, на которую совершается кибератака, урон не может быть нанесен, но наносится ущерб связанным с данной системой бизнес-процессам, а также объектам, не являющимся составными элементами анализируемого объекта критической инфраструктуры, в данной работе ожидание единичной потери будет рассчитано не как произведение цены первичного актива на фактор воздействия (коэффициент, отображающий долю потери актива), а в качестве суммы ущерба, нанесенного ключевым стейкхолдерам:

$$SLE=\sum SLE_n \quad (2)$$

Постаналитическая оценка риска. На заключительном этапе экономический ущерб, выявленный в ходе каждого сценария, будет распределен по группам/категория стейкхолдеров для подсчета их суммарных прямых издержек при отсутствии регулирования.

ОЦЕНКА ПЕРСПЕКТИВ ВНЕДРЕНИЯ NEXTGEN

NEXT GENERATION AIR TRANSPORTATION SYSTEM

Регуляторы в США, осознавая масштабы угрозы безопасности гражданской

авиации в киберпространстве ввиду многочисленных обнаруженных уязвимостей ее компьютерных систем, приняли решение о необходимости использования комплексного подхода для ликвидации данных чувствительных к кибератакам пробелов в безопасности путем реализации масштабной программы модернизации гражданской авиации Next Generation Air Transportation System (NextGen). Данная программа направлена на техническое улучшение различных составляющих гражданской авиации, в том числе, она призваны повысить и уровень кибербезопасности в отрасли.

Программа модернизации Национальной системы управления воздушным движением (National Airspace System) NextGen была разработана Федеральным управлением воздушного транспорта (Federal Aviation Administration, далее FAA) еще в 2007 году, однако окончание ее реализации намечено на 2025 год, в то время как большинство требований, содержащихся в ней, вступят в силу уже в 2020 году.

Де-юро NextGen является не единой программой, а комплексом программ, систем и процедур по усовершенствованию организации воздушного трафика и управления им. В общем виде данный комплекс содержит 5 крупных программ:

- Automatic dependent surveillance-broadcast (ADS-B) - автоматическое зависимое наблюдение-вещание;
- En Route Automation Modernization (ERAM) Technology Refresh – техническое обновление в рамках модернизации полетной автоматики;
- Data Communications – передача данных;
- 2nd segment of the System Wide Information Management (SWIM) – 2-й сегмент расширения информационной системы управления воздушным трафиком;
- National Airspace System (NAS) Voice System – голосовая система национальной системы организации воздушного пространства.

NextGen была разработана с целью снижения издержек в отрасли и уменьшению негативного воздействия на окружающую среду посредством перехода существующей системы УВД наземного базирования к использованию более точных спутниковых технологий, то есть посредством роста цифровизации операционных процессов. В работе будет оценена обоснованность данной программы непосредственно в рамках повышения уровня кибербезопасности гражданской авиации.

Несмотря на тот факт, что данное работа рассматривает только одну сферу, затрагиваемую NextGen, для повышения компьютерной безопасности отрасли необходима реализация всех составляющих элементов данной комплексной программы модернизации, так как их корректное функционирование взаимосвязано между собой, что значительно упрощает процедуру расчетов издержек регулирования.

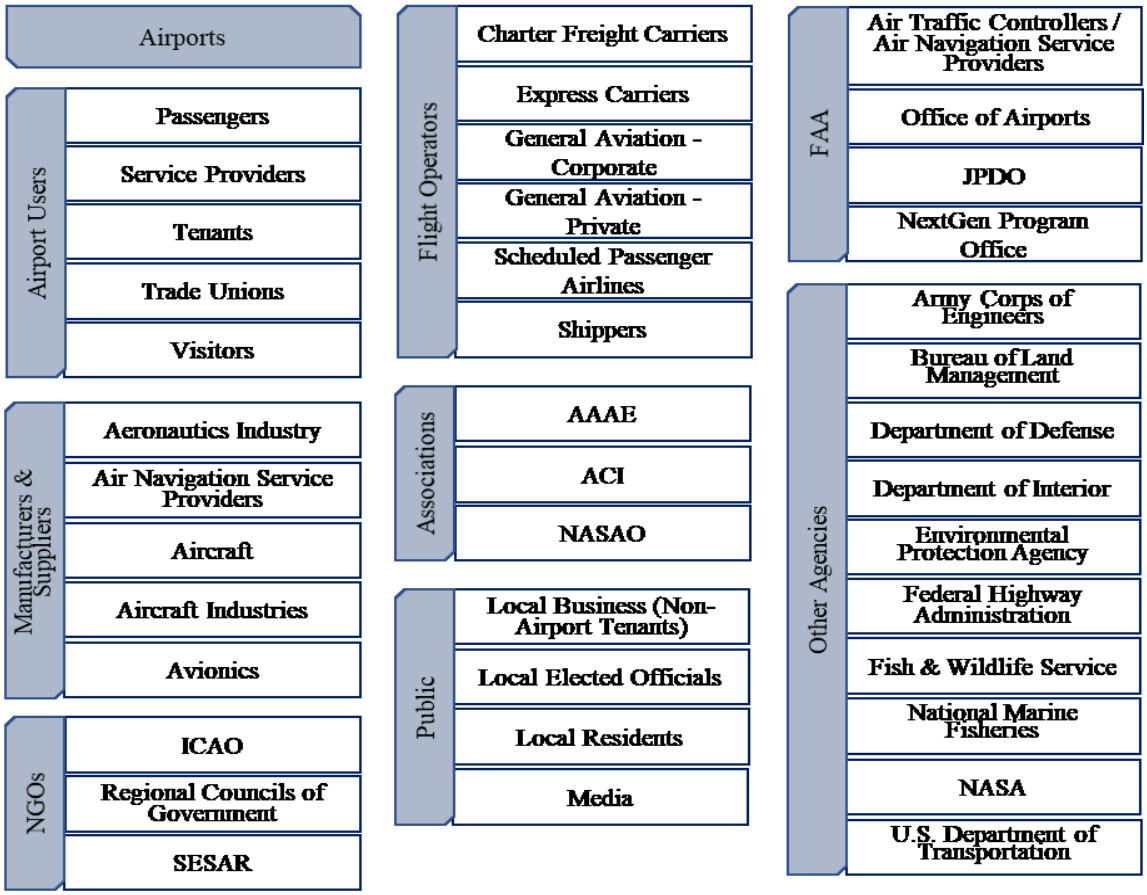
Как уже было отмечено ранее, программа является первым этапом перехода к использованию спутниковых технологий в авиации, в связи с чем основные издержки по ее реализации завязаны на тестировании необходимого нового оборудования и его приобретении ключевыми отраслевыми стейкхолдерами к 2020 году, когда вступает в силу требование по его обязательному использованию операторами воздушного движения. Примечательно, что для реализации данной программы FAA были привлечены партнеры самого различного характера: авиакомпании, аэропорты, производители авиационного оборудования, государственные органы США и других стран, отраслевые организации и вузы (рис. 1).

