Необходимо точное толкование данной проблемы с юридической точки зрения и установление определенных норм возмещения морального ущерба людям, купившим билет, на место, которого нет.

Многие авиакомпании России открыто заявляют, что комфорт пассажиров для них на первом месте, однако, о каком комфорте может идти речь, если человек не уверен в том, что он сможет улететь в нужный ему день.

Покупая билет, люди рассчитывают на порядочность перевозчика и строят соответствующие планы, и, какой бы не была компенсация, она вряд ли может возместить человеку пропущенное событие: семейный праздник, важную встречу, поход в театр или иное мероприятие.

В заключении следует отметить, что инициатива ПАО «Аэрофлот» в этой сфере выглядит как небольшой шаг вперед и обращает внимание общественности на данную проблему. Однако, такой маленький шаг по легализации сверхбронирования может не понизить среднюю стоимость билета на 2%, а наоборот лишь повысить стоимость на билеты с известными заранее датой и временем вылета.

1. Мартиросян Т.Э., Павлюк А.В. Вопросы разграничения гражданско-правовой ответственности в случае авиакатастрофы // Проблемы экономики и юридической практики. No 1. 2018. - С. 83-87.
2. LIVEJOURNAL <http://auzu.livejournal.com/data/atom>
3. Авиаперелет/ Эконом Билет :<http://ekonombilet.ru/metka/aviaperelet>
4. Овербукинг: риск оказаться за бортом:<https://www.advgazeta.ru/ag-expert/advice/overbiking-risk-okazatsya-za-bortom/>

Корниец Е.О.

Информационная безопасность социально-экономических систем

*Кубанский государственный аграрный университет им. И.Т. Трубилина
(Россия, Краснодар)*

doi: 10.18411/trnio-12-2021-36

Научный руководитель: Затонская И.В.

Аннотация

В статье рассматривается определение социально-экономических систем, подходы к их защите, а также создание и описание системы безопасности для данных систем.

Ключевые слова: социально-экономическая система, информационная безопасность, конфиденциальность, информация.

Abstract

The article discusses the definition of socio-economic systems, approaches to their protection, as well as the creation and description of a security system for these systems.

Keywords: socio-economic system, information security, confidentiality, information.

Социально-экономические системы представляют из себя экономические и социальные институты, взаимодействие между собой которых заключается в производстве, распределении и потреблении материальных и нематериальных ресурсов, а также в распределении, обмене и потреблении товаров и услуг.

Современные социально-экономические системы используют новейшие информационные технологии, которые позволили создать довольно обширную базу данных. Для обеспечения информационной безопасности данных систем не только исследуют составляющие их технические системы, но и управление персоналом в определенных экономических ситуациях, учитывая человеческий фактор, что является проблемой. Время идет, а вместе с ним происходят изменения и в социально-экономических системах, такие

как: создание данных систем людьми, различные закономерности определяют ее эффективность, а также достижение цели, посредством выработки управленческих сигналов из-за воздействий внешней среды. Учитывая эти моменты сохранение конфиденциальности информации становится одной из первостепенно важных задач. Но также, интересующая субъектов информация должна быть доступной. Информационная система включает в себя следующие технические средства для работы с данными: средства обработки, обмена и хранения. Чтобы обеспечить доступность информации, необходимо, чтобы социально-экономическая система, в которой она хранится и обрабатывается, своевременно и беспрепятственно разрешала доступ.

Субъектам, которые попытаются несанкционированно получить доступ, может наноситься информационный ущерб. Объектами, которые стоит защитить для обеспечения безопасности, являются: сама информация, носители, на которых она содержится, а также ее обработка. Заинтересованность субъектов в реализации некоторых свойств информационной системы приводит к тому, что они сами становятся уязвимыми.

Очередной проблемой является изучение специфики информационной безопасности социально-экономических систем и различных социальных и экономических факторов, которые составляют основу всего функционала информационной системы.

Самыми важными видами информации, которая подлежат защите, являются: научная, производственная, экономическая и другая информация, которая составляет коммерческую тайну; персональные данные субъектов.

Разглашение открытой информации может нести за собой ущерб, но несущественный, и только в том случае, если она будет обладать следующими свойствами: доступность, целостность или защита от тиражирования, которое не было санкционировано правообладателем.

Специалисты по информационной безопасности говорят, что нужно поработать над созданием более точных прогнозов изменений, а также быстро и оперативно на них реагировать. Именно эти действия помогут приспособиться, тем самым эффективнее решать задачи, которые ставят перед сотрудниками данные изменения.

