МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Тольяттинский государственный университет»

Институт финансов, экономики и управления
(наименование института полностью)

38.04.01 Экономика
(код и наименование направления подготовки)

Аудит, учет, экономическая безопасность в организациях
(направленность (профиль))

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

на тему: IT – аутсорсинг как инструмент обеспечения информационной безопасности экономических субъектов

Обучающийся Л.А. Мартынова
(Инициалы Фамилия) (личная подпись)

Научный руководитель к.э.н., доцент Л.Ф. Бердникова
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2023

Содержание

Введение

Актуальность и научная значимость настоящего исследования. Глобализация информационного пространства, разработка новых видов кибероружия привели к т ому, что российские экономические субъекты превратились в цели для международных корпораций и иностранных государств.

Для реализации эффективной системы информационной безопасности экономической деятельности требуется создание единой базы данных, где необходимо сохранять все сведения о происходивших инцидентах информационной безопасности, методах и используемых методиках борьбы с ними, заключения специалистов, посвященные анализу угроз. Создавая базу знаний, необходимо опираться на понятие информационной и экономической безопасности, подразумевающее под собой такое состояние коммерческой, финансовой, производственной и любой другой бизнес-активности на предприятии, при котором ему невозможно или затруднительно нанести экономический ущерб. От вида бизнеса, сектора экономики, кадровой политики и используемых ресурсов зависит модель угроз.

В настоящее время большую актуальность приобретает использование ИТ-аутсорсинга в системе безопасности предприятия.

Использование предприятиями услуг аутсорсинговых компаний способствует оптимизации бюджета организации и сосредоточению на профессиональной деятельности организации.

Объекты исследования: Управление культуры Администрации г.о. Сызрань, Департамент культуры Администрации г.о. Тольятти, Департамент культуры и молодежной политики Администрации г.о. Самара.

Предмет исследования: IT – аутсорсинг как инструмент обеспечения информационной безопасности экономических субъектов.

Цель исследования: проанализировать особенности обеспечения информационной безопасности экономических субъектов на примере Управления культуры Администрации г.о. Сызрань и разработать проект внедрения IT – аутсорсинга как инструмента обеспечения информационной безопасности Управления культуры Администрации г.о. Сызрань, оценить его эффективность.

Гипотеза исследования состоит в том, что использование IT – аутсорсинга позволит обеспечить информационную безопасность экономических субъектов. В процессе исследования необходимо решить следующие задачи:

- исследовать теоретические аспекты использования IT – аутсорсинга в качестве инструмента обеспечения информационной безопасности экономических субъектов;
- проанализировать особенности обеспечения информационной безопасности экономических субъектов;
- разработать проект внедрения IT – аутсорсинга как инструмента обеспечения информационной безопасности Управления культуры Администрации г.о. Сызрань и оценить его эффективность.

Теоретико-методологическую основу исследования составили труды отечественных и зарубежных учёных в области экономики, учета, аудита и экономической безопасности.

Базовыми для настоящего исследования явились также работы в сфере информационной безопасности экономических субъектов и экономической эффективности.

Методы исследования: анализ, синтез, индукция, дедукция, обобщение и классификация.

Опытно-экспериментальной базой исследования стало Управление культуры Администрации г.о. Сызрань.

Научная новизна исследования состоит:

– в оспределении цели обеспечения информационной безопасности в органах местного самоуправления: цель обеспечения информационной безопасности в органах местного самоуправления – защита информационных ресурсов от возможного несанкционированного доступа к ним, которое может привести к нанесению ущерба органам местного самоуправления и их сотрудникам, а также ограничить возможность выполнения своих полномочий;
– разработке авторского проекта внедрения IT – аутсорсинга как инструмента обеспечения информационной безопасности в сфере культуры на муниципальном уровне и оценке его экономической эффективности.

Теоретическая значимость исследования заключается в систематизации имеющейся информации по использованию IT – аутсорсинга в качестве инструмента обеспечения информационной безопасности экономических субъектов.