Широкий круг представленных стейкхолдеров во многом объясняется разносторонностью программы и охватываемых ею сфер жизнедеятельности человека. В рамках данного исследования будут рассмотрены лишь несколько из них, ключевые экономические агенты, затронутые сферой кибербезопасности в части издержек и выгод устанавливаемого регулирования: отраслевые регуляторы (государство), авиакомпании и страховые компании (бизнес), пассажиры (население). Вторая группа (страховые компании) введена исключительно для дальнейшего проведения оценки риска, хотя и не является прямым адресатом регулирования.

КЕЙС США

Для проведения оценки регулирующего воздействия сперва необходимо обозначить роль каждого стейкхолдера через призму издержек регулирования и рассчитать их совокупную величину для оценки экономического бремени, возлагаемого рассматриваемыми регуляторными мерами на протяжении всего срока реализации NextGen (с момента внедрения непосредственно самой меры)

Рис. 1. Полная карта стейкхолдеров комплекса программ NextGen.



В Соединенных Штатах основным отраслевым регулятором является FAA. Именно оно в рамках данного кейса рассматривается в качестве единственной группы стейкхолдеров, входящей в категорию «государство».

На основании заявленных расходов бюджета в рамках NextGen FAA планирует потратить порядка $20,600 млн на реализацию программы; при этом часть данных расходов будет направлена на деятельность Технического центра Уильяма Дж. Хьюса (WJHTC), который является единственной в

своем роде базой FAA для исследования, тестирования, оценки и развития NAS с условиями, максимально приближенными к реальным. Остальная сумма бюджетных расходов будет направлена на переустройство основной инфраструктуры (замена наземного оборудования, установка и настройка оборудования для спутниковой навигации) и развитие информационно-коммуникационных систем. Несмотря на то, что в работе данный комплекс программ модернизации рассматривается исключительно в части кибербезопасности, все программы, входящие в NextGen и перечисленные ранее, взаимосвязаны, как уже было отмечено ранее, в связи с чем взаимосвязаны и расходы на их реализацию. Следовательно, вся заявленная сумма в рамках данной работы может рассматривается в качестве издержек регулирования, возлагаемых непосредственно на регулятора.

Внушительные издержки по реализации NextGen возложены и на негосударственных экономических агентов. По оценке Министерства транспорта США, покупка и установка нового оборудования обойдется американским авиакомпаниям более, чем в $15 млрд. (табл. 3). Если распределить данные издержки среди 10 крупнейших по пассажиропотоку американских авиакомпаний (при учете того, что 3 из них контролируют 80% всех авиаперевозок США), то издержки на оборудование необходимой техникой в краткосрочном периоде составят $3,6 млн в расчете на одно воздушное судно (табл. 4).

Табл. 3. Издержки авиаперевозчиков по переоборудованию ВС, в $ млрд [42].

Operator Type	***Baselined Improvements***	***Anticipated Improvements***	***Total Improvements***
Commercial Aviation	4.5	0.8	5.3
General Aviation	4.6	5.2	9.8
Total	**9.1**	**6.0**	**15.1**

Табл. 4. Размеры авиапарка 10 крупнейших по пассажирообороту авиаперевозчиков США на 2018 год.

Aviation Operator	***Fleet Size***
American Airlines	950
Delta AirLines	857
Southwest Airlines	717
United Airlines	754
Alaska Airlines	316
JetBlue Airways	243
Spirit Airlines	119
Frontier Airlines	78
Allegiant Air	100
Hawaiian Airlines	53
Total	**4187**

Ожидается, что авиакомпании попробуют в среднесрочном периоде переложить экономическое бремя на пользователей услуг авиаперевозок – пассажиров. Если полагать, что авиакомпании предпочтут окупить оборудование к окончанию реализации программы NextGen при объеме пассажирооборота авиалиний США, приближенного к значениям 2015 года (798,4 млн чел.), то стоимость авиабилетов в среднем возрастет минимум на $1,89, что не ударит по потребительскому кошельку.

В соответствии с проанализированными данными, наибольшие издержки несут государство и бизнес, в тоже время издержки населения тождественны издержкам авиаперевозчиков, но невелики при условии

их распределения между пассажирами (табл. 5).

Как уже было сказано прежде, ядром программы служит переход на спутниковую навигацию, в результате которого будет сокращено число наземных радиолокационных комплексов (РЛК), подвергавшихся кибератакам с целью введения в систему коммуникации ложных данных о фактическом местоположении самолета в системе «земля-воздух» и рельефе близлежащих территорий.

Табл. 5. Издержки регулирования по стейкхолдерам.

Категория стейкхолдеров	***Группа стейкхолдеров***	***Описание издержек***	***Размер издержек, $ млрд***
Государство	FAA	Заявленные бюджетные расходы по реализации программ	20.6
Бизнес	Авиакомпании	Переоборудование ВС (краткосрочный период)	15.1
Население	Пассажиры	Повышение стоимости авиабилетов (среднесрочный период)	15.1

Реализация данной комплексной программы модернизации поможет ликвидировать сразу 2 серьезные уязвимости компьютерных систем гражданской авиации. Ликвидация первой из них - пробелы в системе безопасности коммуникации с воздушным судном (ВС) посредством наземных локационных установок, которые могут использоваться хакерами для передачи ложной информации о местоположении ВС - являлась одной из целей NextGen [5]. Другая же - взаимосвязь бортовых систем с сетью WiFi, раздаваемой на борту для общего пользования - была обнаружена случайно уже после утверждения программы, о ней уже упоминалось прежде. В целом кибератаки, основанные на данных уязвимостях, проводятся с целью тестирования систем безопасности, однако могут использоваться для целенаправленного нанесения ущерба и приводят к схожим последствиям: к нарушению запланированного маршрута полета с последующим нарушением расписания ряда рейсов и их задержкой, а также к авиакатастрофам (табл. 6).

Вторая уязвимость позволяет целиком контролировать полет, в отличие от первой, что дает возможность злоумышленнику более точно реализовать свой замысел и повышает вероятность нанесения большего урона. Тем не менее, в целях упрощения проведения оценки экономических последствий по представленным сценариям, в общем виде совпадающим для обеих обозначенных уязвимостей, данное исследование будет основываться на равенстве оценочных величин данных последствий для указанных уязвимостей.

Существует еще один сценарий развития событий с установлением ряда требований со стороны террористов во избежание совершения террористического акта; в рамках данной работы не рассматривается, однако такой вариант развития события имеет место быть.

Табл. 6. Уязвимости, ликвидируемые программой NextGen, и сценарии наступления рискового события.