Современной концепцией безопасности информационных систем является повышение требований к оперативности и сроку службы их работы. У данных требований есть две стороны влияния: с одной, они требуют разработки и создание эффективных видов защиты от несанкционированного доступа; с другой, их использование ограничено для исполнения функционала системы. Решение данных противоречий заключается в том, чтобы рациональнее использовать защитные ресурсы в зависимости от сложившихся обстоятельств.

Учитывая данные условия, система безопасности должна не то чтобы категорически ограничивать доступ сотрудникам к информации, а распределять между ними полномочия во время коллективного решения поставленных задач, проводить анализ и распознавать необычное потребление ресурсов, прогнозировать чрезвычайные происшествия, устраняя их последствия, адаптируя структуру при блокировке или потере информационного ресурса. Используя данную модель действий, в такой системе должна присутствовать идентификация пользователя как по имени его учетной записи, паролю, биометрии, так и по модели его поведения. При работе с очень важной или, даже, секретной информацией, на определенных стадиях система может потребовать у сотрудника прохождение контрольного теста, данные которого она сравнит с результатом прошлого тестирования и запишет эти данные в свою БД. Также, для того чтобы провести дополнительную проверку можно использовать скрытую аутентификацию набора на клавиатуре. Она поможет определить, кто является «ложным оператором». Полученные статистические данные позволяют производить корректировку модели поведения персонала.

При решении данной задачи потребуется социально-психологический портрет субъекта, который отражает его особые качества, индивидуальность, интересы, наклонности, способности, характер, темперамент, идеалы, принципы, а также волевые, эмоциональные и

интеллектуальные особенности, профессиональная квалификация и жизненный опыт. Исследования показали, что решение данной задачи состоит не в том, чтобы проводить анализ психо-типа, а в изучении социального, бытового, культурного и исторического окружения, в котором индивид желает найти призвание в обществе. Различного рода факторы, а в особенности человеческий, положили начало созданию и развитию рациональному планированию и организации информационных, телекоммуникационных, вычислительных и трудовых ресурсов по типу «матрица». Данная система способна централизованно, гибко и безопасно распределять ресурсы организаций, которые нужны при решении управленческих задач в динамической обстановке. Управление – функция, обеспечивающая хранение и воспроизводство элементов собственной структуры и оптимальное взаимодействие между ними.

Для закрытой системы безопасности, необходимо создать целостную структуру, подчиненную определенным установкам. Есть ряд факторов, которые повысят качество управления системой безопасности: структурная архитектура, которая характеризуется своим функциональным назначением и упорядоченностью элементов; характеристики работоспособности, которые задаются их разработкой для достижения определенных целей.

С одной стороны, если базовые защитные системы справляются со своей задачей, то административные обязанности разделяются между, собственно, самими администраторами данных систем и другими сотрудниками по иерархии. С другой, если использовать дополнительные системы защиты, то это потребует более эффективного решения поставленных задач с помощью рационального распределения обязанностей между сисадминами. Решением данной дилеммы является создание не централизованной управленческой системы, сисадмин которой сможет производить координацию управленческой деятельности. При использовании хоть одной из множества систем информационной безопасности, риск того, что посторонние и не зарегистрированные в базе данных системы лица получают несанкционированный доступ к информации предприятия – сильно понижается.

1. Осенний В. В. Перспективы применения методов и средств имитационного моделирования в аграрной сфере / В. В. Осенний, О. Ю. Франциско // Труды кубанского государственного аграрного университета. – 2019. – № 79. – С. 55–60.
2. Гришина, Н.В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - М.: Форум, 2018. - 118 с.
3. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: Форум, 2018. - 256 с.
4. Осенний В.В. Методические особенности преподавания дисциплины "Методы исследования и моделирования процессов и технологий управления" для магистрантов, обучающихся по направлению подготовки "Информационные системы и технологии" / В. В. Осенний, С. И. Турлий // Практико-ориентированное обучение: опыт и современные тенденции : Сборник статей по материалам учебно-методической конференции. – 2017. – С. 250-251.
5. Бабаш, А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2019. - 432 с.

Кулагина М.К., Хаматова А.Р., Григорьева Д.Р.

Управление запасами предприятия в целях их эффективности использования

*Набережночелнинский институт КФУ
(Россия, Набережные Челны)*

doi: 10.18411/trnio-12-2021-37

Аннотация

В статье затрагивается тема управления запасами предприятия с целью повышения эффективного функционирования. Политика управления запасами представляет собой часть