Практическая значимость исследования состоит в возможности применения разработанного проекта внедрения IT – аутсорсинга как инструмента обеспечения информационной безопасности в сфере культуры на муниципальном уровне.

Достоверность и обоснованность результатов исследования подтверждена теоретической основой исследования, личным участием автора при разработке проекта внедрения IT – аутсорсинга как инструмента обеспечения информационной безопасности Управления культуры Администрации г.о. Сызрань и оценке его эффективности.

Личное участие автора в организации и проведении исследования состоит в разработке проекта внедрения IT – аутсорсинга как инструмента обеспечения информационной безопасности Управления культуры Администрации г.о. Сызрань и оценке его эффективности.

Апробация и внедрение результатов работы велись в течении всего исследования.

На защиту выносятся:

- уточненная цель обеспечения информационной безопасности в органах местного самоуправления, как защита информационных ресурсов от возможного несанкционированного доступа к ним, которое может привести к нанесению ущерба органам местного самоуправления и их сотрудникам, а также ограничить возможность выполнения своих полномочий;
- разработанный авторский проект внедрения IT – аутсорсинга как инструмент обеспечения информационной безопасности в сфере культуры на муниципальном уровне.

Структура магистерской диссертации**.** Работа состоит из введения, трех глав, заключения, содержит 9 рисунков, 12 таблиц, список используемой литературы и используемых источников (37 источников), 3 приложения. Основной текст работы изложен на 73 страницах.

1 Теоретические аспекты использования IT – аутсорсинга в качестве инструмента обеспечения информационной безопасности экономических субъектов

1.1 Понятие и необходимость обеспечения информационной безопасности экономических субъектов

Концепция экономической безопасности «в течении последних лет стала одним из актуальных и динамично развивающихся разделов экономики, экономической науки. Как и в отношении существования и развития любого государства, можно без преувеличения сказать, что, во-первых, во всех сферах человеческой деятельности в какой-то степени содержатся какие-либо индикаторы, которые сигнализируют о возможных рисках и опасностях, которые должны быть приняты при определении и применении целей, выдвигаемых обществом, корпорациями и отдельными лицами. Во-вторых, значение понятия безопасность сейчас усиливается из-за растущего многомерного и альтернативного экономического развития, угроз со стороны других стран. Также и экономический кризис в современной России обострил проблему экономической безопасности» [24].

В последнее десятилетие XX века «в российской экономической литературе произошло заметное оживление дискуссии по вопросам национальной экономической безопасности. Понятие «экономическая безопасность» появилось не так давно, оно упоминается как в политических спорах, так и в нормативных документах. Экономическая безопасность - это такое состояние экономики, при котором обеспечивается устойчивый экономический рост, эффективное удовлетворение общественных потребностей, высокое качество управления, защита экономических интересов на национальном и международном уровнях» [7].

Закон Российской Федерации «О безопасности» определяет экономическую безопасность России как «защиту жизненно важных

интересов всех жителей её страны, российского общества в целом и государства в экономической сфере от внутренних и внешних угроз со стороны других государств. Гарантии экономической безопасности являются необходимым условием для обеспечения стабильного развития национальной экономики» [19].

Концепция экономической безопасности России « представляет собой комплекс положений, направленных на поддержание стабильности и роста экономических показателей, необходимых для обеспечения нормальной жизнедеятельности граждан и сохранения надёжного статуса государства на международном рынке. Поддержание экономической устойчивости напрямую влияет на общую национальную безопасность. Именно поэтому при возникновении политических конфликтов первый удар всегда приходится по экономике» [31].

Стратегия экономической безопасности России до 2030 года является документом, который приказал утвердить президент РФ Владимир Путин в 2017 году. В ней «содержатся главные цели и задачи экономической политики, направленные на поддержание финансовой безопасности. Реализация стратегии должна полностью наладить обстановку в стране и на мировом рынке, несмотря на сложные международные отношения с некоторыми государствами» [28].