Уязвимость, (комп. система)	*Угроза*	*Связанные бизнес-процессы*	*Сценарий последствий*	*Последствия успешной кибератаки*
Пробел в системе безопасности наземных локационных установок	Передача ложных геолокационных данных на борт самолета	a) Управление ВС; b) Управление полетами в рамках транспортного узла	1.1 Оптимистичный	«Тестирование» системы безопасности злоумышленником, поиск и изучение уязвимостей; передача неверных данных, не угрожающих безопасности полета. Негативные последствия отсутствуют.
			1.2 Сдержанно оптимистичный	Задержка ряда рейсов в связи с нарушением запланированных маршрута и времени полета атакуемого ВС.
			1.3 Пессимистичный	1.3.1 Крушение воздушного судна 1.3.1.1 на открытой местности 1.3.1.2 в черте населенного пункта
				1.3.2 Столкновение нескольких ВС и их крушение 1.3.2.1 на открытой местности 1.3.2.2 в черте населенного пункта
Взаимосвязь бортовой сети WiFi с бортовыми системами воздушного судна	Дистанционный перехват управления через подключение к бортовой сети WiFi	a) Управление ВС; b) Управление полетами в рамках транспортного узла	2.1 Оптимистичный	«Тестирование» системы безопасности злоумышленником, поиск и изучение уязвимостей. Негативные последствия отсутствуют.
			2.2 Сдержанно оптимистичный	Задержка рейса в связи с нарушением запланированного маршрута и времени полета атакуемого ВС.
			2.3 Пессимистичный	2.3.1 Крушение воздушного судна 2.3.1.1 на открытой местности 2.3.1.2 в черте населенного пункта
				2.3.2 Столкновение нескольких ВС и их крушение 2.3.2.1 на открытой местности 2.3.2.2 в черте населенного пункта

В рамках дальнейшего исследования будет рассмотрено 3 общих сценария: задержка рейса, крушение 1 ВС на открытой местности и столкновение нескольких (2) ВС на открытой местности. Ввиду сложности подсчета экономических потерь в случае падения одного/нескольких воздушных суден на территории населенного пункта, а также отсутствия негативных последствий при тестировании компьютерных систем на уязвимости, оптимистичные сценарии исключаются из последующего анализа. Помимо этого, рассматриваются инциденты, произошедшие исключительно в воздухе, в связи с чем исключается рассмотрение потенциальных прямых экономических потерь аэропортов.

Согласно сдержанно оптимистичному сценарию кибератаки на наземные системы локации, авиакомпания терпит дополнительные издержки только непосредственно за простой ВС. За среднюю стоимость за-

держки рейса в США на сутки примем стоимость задержки воздушного судна AirBus A380, общей вместимость до 400 пассажиров, которая составляет €925,000, что приблизительно соответствует $1,087,153 (по курсу Forex на 19.05.2018) [3]. В данную стоимость уже включены услуги аэропорта и компенсационные выплаты пассажирам задержанного рейса. Наиболее популярной моделью ВС в США является Boeing B737-800, в частности, самолеты данной модели составляют практически 1/3 авиапарка самой крупной по пассажирообороту американского авиаперевозчика American Airlines (304/951) [13]. Данная модель вмещает в себя до 160 пассажиров. Условимся, что издержки простоя находятся в прямо пропорциональной зависимости от вместимости ВС, тогда издержки суточной задержки B737-800 составляют порядка $434,861.

Государственные же структуры, согласно законодательству Соединенных Штатов, не несут ответственность за задержку рейсов, в связи с чем их издержки в рамках данного сценария равны нулю.

Издержки же пассажиров можно представить в качестве суммы, тождественной сумме компенсационных выплат за задержку рейса, то есть не более $700 на человека. Следовательно, общие издержки данной группы стейкхолдеров от суточной задержки одного рейса B737-800 составят $112 тыс. [17]. Данный подход не отображает полной картины многоструктурных реальных издержек пассажиров, таких как потеря времени, поиски жилья, дополнительные расходы на транспорт и т.д., но дает возможность усреднить данные затраты для оценки.

В рамках второго сценария в случае крушения самолета на открытой местности, общие убытки авиакомпании состоят из 2-х основных частей: непосредственно потеря самого воздушного судна и выплата компенсации семьям жертв авиакатастрофы.

Заводская стоимость нового B737-800 на 2015 г. составляет $96 млн, однако в авиапарках компаний большинство самолетов не являются новыми, то есть необходимо учесть стоимость самолета за вычетом амортизации. Средний возраст ВС модели B737-800, находящихся в парке авиакомпании American Airlines, насчитывает в среднем 8,3 года [24]. На ВС коэффициенты амортизации для планера (часть самолета без силовой установки) и для двигателя разнятся. Для первого он составляет 8% в год, а для второго – 10%. Тем не менее, отталкиваясь от условного единства конструкции в рамках данной работы для расчета следует взять наибольший коэффициент. Таким образом, стоимость ВС при учете износа вычисляется по следующей формуле:

$$RA = FC \times k^n \quad (3),$$

где RA – переоцененная стоимость ВС, FC – первоначальная стоимость ВС, k – коэффициент амортизации, а n – возраст ВС. В соответствии с данной формулой при расчете износа на полные 8 лет переоцененная стоимость B737-800 составит приблизительно $40.89 млн.

Что же касается выплат пассажирам, то авиакомпания в соответствии с Монреальской конвенцией, к которой присоединились США, обязана выплатить членам семьи погибшего до $170 тыс. в том случае, если рейс был международным [32]. По итогам расчетов экономические потери авиакомпании в рамках анализируемого сценария превысят $68 млн.

Помимо этого, определенные выплаты – по обязательному страхованию – осуществляют страховые компании. В среднем максимальная сумма выплаты составляет $221,875 (табл. 7). Следовательно, общая

сумма выплат при крушении B737-800 достигает $35.55 млн.

Табл. 7. Максимальная сумма страховых выплат в случае гибели пассажира в результате авиакатастрофы [25].

Company	*Plan*	*Policy Limit, $000*
CSA	Custom Luxe	100
	Custom	50
Global Alert	Preferred Plus	100
HTH Worldwide	TripProtect e-Saver	200
	Trip Protector Preferred	200
	Trip Protector	100
M.H. Ross	Bridge	100
	Complete	250
Seven Corners	Liaison Silver	100
	RoundTrip	25
Travelex	Travel Max	50
Travel Guard	Silver	500
	Flight Guard	500
	Adventure Travel	500
	Basic	500
	Gold	500
	Platinum	500
Travel Insurance	Voyager Annual	500
	Worldwide Trip Protector	100
	Worldwide Trip Protector Gold	100
	Atlas Medical	50
	Ticket Protection Plan	100
	Trip Protector Lite	100
	Trip Protector Lite Expanded	100
	Average	**221,875**

В данном случае обязательство по выплате компенсаций ложится и на государственные органы. Во-первых, из бюджета выделяются средства в размере заработной платы погибшего за 5 лет. Медианная заработная плата в США в 2017 году составила $37.69 тыс., то есть сумма выплаты семьям 160 погибших пассажиров за 5 лет составит $30,152 тыс. [16]. Во-вторых, государство компенсирует семьям погибших в авиакатастрофе моральный ущерб в размере $250 тыс. Таким образом, общие издержки государства от авиакатастрофы составят порядка $68 млн.

Существует множество подходов к расчету ценности человеческой жизни, используемых, в том числе, и при расчете экономических потерь при авиакатастрофе. Согласно оценкам Министерства транспорта США, ценность человеческой жизни расчетов составляет $9.6 млн [37]. Именно данная цифра закладывается министерством при расчете выгод предотвращения авиакатастрофы. Следовательно, экономические потери пассажиров Boeing B737-800 в общей сложности составят $1.536 млрд.

Соответственно при столкновении двух самолетов издержки стейкхолдеров, рассчитанные для крушения одного самолета на открытой местности и в черте населенного пункта, увеличиваются в 2 раза.

В таблице 8 представлены чистые экономические потери стейкхолдеров. В рамках оценки риска эти расчеты необходимо скорректировать годовую частотность наступления рискового события, то есть успешной кибератаки. Однако издержки стейкхолдеров при внедрении программы NextGen были рассчитаны на 10 лет, с момента вступления в силу первых требований программы и до окончания реализации программы, в связи с чем и частотность кибератак в рамках оценки риска будет рассчитана на 10 лет.

В открытом доступе отсутствует статистика кибератак на радиолокационный комплекс, однако публично известен случай кибератаки на компьютерные системы FAA, в результате которого произошли сбои в РЛК по всей стране, включая Атланту, Бостон и Чикаго [18]. Итогом данного сбоя стали многочисленные задержки рейсов. Ввиду того, что данный случай является единичным общеизвестным (содержится в

базе инцидентов индустриальной безопасности (Repository of Industrial Security Incidents)) случаем подобного рода, а общее количество отложенных рейсов неизвестно, он будет использован в качестве единственного возможного за 10 лет случая задержки 1 (!) рейса, следовательно, общие экономические потери, представленные в таблице 9 в рамках сценария 1.2 и 2.2, не нуждаются в корректировке.

Табл. 8. Экономические потери стейкхолдеров по категориям и группам в США (NextGen).

№ сценария	*Категория стейкхолдеров*	*Группа стейкхолдеров*	*Экономические последствия*	*Размер ЭП, $ тыс.*	*∑ЭП, $ тыс.*
1.2 ***2.2***	Государство	FAA	-	-	-
	Бизнес	Авиакомпании	Простой ВС в аэропорту (услуги аэропорта, компенсации пассажирам)	1,087	1,087
		Страховые компании	-	-	
	Население	Пассажиры	Потеря времени, тождественная сумме компенсационных выплат	112	112
1.3.1.1 ***2.3.1.1***	Государство	FAA	Компенсация морального ущерба	40,000	70,152
			Выплаты семьям погибших из расчета среднего заработка за 5 лет	30,152	
	Бизнес	Авиакомпании	Потеря воздушного судна	40,894	103,594
			Выплата компенсации в соответствии с Монреальской конвенцией	27,200	
		Страховые компании	Страховые выплаты по обязательному страхованию жизни	35,500	
	Население	Пассажиры	Стоимость жизни в соответствии с оценкой U.S. DoT	1,536,000	1,536,000
1.3.2.1 ***2.3.2.1***	Государство	FAA	Компенсация морального ущерба	80,000	140,304
			Выплаты семьям погибших из расчета среднего заработка за 5 лет	60,304	
	Бизнес	Авиакомпании	Потеря воздушного судна	81,788	207,188
			Выплата компенсации в соответствии с Монреальской конвенцией	54,400	
		Страховые компании	Страховые выплаты по обязательному страхованию жизни	71000	
	Население	Пассажиры	Стоимость жизни в соответствии с оценкой U.S. DoT	3,072,000	3,072,000

Что касается кибератак с использованием связанности сети WiFi с бортовыми системами воздушного судна, то, как уже говорилось в описании кейса в теоретической части, по данным ФБР, хакеру за 4 года удалось 15 раз обойти системы безопасности, воспользовавшись данной уязвимостью. Таким образом, за 10 лет данное количество успешных попыток могло достичь порядка 37 кибератак. В таблице 8 приведены сценарные общие экономические потери стейкхолдеров в США, скорректированные на частотность успешных кибератак.

Для расчета же окончательных экономических потерь, которые будут использованы для определения баланса «выгоды-издержки» регулирования, необходимо сложить общие сценарные издержки. В данном исследовании потери от уязвимости РЛК являются реальными, так как успешная кибератака повлекла за собой негативные последствия, в то время как экономические потери от взлома бортовых систем через WiFi являются потенциальными, так как хакер не воспользовался возможностью нанести ущерб. В связи с этим необходимо сло-

жить сценарные ЭП первой из-за первой уязвимости с ЭП каждого из 3 сценариев, вызванных второй уязвимостью и в дальнейшем для каждого мегасценария посчитать баланс регулирования (рис. 2, табл. 9).

Рис. 2. Формирование мегасценариев и вычисление сценарных экономических потерь (ЭП).

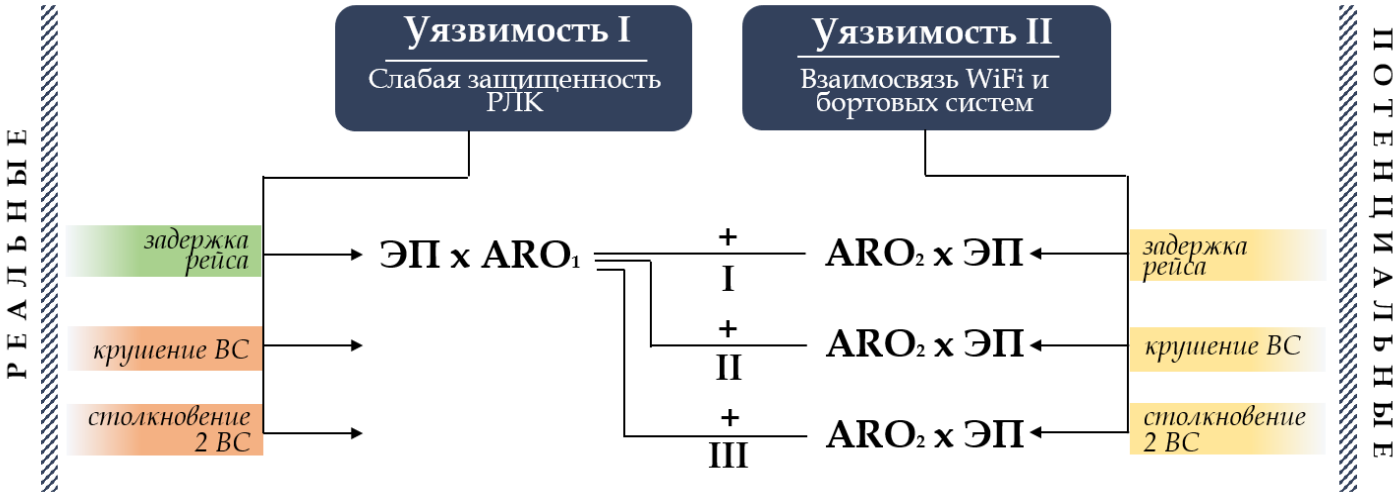


Табл. 9. Экономические потери стейкхолдеров в США в рамках мегасценариев.