Управление ресурсами предприятия «представляет собой организацию всех составляющих, на которых держится фирма. В первую очередь, это экономическая сторона дела. Грамотное управление финансами — залог того, что компания просуществует долгое время. Из-за неправильного управления предприятие может влезть в долги или обанкротиться. Помимо планирования денег нельзя упускать из виду управления персоналом, материальной базой, информационными ресурсами. Если использовать специальные программы, облегчающие управление бизнесом, можно получить максимальную выгоду и производительность от организации.

Для обеспечения безопасности ресурсов предприятия средства защиты информации обычно размещаются непосредственно в корпоративной сети. Межсетевые экраны контролируют доступ к корпоративным ресурсам, отражая атаки злоумышленников извне, а шлюзы виртуальных частных сетей обеспечива ют конфиденциальную передачу информации через открытые глобальные сети, в частности» [32].

Защита информации – это комплекс правовых, организационных и технических мероприятий по предотвращению угроз информационной безопасности и устранению их последствий при сборе, хранении, обработке и передаче информации в информационных системах.

Основные «виды защиты информации:

– защита информации от утечек характеризуется мероприятиями, направленными на сохранность конфиденциальных данных, которые используются на предприятии;
– защита информации от разглашения может производиться посредством мер, которые направлены на недопущение умышленных действий или действий по неосторожности сотрудников или иных лиц, оглашающих конфиденциальные сведения;
– защита информации от несанкционированного доступа может проводиться с помощью мер, устанавливающих запрет к доступу компьютерной сети» [15].

Информационная безопасность предприятия связана с обеспечением необходимого уровня защиты информации. Поэтому информационная безопасность должна контролироваться, должны разрабатываться меры по управлению рисками, формироваться стандарты по управлению защитой информации. В процессе обеспечения информационной безопасности следует уделять внимание формальным методам защиты информации. В основе заложена стандартизация. Ее цель направлена на доверие, реализацию мер по защите данных от вероятных рисков, снижение угроз.

С учетом изложенного выделяют «три уровня формирования режима информационной безопасности:

– законодательно-правовой;

– административный;

– программно-технический.

Законодательно-правовой уровень представляется комплексом законодательных актов, устанавливающих правовой статус субъектов информационных отношений, субъектов и объектов защиты, их правовой статус. Административный уровень включает комплекс взаимокоординируемых мероприятий и технических мер, которые реализуют практические механизмы защиты в ходе формирования и эксплуатации систем защиты информации. Данный уровень охватывает все структурные элементы систем обработки данных

Программно-технический уровень включает три подуровня: физический, технический и программный. Физический подуровень решает задачи с ограничением физического доступа к информации и информационным системам. Средства защиты технического и программного подуровней непосредственно связаны с системой обработки информации. Эти средства либо встроены в аппаратные средства обработки, либо сопряжены с ними по стандартному интерфейсу. К техническим средствам относятся схемы контроля информации по четности, схемы доступа по ключу и так далее. К программным средствам защиты относится программное обеспечение, которое используется для защиты информации. Формирование режима информационной безопасности является сложной системной задачей, которую должны решать все современные организации» [13].

Немаловажную роль в формировании системы экономической безопасности играет профессиональный опыт руководителя службы экономической безопасности и уровень технической оснащенности предприятия. Однако основная сложность построения системы

экономической безопасности заключается в ее зависимости от человеческого фактора. Сложно достичь желаемого результата, если работники не осознают значимости и потребности мероприятий для поддержания экономической безопасности.

Особенностью и одновременно сложностью системы экономической безопасности является ее зависимость от человеческого фактора. Даже при компетентном руководителе службы безопасности успеха предприятие может добиться тогда, когда каждый сотрудник осознаёт значимость и потребность во внедряемых мерах экономической безопасности.