		ЭП, ($000)					
	Мегасценарии	**I**		**II**		**III**	
	Сценарии	1.2	2.2	1.2	2.3.1.1	1.2	2.3.2.1
Группы стейкхолдеров	FAA	-	-	-	2,595,624	-	5,191,248
		-		2,595,624		5,191,248	
	Авиакомпании	1,087	40,219	1,087	25,119,478	1,087	50,238,954
		41,306		25,120,565		50,240,043	
	Страховые компании	-	-	-	1,313,500	-	2,627,000
		-		1,313,500		2,627,000	
	Пассажиры	112	4,144	112	56,832,000	112	113,664,000
		4,256		56,832,112		113,664,112	

На основании результатов расчета баланса регулирования можно сделать вывод, что в двух мегасценариях (II, III) из трех издержки негосударственных стейкхолдеров обоснованы (табл. 10). Выгоды бизнеса и общества исчисляются миллиардами долларов. Единственными стейкхолдерами, которым выгодна реализация программы модернизации в части кибербезопасности при любом мегасценарии, являются страховые компании. В то же время, к сожалению, главным недостатком NextGen являются колоссальные расходы государственного бюджета на реализацию программы, об окупаемости которых не идет и речи.

Табл. 10. Балансы регулирования при внедрении комплексной программы NextGen по группам и категориям стейкхолдеров в США.

Мега-сценарий	***Группа Стейкхолдеров***	***Издержки регул-я, ($000)***	***Выгоды регул-я, ($000)***	***Баланс регул-я, ($000)***	
				Для группы	**Для категории**
I	FAA	20,600,000	0	- 20,600,000	- 20,600,000
	Авиакомпании	15,100,000	41,306	- 15,058,694	- 15,058,694
	Страховые компании	0	0	0	
	Пассажиры	15,100,000	4,256	- 15,095,744	- 158,095,144
II	FAA	20,600,000	2,595,624	- 18,004,376	- 18,004,376
	Авиакомпании	15,100,000	25,120,565	10,020,565	11,334,065
	Страховые компании	0	1,313,500	1,313,500	
	Пассажиры	15,100,000	56,832,112	41,732,112	41,732,112
III	FAA	20,600,000	5,191,248	- 15,408,752	- 15,408,752
	Авиакомпании	15,100,000	50,240,043	35,140,043	37,767,043
	Страховые компании	0	2,627,000	2,627,000	
	Пассажиры	15,100,000	113,664,112	98,564,112	98,564,112

КЕЙС РОССИИ

Теперь оценим перспективы внедрения программы NextGen в российских условиях при том же наборе сценариев. В рамках первого из анализируемых сценария развития событий издержки, по своей сути идентичные уже ранее рассчитанным для Соединенных Штатов, несут только авиаперевозчики и пассажиры.

Для оценки средней стоимости суточной задержки рейса для российских авиакомпаний необходимо найти средневзвешенную вместимость воздушного судна каждой из компаний и помножить на стоимость 1 суток простоя самолета пассажировместимостью 1 человек. По итогам проведенных расчетов, в среднем российским авиакомпаниям подобная задержка обойдется в €380,406, что составляет $447,814 по курсу Forex на 19.05.2018.

Что касается издержек пассажиров, то они также, как и прежде, будут тождественны компенсационным выплатам за суточную задержку рейса. В России компенсация за отложенный рейс рассчитывается 2-мя способами:

- в размере 25% от МРОТ за каждый час задержки;
- в размере 3% от стоимости билета за каждый час опоздания.

Для поведения расчетов наиболее удобен первый способ, так как данные о МРОТ находятся в открытом доступе. С 1 мая 2018 года МРОТ в Российской Федерации составляет ₽11,163, следовательно, выплаты на одного пассажира за 24 часа задержки рейса составят $1,083.4, а на 164 пассажира (средняя вместимость российского самолета) – $177.7 тыс. (по курсу ЦБ России на 18.05.2018) [11].

В рамках второго сценария - крушения самолета на открытой местности – необходимо вычислить экономический ущерб авиаперевозчиков при потере самолета и при выплате компенсаций, издержки страховых компаний, а также рассчитать экономический ущерб, нанесенный пассажирам (семьям пассажиров, погибших в авиакатастрофе).

Для расчетов данного вида издержек от потери воздушного судна российского авиаперевозчика, как и для американского,

будет взят B737-800, так как он шире всего представлен среди отечественных авиакомпаний. По исследованиям издательства РБК, средний возраст самолетов поколения Boeing 737 Next Generation, представителем которого является B737-800, на ноябрь 2015 года составляла 9,1 года, следовательно, сейчас он достиг 11 лет [4]. Следовательно, при учете износа по тем же коэффициентам, что были использованы прежде, стоимость данного ВС ориентировочно составляет $29,812 тыс.

Что же касается компенсационных выплат, то законодательно в России ответственность авиакомпании за гибель пассажира в результате авиакатастрофы достигает до ₽2 млн на человека, однако в связи с тем, что в апреле 2017 года Россия присоединилась к Монреальской конвенции, ближайшее время ожидается увеличение суммы компенсации погибшим пассажирам международных рейсов до $170 тыс. Так как средняя вместимость самолета российского авиапарка составляет 164 пассажира, то итоговые экономические потери пассажиров составят $27,880 тыс.

Сумма выплаты при обязательном страховании жизни в России эквивалентна сумме 120 МРОТ, значит, сумма страховой выплаты за одного пассажира составит ₽1,339,569 тыс. или $21.668 тыс. и $3,466 тыс. на всех пассажиров рейса, потерпевшего крушение (по курсу ЦБ России на 18.05.2018).

Государство периодически выплачивает семьям погибших определенные суммы, однако делает это исключительно на добровольной основе (обязательство и порядок законодательно не установлены) в рамках распоряжений Президента, в связи с чем данные выплаты не будут учитываться в издержках.

Стоимость же человеческой жизни в 2016 году, по данным РОСГОССТРАХ, составила ₽4.5 млн или $76,025 (по курсу ЦБ России на 18.05.2018) [7]. На основе средней вместимости ВС в России (табл. 11) суммарные издержки данной группы стейкхолдеров составят порядка $12,468.

Теперь также необходимо скорректировать экономические потери по категориям и группам стейкхолдеров на частоту успешных кибератак. При проведении оценки риска для России будут использованы те же данные по частотности успешных атак на компьютерные системы гражданской авиации, что и для США, ввиду отсутствия актуальных для России данных у отраслевого регулятора. Мегасценарные издержки отображены в таблице 12.

Табл. 11. Экономические потери стейкхолдеров по категориям и группам в России.

№ сценария	*Категория стейкхолдеров*	*Группа стейкхолдеров*	*Экономические последствия*	*Размер ЭП, $ тыс.*	*∑ЭП, $ тыс.*
1.2	Государство	ФОИВ	-	-	-
2.2	Бизнес	Авиакомпании	Простой ВС в аэропорту (услуги аэропорта, компенсации пассажирам)	447.814	447.814
		Страховые компании	-	-	
	Население	Пассажиры	Потеря времени, тождественная сумме компенсационных выплат	177.7	177.7
1.3.1.1 ***2.3.1.1***	Государство	ФОИВ	-	-	-
	Бизнес	Авиакомпании	Потеря воздушного судна	29,812	61158

			Выплата компенсации в соответствии с Монреальской конвенцией	27,880	
		Страховые компании	Страховые выплаты по обязательному страхованию жизни	3,466	
	Население	Пассажиры	Стоимость жизни в соответствии с оценкой РОСГОССТРАХ	12,468.1	12,468.1
1.3.2.1	Государство	ФОИВ	-	-	-
2.3.2.1	Бизнес	Авиакомпании	Потеря воздушного судна	59,624	122,316
			Выплата компенсации в соответствии с Монреальской конвенцией	55,760	
		Страховые компании	Страховые выплаты по обязательному страхованию жизни	6,932	
	Население	Пассажиры	Стоимость жизни в соответствии с оценкой РОСГОССТРАХ	24,936.2	24,936.2

Далее необходимо рассчитать издержки стейкхолдеров по внедрению NextGen в России. Так как данная программа обладает высокой структурированностью, в части издержек авиакомпании для упрощения вычислений можно скорректировать издержки на разницу между размерами авиапарка топ-10 авиакомпаний США (4,187 ВС) и России (586 ВС). Таким образом, расходы российских авиаперевозчиков в общей сумме составят $2,116,967 тыс., идентичными будут и издержки пассажиров. В связи с тем, что органы власти, участвующие в реализации программы, не имеют выгод регулирования, то есть в любом случае для них баланс регулирования окажется отрицательным, условно для расчетов возьмем государственные расходы FAA.

Табл. 12. Экономические потери стейкхолдеров в РФ в рамках мегасценариев.

		ЭП, ($000)					
	Мегасценарии	**I**		**II**		**III**	
	Сценарии	1.2	2.2	1.2	2.3.1.1	1.2	2.3.2.1
Группы стейкхолдеров	ФОИВ	-	-	-	-	-	-
		-					
	Авиакомпании	447.814	16,569.118	447.814	173,076	447.814	346,152
		17,016.932		173,523.814		36,599.814	
	Страховые компании	-	-	-	12824	-	256484
		-		12824		256484	
	Пассажиры	177.7	4,354.3	177,7	461,319.7	177,7	922,639.4
		4,532		461,497.4		922,817.1	

В ходе анализа было выявлено, что баланс регулирования для всех рассмотренных групп стейкхолдеров в России отрицателен в рамках всех трех мегасценариев, что говорит об отсутствии необходимости внедрения данной программы в текущем ее виде в современных российских условиях (табл. 13).

Единственной группой, «оставшейся в плюсе», являются страховые компании, однако это связано с тем, что они не являются адресатами регулирования и, следовательно, не несут регуляторных издержек.

Табл. 13 Балансы регулирования при внедрении комплексной программы NextGen по группам и категориям стейкхолдеров в РФ.

Мега-сценарий	*Группа стейкхолдеров*	*Издержки регул-я, ($000)*	*Выгоды регул-я, ($000)*	*Баланс регул-я, ($000)*	
				Для группы	**Для категории**
I	ФОИВ	20,600,000	0	- 20,600,000	- 20,600,000
	Авиакомпании	2,116,967	17,016.932	- 415,035	- 415,035
	Страховые компании	0	0	0	
	Пассажиры	2,116,967	4,532	-2,112,435	-2,112,435
II	ФОИВ	20,600,000	0	- 20,600,000	- 20,600,000
	Авиакомпании	2,116,967	173,523.814	- 1,943,443.186	- 1,930,619.186
	Страховые компании	0	12,824	12,824	
	Пассажиры	2,116,967	461,497.4	-1,655,469.6	-1655,469.6
III	ФОИВ	20,600,000	0	- 20,600,000	- 20,600,000
	Авиакомпании	2,116,967	36,599.814	- 2,080,367.186	-2,054,719.186
	Страховые компании	0	25,648	25,648	
	Пассажиры	2,116,967	922,817.1	- 1,194,150	- 1,194,150

СРАВНИТЕЛЬНАЯ ОЦЕНКА ОБОСНОВАННОСТИ РЕГУЛИРОВАНИЯ

На стадии обзора литературы и ознакомления со спецификой функционирования гражданской авиации ожидалось, что высокая интегрированность данной отрасли в процесс глобализации, функционирование на международном уровне и наличие внушительных по полномочиям наднациональных регуляторов, оказывающих серьезное влияние на национальную отраслевую политику государств, выступят в качестве гарантов установления на национальном уровне ежели не схожих, то близких условий для осуществления деятельности ключевых стейкхолдеров (национального регулятора и адресатов регулирования), в результате чего выгоды и издержки регулирования для ключевых стейкхолдеров будут близкими по значению.

Несмотря на это, результаты проведенной оценки регулирующего воздействия мер кибербезопасности на примере комплексной программы модернизации NextGen опровергли указанное выше предположение. Единственным экономическим актором, имеющим положительный баланс, является стейкхолдер, по сути не являющийся адресатом анализируемых мер регулирования, а именно страховые компании.

Различие баланса «издержки-выгоды» между государствами во многом объясняется различной социальной ответственностью за факт авиакатастрофы, возложенной на себя государственными структурами. Так, в США выплаты семьям жертв авиакатастрофы закреплены законодательно и совершаются на постоянной основе, в то время как в России они назначаются указом Президента от случая к случаю, так как законодательно не закреплены выплаты компенсаций на постоянной основе.

Разницу балансов российских и американских авиакомпаний можно объяснить меньшими издержками российских авиаперевозчиков при наступлении рискового события в рамках каждого из трех рассматриваемых сценариев. В связи с относительно более возрастным авиафлотом, ущерб авиакомпаний от потери воздушного судна в России практически в 2 раза ниже, чем в Соединенных Штатах, как и ниже стоимость суточного простоя воздушного судна в аэропорту. Выше в США и компенсация за

задержку рейса, в отличии от России, где суммы компенсации во много ничтожны.

Особо стоит отметить колоссальную разницу в оценке стоимости человеческой жизни в США и России, которая приводит к такому же разрыву балансов регулирования в данных странах.

Таким образом, и для России, и для Соединенных Штатов программа модернизации NextGen в части кибербезопасности возлагает и на регулятора, и на адресатов регулирования необоснованно высокое экономическое бремя. Тем не менее, для США данная программа более актуальна для внедрения при должной адаптации и пересмотре ее положений в части расходов государства и требований к стейкхолдерам частного сектора.

ОГРАНИЧЕНИЯ ИССЛЕДОВАНИЯ

В данной работе проведение многих расчетов стало возможно благодаря ряду допущений и ограничений исследования. В первую очередь, стоит отметить ограничения, касающиеся выбора стейкхолдеров регулирования для проведения дальнейшего анализа. Исключение нескольких групп стейкхолдеров обосновано тем, что в работе в рамках анализа выгод и издержек для конечного подсчета баланса могли быть использованы только монетизируемые и прямые выгоды и издержки. Помимо этого, в анализ были включены и экономические агенты, не являющиеся адресатами регулирования, но несущие колоссальные экономические потери в случае проведения успешной кибератаки. Стоит отдельно отметить и исключение присутствия государства в бизнесе, которое безусловно имеет место быть в анализируемых отраслях (например, Аэрофлот), и рассмотрение его исключительно в качестве регулятора, что не отображает действительный баланс регулирования для данного экономического актора.