Следует понимать, кто является субъектами и объектами кадровой безопасности организации. К субъектам относятся:

- служба управления персоналом;
- служба безопасности предприятия. Стоит отметить, что служба управления персоналом играет значимую роль, так как непосредственно участвует в формировании кадров и взаимодействует с каждым сотрудником лично и индивидуально. Именно минимизацией негативных действий со стороны персонала занимается служба управления персоналом, поэтому она должна обладать строгими полномочиями для качественного осуществления своих действий.

Служба управления персоналом должна работать взаимосвязанно:

- с финансовыми отделами;
- юридическими отделами;
- профсоюзными организациями.

К объектам кадровой безопасности относятся внутренние риски и угрозы предприятия. Риск-менеджмент позволяет выявить основные шаги для анализа рисков:

- определение рисков и угроз, вызванных действиями персонала.
- анализ выявленных факторов.
- определение общего уровня всех рисков организации.

– оценка финансовой стороны рисков.

Полученные результаты должны быть применены для формирования стратегий, способов и мер обеспечения кадровой безопасности предприятия. Работая со всеми вышеуказанными методами и способами, можно добиться высоких результатов в обеспечении безопасности. В настоящее время в период высокой и острой конкуренции действительно следует уделять большое внимание обеспечению кадровой безопасности. При необходимости выделять средства и нужные ресурсы, нанимать квалифицированный персонал и работать на улучшение рабочего климата внутри коллектива. Ведь вред, нанесенный сотрудниками, имеющими доступ к конфиденциальной и закрытой информации, может нанести серьезный ущерб предприятию.

Мониторинг экономической безопасности - это система сбора, анализа, оценки и прогнозирования сведений, характеризующих уровень безопасности организации.

Организации «создают, собирают и хранят огромные объемы информации от клиентов и партнеров: поведенческую аналитику, личную информацию, данные о кредитных картах и платежах и другое. Увеличение объема корпоративных данных приводит к росту кибератак и количеству утечек. В качестве контрмеры стремительно развивается область управления информационной безопасностью» [5].

Каждый «бизнес-процесс, основанный на технологиях, подвержен угрозам безопасности. Сложные решения для кибербезопасности способны противостоять атакам, угрозам и новым методам хакеров, но этого недостаточно. Организации должны гарантировать, что процессы, политики и сотрудники минимизируют риски» [7].

Здесь «на помощь приходят системы управления информационной безопасностью. Независимо от метода хранения данных (в цифровом или физическом формате), управление информационной безопасностью имеет

решающее значение для защиты данных от несанкционированного доступа и кражи. Оно:

- описывает набор политик и процедурных средств контроля, которые внедряются для защиты корпоративных активов от рисков и угроз;
- включает изучение рисков, обеспечение соответствия, консультационные услуги по безопасности и управлению» [2].

Именно поэтому в целях защиты информации, размещенной в информационной системе общего пользования должна быть обеспечена разработка мер при ее проектировании и эксплуатации, направленных на выполнение требований к безопасности этой информационной системы общего пользования.

На основании проведенного исследования можно сделать вывод, на все исследуемые объекты уделяют важное значение обеспечению информационной безопастности.

Цель обеспечения информационной безопасности в органах местного самоуправления – защита информационных ресурсов от возможного несанкционированного доступа к ним, которое может привести к нанесению ущерба органам местного самоуправления и их сотрудникам, а также ограничить возможность выполнения своих полномочий.

1.2 Понятие и отличительные особенности аутсорсинга

Термин «аутсорсинг» в переводе с английского означает «использование внешних ресурсов» [13].

Овакимян Г. С определяет аутсорсинг как «перевод внутреннего подразделения или подразделений предприятий и всех связанных с ним активов в организацию поставщика услуг, который предлагает предоставить определенную услугу в течение определенного времени по оговоренной цене» [23].

Джобава Р.Г. полагает, что аутсорсинг представляет собой «один из десяти наиболее существенных факторов, определяющих характер развития мировой экономики на современном этапе» [6].