Что же касается выстраивания логики расчетов в рамках процедуры risk assessment, то она основана на экономических потерях не всех представителей обозначенных групп стейкхолдеров, а, например, лишь топ-10 самых крупных из них, что несколько искажает общую картину, хотя в общем виде дает довольно приближенное к реальному положению дел понимание. Кроме того, в издержки государства закладываются только заявленные издержки по внедрению регуляторных мер, в то время как издержки мониторинга их соблюдения и исполнения другими стейкхолдерами не включены в анализ ввиду сложности их оценки и отсутствия открытой информации.

Отдельно стоит отметить, что внедрение анализируемых мер предполагает ликвидацию обозначенных уязвимостей, которые могут быть использованы злоумышленниками для проведения успешной кибератаки, однако в то же время они могут породить и новые не рассматриваемые прежде уязвимости, использование которых потенциально может привести к гораздо более серьезным последствиям. Так, например, в письме Исследовательской службы Конгресса США от 18 июня 2015 года обращается внимание на уязвимость технологии ADS-B (одно из технических нововведений программы), которая на данный момент не подразумевает необходимость шифрования сигналов; в тому же данная технология особо уязвима в связи с использованием открытой архитектуры [35]. В данном письме отмечены и несколько других слабых мест киберпространства модернизированной гражданской авиации, использование которых могут вызвать череду негативных последствий [22].

ЗАКЛЮЧЕНИЕ

На данный момент регуляторы различных стран еще не готовы рационально и взвешенно отвечать на современные вызовы безопасности в киберпространстве. Отсутствие четкого понимания данной сферы на фоне «импульсивных» попыток минимизации рисков для жизни граждан и функционирования государства приводит к установлению хаотичного и необоснованного с точки зрения баланса выгод и издержек стейкхолдеров регулирования кибербезопасности критической инфраструктуры. Более того, зачастую принимаемые меры подвергают подлежащие защите активы и процессы еще большей угрозе, что было выявлено при анализе комплексной программы NextGen. Данный факт свидетельствует о низком качестве выстроенной на государственном уровне системе управления рисками, в частности, в США, что имеет исключительную важность при регулировании отраслей с высокими рисками, в том числе, и отраслей критической инфраструктуры.

Данное исследование показало необходимость проведения более детального анализа выгод и издержек регулирования ключевых стейкхолдеров в таких комплексных высокорисковых отраслях, как гражданская авиация, и исключения общего подхода и уход от множества допущений и ограничений при изучении международного опыта с целью оценки перспектив внедрения мер кибербезопасности данной отрасли в России ввиду высокой стоимости объектов отраслевой критической инфраструктуры, сложности их взаимосвязей и высоких рисках.

Ожидалось, что как в России, так и в США внедрение программы NextGen приведет к установлению схожих регуляторных балансов. Этому способствовало и наличие мощного наднационального регулятора в лице ИКАО, а также деятельность ряда других международных отраслевых организаций, общее построение отрасли, схожий модельный ряд оборудования и единые поставщики техники. Тем не менее, итоговая разница между анализируемыми странами в балансах как групп, так и категорий ключевых стейкхолдеров оказалась колоссальной. Стоит отметить, что данное исследование требует проведения более глубокого анализа, как в рамках процедуры regulatory impact assessment в целом, так и risk assessment в частности.

Так или иначе, с практической точки зрения проведенное исследование выявило невозможность предварительного прогнозирования последствий принятия тех или иных мер ввиду их непредсказуемости и наличия сложных взаимосвязей как между стейкхолдерами, так и между процессами, игнорирование значимости которых может привести к негативным эффектам при внедрении конкретных мер. В следствии на основе практической части данной работы можно сделать вывод о необходимости развития института доказывания и применении процедуры оценки регулирующего воздействия не в порядке исключения, а на постоянной основе, особенно тех регуляторных мер, которые касаются сферы безопасности государства и его населения, в том числе и кибербезопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Безопасность: теория, парадигма, концепция, культура. Словарь-справочник / Автор-сост. профессор В. Ф. Пилипенко. 2-е изд., доп. и перераб. — М.: ПЕР СЭ-Пресс, 2005.

2. Воздушный кодекс Российской Федерации от 19.03.1997 N 60-ФЗ (ред. от 31.12.2017).

3. Во сколько обходится задержка A380? [Электронный ресурс] URL:

http://aviakomplekt.ru/skolko-stoit-prostoj-a380/ (Дата обращения: 04.05.2018).

4. Исследование РБК: на чем летает Россия // РБК [Электронный ресурс] URL: https://www.rbc.ru/research/society/27/11/2015/564de81a9a79472dab71463a (Дата обращения: 12.05.2018).

5. Международная конференция «Беспилотная авиация - 2017» //Центр стратегических разработок в гражданской авиации [Электронный ресурс] URL: http://aviacenter.org/d/166600/d/bespilotnye_aviatsionnyye_sistemy_i_kiberbezopasnost.pdf (Дата обращения: 08.01.2018).

6. Проект «Концепции стратегии кибербезопасности Российской Федерации» // Совет Федерации Федерального Собрания РФ [Электронный ресурс] URL: http://www.council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (Дата обращения: 08.01.2018).

7. Стоимость человеческой жизни в России в 2015 году составила 4,5 млн. рублей // РОСГОССТРАХ [Электронный ресурс] URL: http://www.rgs.ru/media/CSR/on_startup/Life_value_2015.pdf (Дата обращения: 04.05.2018).

8. ФБР уличило хакера в перехвате управления самолетом // Портал деловой авиации [Электронный ресурс] URL: http://www.ato.ru/content/fbr-ulichilo-hakera-v-perehvate-upravleniya-samoletom (Дата обращения: 20.01.2018).

9. ФБР предупредило авиакомпании о возможных атаках хакеров // Русская служба BBC https://www.bbc.com/russian/international/2015/04/150422_fbi_airlines_hack (Дата обращения: 20.01.2018).

10. Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

11. Федеральный закон от 07.03.2018 N 41-ФЗ «О внесении изменения в статью 1 Федерального закона «О минимальном размере оплаты труда».

12. Airports and nuclear power stations on terror alert as government officials warn of 'credible' cyber threat / The Telegraph [Электронный ресурс] URL: http://www.telegraph.co.uk/news/2017/04/01/airports-nuclear-power-stations-terror-alert-government-officials/ (Дата обращения: 20.01.2018).

13. American Airlines Fleet Details and History [Электронный ресурс] URL: https://www.planespotters.net/airline/American-Airlines (Дата обращения: 12.04.2018).

14. Beyond Traffic: 2045 Final Report // U.S. Department of Transportation [Электронный ресурс] URL: https://www.transportation.gov/policy-initiatives/beyond-traffic-2045-final-report (Дата обращения: 03.05.2018).

15. Britain will ban electronic devices on flights from six Middle Eastern nations amid terror threat / The Telegraph [Электронный ресурс] URL: http://www.telegraph.co.uk/news/2017/03/21/exclusive-britain-poised-follow-us-ban-laptops-ipads-flights/ (Дата обращения: 20.01.2018).