Луцкая Н.В. аутсорсингом подразумевает «использование материальных средств, имущества и знаний третьего лица с гарантированным уровнем качества, гибкости и ценности стоимостных критериев и оценок для предоставления услуг, которые ранее предоставлялись за счет внутренних сил компании, с возможным переходом 10 имеющегося персонала поставщика услуг и (или) трансформацией (обновлением) процессов или технологий, поддерживающих бизнес» [16].

Попов И.С. и Березин В.В. дают следующее определение - «аутсорсинг это передача организацией определенных бизнес-процессов или производственных функций на обслуживание другой компании, специализирующейся в соответствующей области» [25].

Райзберг Б. А., ЛозовскоийЛ. Ш., Стародубцева Е. Б. считают, что «аутсорсинг — это передача традиционных не ключевых функций организации (таких как бухгалтерский учет или рекламная деятельность для машиностроительной компании) внешними исполнителями — высококвалифицированным специалистам сторонней фирмы, субподрядчикам, аутсорсерами» [26].

Гильмиярова М.Р. отмечает, что «аутсорсинг — это комплексное понятие и стратегическое коммерческое решение, направленное на целенаправленную реструктуризацию предприятия с передачей отдельных функций, бизнес-процессов и, соответственно, полномочий, ответственности и рисков внешним компетентным исполнителям на договорных началах» [4].

Райзберг Б. А., ЛозовскоийЛ. Ш., Стародубцева Е. Б. также добавляют, что «аутсорсинг в виде отказа компании от самостоятельного выполнения ряда некритических для бизнеса функций или части бизнес-процессов и передачи их стороннему подрядчику» [26].

А.Н. Кириллова предлагает использовать несколько транктовок данного понятия:

- «аутсорсинг - это приобретение существенного количества промежуточных компонентов у внешних поставщиков;
- аутсорсинг - это осуществление сторонней организацией производственной деятельности, которая ранее выполнялась внутри фирмызаказчика;
- аутсорсинг - перевод внутреннего подразделения или подразделений редприятия и всех связанных с ними активов в организацию поставщика услуг, предлагающего оказывать некую услугу в течение определенного времени по оговоренной цене» [11].

Таким образом, в данной работе под аутсорсингом будет подразумеваться процесс передачи части непрофильных функций организации сторонним организациям на договорной основе.

Аутсорсинг « насчитывает глубокую историю:

- первый этап и истоки применения аутсорсинга начались еще в 30-е гг. XX века, в период столкновения одних из самых величайших менеджеров – Генри Форда и Альфреда Слоуна. Уже в этот период отрасль автомобилестроения показала, что справиться с серьезной конкуренцией, опираясь на внутренние ресурсы компаний невозможно. Эффективнее передавать часть процессов компании на аутсорсинг. Значимость принятия решения о переводе на аутсорсинг некоторых функций можно заметить и сейчас, так как эти две компании являются мировыми гигантами. Тем не менее, в ту пору такое решение не было замечено и оценено другими компаниями. Фактическое активное применение аутсорсинга началось лишь в 80-90 гг. XX века;
- на втором этапе активно начинает развиваться передача производственных функций и информационных технологий на аутсорсинг. Примерами компаний, передавшими производство на

аутсорсинг в тот период, могут служить: Ford – производство автомобилей и Mattel – фирма, производящая куклы Barbie. Аутсорсинг информационных технологий в 80- 90е гг. можно изучить на примере такой компании, как Kodak, которая передала свой центр обработки данных аутсорсинговым фирмам IBM Digital Equipment Corp и другим;

– третий этап характеризуется активным развитием передачи на аутсорсинг различных функций, помимо производственных и IT., таких как бухгалтерский учет, принятие на работу персонала, маркетинговые исследования, обработка первичной информации и так далее» [18].

Наиболее распространенным видом аутсорсинга в настоящее время является «аутсорсинг знаний, предполагающий передачу на аутсорсинг процессов, требующих серьезного анализа, изучения и глубокой аналитической обработки данных. К таким процессам относят: работу с результатами интеллектуальной собственности, получение патентов, оказание юридических и медицинских услуг, проведение обучения, консультирования и исследований» [22].

В современной литературе отмечается, что «традиционный тип управления с вертикально интегрированными транснациональными корпорациями уходит в прошлое, лидирующую роль уже десятилетие занимают международные горизонтальные сетевые структуры. Главенствующую роль в таких структурах занимает технология аутсорсинга. Применение аутсорсинга в таких компаниях приводит к удвоению прибыли в связи с сокращением организационных и производственных издержек, повышению эффективности функционирования компаний. Впечатляющих результатов с помощью перехода на аутсорсинг добились такие компании, как Ford, British Petroleum, Procter&Gamble, Dell, Exel и другие» [21].

В настоящее время можно выделить следующие «преимущества аутсорсинга:

– упрощение системы управления персоналом. (Нет необходимости начислять заработную плату, выплачивать премии и осуществлять другие стимулирующие выплаты (все это производит агентство));
– сокращение временных затрат на поиск новых работников (достаточно обратиться в агентство, предоставляющее услугу);
– упрощение системы налогообложения и страхования;
– уменьшение степени риска при найме сотрудника (всю ответственность несет исполнитель);
– возможность нанять квалифицированный персонал на срочные и кратковременные проекты;
– минимизация издержек на освоение и развитие новой территории (открытие нового обособленного структурного подразделения);
– повышение инвестиционной привлекательности организации» [17].

Однако, актсорсинг имеет и «ряд недостатков:

– несвоевременное предоставление или не предоставление заказчику необходимых работников;
– несоответствие работников, заявленным требованиям;
– невыплата или выплата не в полной мере сотрудникам заработной платы, премий, что может способствовать формированию негативного мнения и об организации, в которой непосредственно трудились данные работники» [14].

Таким образом, «развитие аутсорсинга в зарубежных странах уже преодолело в своей истории несколько этапов, компании-мировые лидеры передают свои услуги на аутсорсинг и получают от этого прибыль. В Российской Федерации таких примеров пока нет, и для внедрения аутсорсинга своих бизнес-процессов необходимо проводить глубокий анализ. Несмотря на то, что авторы многих исследований отмечают существенный рост числа аутсорсинговых услуг и обращения к ним. Некоторые их них устанавливают, что:

– лишь 1/3 всех компаний, обратившихся к аутсорсингу, действительно достигают цели;
– более 50% компаний каждый год меняют компаний-аутсорсеров или условия их сотрудничества;
– более 20% компаний не удовлетворено результатами аутсорсинга;
– более половины поставщиков услуг не заинтересованы в повышении качества конкурентоспособности продукта» [20].

В нашей стране в настоящее время «аутсорсинг развит недостаточно. Первыми, кто стал предоставлять такие услуги стали частные охранные предприятия (ЧОП). Основная идея передачи охраны фирм на аутсорсинг заключалась в том, что качественнее и профессиональнее можно защитить свою компанию воспользовавшись услугами специально подготовленных кадров, отобранных и обученных для этой работы, а не несколькими штатными охранниками. Следующими, кто стал осваивать эту отрасль стали рекламные агентства. Отсутствие специалистов по рекламе и невозможность каждой компании в связи с этим нанять их в штат, позволило образовать специализированные рекламных предприятия, способные выполнять сложнейшие проекты качественно» [1].

1.3 Особенности аутсорсинга процессов информационной безопасности

В связи «с постоянным усложнением информационных систем компаний и ростом потребности в них, найти квалифицированный ИТ-персонал становится всё сложнее, да и сам персонал постоянно дорожает. Для разрешения этой проблемы всё больше российских компаний начинают пользоваться услугами ИТ-аутсорсинга, следуя примеру Европейских компаний, где затраты на ИТ-аутсорсинг составляют в среднем более 50 % ИТ-бюджета» [3].