16. Bureau of Labour Statistics // U.S. Department of Labour [Электронный ресурс] URL: https://www.bls.gov (Дата обращения: 08.05.2018).

17. Claim compensation for your flight delay or cancellation // AirHelp [Электронный ресурс] URL: https://www.airhelp.com/en/ (Дата обращения: 08.05.2018).

18. Computer Problems Causes Flight Delays // The Repository of Industrial Security

Incidents [Электронный ресурс] URL http://www.risidata.com/Database/Detail/computer_problems_causes_flight_delays (Дата обращения: 18.05.2018).

19. Critical Infrastructure Sectors / U.S. Department of Homeland Security [Электронный ресурс] URL: https://www.dhs.gov/critical-infrastructure-sectors# (Дата обращения: 15.02.2018).

20. Cyber-Security, a new challenge for the aviation and automotive industries // Harvard Journal of Strategic Threat Intelligence [Электронный ресурс] URL: http://blogs.harvard.edu/cybersecurity/files/2017/01/Cybersecurity-aviation-strategic-report.pdf (Дата обращения: 22.03.2018).

21. Cyber Security in Aviation // Cozen O'Connor. 2016 Risk Management Conference [Электронный ресурс] URL: https://www.aci-na.org/sites/default/files/gs-10_aci-na_presentation.pdf (Дата обращения: 21.02.2018).

22. FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen // U.S. Government Accountability Office [Электронный ресурс] URL: https://www.gao.gov/assets/670/669627.pdf (Дата обращения: 15.05.2018).

23. FBI probe of alleged plane hack sparks worries over flight safety // The Washington Post [Электронный ресурс] URL: https://www.washingtonpost.com/business/economy/fbi-probe-of-plane-hack-sparks-worries-over-flight-safety/2015/05/18/8f75e662-fd69-11e4-805c-c3f407e5a9e9_story.html?utm_term=.44ea631122bd (Дата обращения: 21.02.2018).

24. Fleet Age American Airlines // Airfleets Aviation [Электронный ресурс] URL: http://www.airfleets.net/ageflotte/American%20Airlines.htm (Дата обращения: 14.04.2018).

25. Flight Accident Coverage // Travel Insurance Review [Электронный ресурс] URL: http://www.travelinsurancereview.net/coverages/flight-accident/ (Дата обращения: 17.04.2018).

26. Framework for Improving Critical Infrastructure Cybersecurity // National Institute of Standards and Technology [Электронный ресурс] URL: https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.11.pdf (Дата обращения: 10.01.2018).

27. ISO/IEC, "Information technology -- Security techniques-Information security risk management" ISO/IEC FIDIS 27005:2008.

28. Kaspersky Cyberthreat Real-Time Map // Kaspersky Lab [Электронный ресурс] URL: https://cybermap.kaspersky.com/stats (Дата обращения: 13.05.2018).

29. Katz Y. Stuxnet Virus Set Back Iran's Nuclear Program by 2 Years // The Jerusalem Post [Электронный ресурс] URL: https://www.jpost.com/Iranian-Threat/News/Stuxnet-virus-set-back-Irans-nuclear-program-by-2-years (Дата обращения: 12.04.2018).

30. Kittichaisaree K. Public International Law of Cyberspace. – Springer, 2017. – T. 32.

31. Lewis T. G. Critical infrastructure protection in homeland security: defending a networked nation. – John Wiley & Sons, 2014.

32. Montreal Convention 1999 // International Air Transport Association [Электронный ресурс] URL: https://www.iata.org/policy/Documents/MC99_en.pdf (Дата обращения: 03.05.2018).

33. National Strategy and Action Plan for Critical Infrastructure / Government of Canada/ P. 2 [Электронный ресурс] URL:

https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf (Дата обращения: 15.02.2018).

34. NIST SP 800-30 Risk Management Guide for Information Technology Systems [Электронный ресурс] URL: https://csrc.nist.gov/publications/detail/sp/800-30/archive/2002-07-01 (Дата обращения: 16.02.2018).

35. Protecting Civil Aviation from Cyberattacks // Federation of American Scientists [Электронный ресурс] URL: https://fas.org/sgp/crs/homesec/IN10296.pdf (Дата обращения: 08.04.2018).

36. Recommendation of the Council on the Government of Critical Risks / OECD. May 2014 [Электронный ресурс] URL: http://www.oecd.org/gov/risk/Critical-Risks-Recommendation.pdf (Дата обращения: 16.02.2018).

37. Revised Departmental Guidance 2016: Treatment of the Value of Preventing Fatalities and Injuries in Preparing Economic Analyses // U.S. Department of Transportation [Электронный ресурс] URL: https://cms.dot.gov/sites/dot.gov/files/docs/2016%20Revised%20Value%20of%20a%20Statistical%20Life%20Guidance.pdf (Дата обращения: 12.05.2018).

38. Russians Have Learned How to Hack Power Grids. A December power outage in Ukraine was caused by a malware attack // Bloomberg [Электронный ресурс] URL: https://www.bloomberg.com/view/articles/2016-01-07/russians-have-learned-how-to-hack-power-grids (Дата обращения: 14.04.2018).

39. Ten C. W., Manimaran G., Liu C. C. Cybersecurity for critical infrastructures: Attack and defense modeling // IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans. – 2010. – Т. 40. – №. 4. – С. 853-865.

40. Transportation Security: Protecting Passengers and Freight // Transportation Security Administration [Электронный ресурс] URL: https://www.tsa.gov/news/testimony/2016/04/06/statement-peter-neffenger-administrator-transportation-security-0 (Дата обращения: 16.05.2018).

41. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 [Электронный ресурс] URL: https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/html/PLAW-107publ56.htm (Дата обращения: 15.02.2018).

42. US bans laptops, iPads and other electronic devices on flights from certain Middle Eastern airports / The Telegraph [Электронный ресурс] URL: http://www.telegraph.co.uk/news/2017/03/20/donald-trump-announce-ban-passengers-dozen-countries-carrying/ (Дата обращения: 20.01.2018).

CIVIL AVIATION CYBERSECURITY REGULATION: PROSPECTS FOR IMPLEMENTING NEXTGEN MODERNIZATION PROGRAM IN RUSSIA AND THE UNITED STATES

Goncharova Natalia – Expert of the Research and Education Laboratory of Business Communications Study of the National Research University - Higher School of Economics. Address: 20 Myasnitskaya Ulitsa, Moscow, 101000, Russia. E-mail: nagoncharova@hse.ru.

Implementation of high-tech turns the vulnerabilities if critical infrastructure into cyberspace, in this connection the issue of increasing the level of cybersecurity has become relevant. Civil aviation is no exception, which new vulnerabilities and threats have been discussed over recent years. Due to high importance of critical infrastructure to every state and its citizens state bodies are prone to establishing strict regulation whereas these measures are not always justified in the framework of real risk dimension. In this article the author analyzes and compares the validity of NextGen civil aviation modernization program implementation in Russia and the United States with regard to balance of regulatory costs and risk dimension.

Key words:

Cybersecurity, critical infrastructure, civil aviation, NextGen, modernization, regulatory impact assessment, RIA, risk assessment.