Использование ИТ-аутсорсинга «позволяет компаниям отказаться от непрофильных активов и сконцентрироваться на основном направлении

своего бизнеса» [9]. Но при передаче компонентов информационной системы (ИС) на аутсорсинг «очень острой становится проблема обеспечения её информационной безопасности» [12].

При «передаче компонентов ИС на аутсорсинг возникают следующие новые условия окружения :

- расширяется круг лиц, допущенных к работе с ИС;
- более активное использование внешних каналов связи;
- неизвестная исходная защищенность инфраструктуры аутсорсера;
- неизвестный круг третьих лиц, получающих доступ к инфраструктуре и системе, включая физический уровень;
- отсутствие контроля над регламентами и их исполнением на стороне провайдера;
- инсайдерская деятельность;
- отсутствие оперативной обратной связи и информирования по инцидентам ИБ на стороне аутсорсера» [34].

Аутсорсер «получает доступ ко всем компонентам ИС. Оценки рисков ИС при передаче на аутсорсинг будут ассоциированы с компонентами ИС» [27] (таблица 1).

Таблица 1 - Компоненты и методы оценки рисков

Компонент ИС	Методы оценки риска
Аппаратное обеспечение	«Инвентаризация аппаратного обеспечениядо, в процессе и после аутсорсинга с возможностью контроля изменений» [29]
Программное обеспечение (в том числе прикладное)	«Инвентаризация и мониторинг программного обеспечения до, в процессе и после аутсорсинга с возможностьюконтроля изменений» [29]
Конфигурационные файлы	«Резервное копирование конфигурационных файлов на внешний носитель и восстановление с него» [29]
Базы данных	«Резервное копирование баз данных на внешний носитель и восстановление с него» [29]
Другая информация, не держащаяся в базах данных лектронные документы, изображения и т.д.)	«Резервное копирование другой информациина внешний носитель и восстановление с него» [29]

Услуги аутсорсинга, ассоциированные с угрозами для информационной сисемы, с добавлением компонент ИС, приведены в таблице 2 [36].

Таблица 2 - Угрозы для информационной системы и ее компонент, связанные с услугами аутсорсинга

Услуга аутсорсинга	Компонент ИС	Угроза
Поддержка пользователей	«Аппаратное обеспечение, программное обеспечение, конфигурационные файлы, базы данных, другая Информация» [29]	«Доступ к конфиденциальной информации на рабочих станциях пользователей в результатепередачи на аутсорсинг» [29]
Управление вспомогательными активами	«Аппаратное обеспечение, программное обеспечение» [29]	«Воздействие на вспомогательныеактивы в результате передачи на аутсорсинг» [29]
		«Нарушение качества сервиса в результате передачи на аутсорсинг» [29]
Поддержка непрерывности бизнеса	«Аппаратное обеспечение, программное обеспечение, базы данных, конфигурационные файлы» [29]	«Угрозы природного и техногенного характера затрагивающие аутсорсера» [29]
Управление сетями	«Аппаратное обеспечение, конфигурационные файлы, другая информация» [29]	«Несанкционированное сетевое взаимодействие в результате передачи на аутсорсинг» [29]
Управление безопасностью	«Аппаратное обеспечение, программное обеспечение, конфигурационные файлы, другая информация, базы данных» [29]	«Данные об инцидентах ИБ под контролем Исполнителя, а не Заказчика» [29]
Поддержка приложений	Программное обеспечение, конфигурационные файлы, другая информация	«Доступ к конфиденциальной информации, содержащейся в бизнес-приложениях в результате передачи на аутсорсинг» [29]
Хостинг приложений	«Программное обеспечение, конфигурационные файлы, другая информация, базы данных» [29]	№Нарушение необходимого качества сервиса в связи с удаленностью инфраструктуры в результате передачи на аутсорсинг»

На основании данных таблицы строится дерево угроз информационной системе при ее аутсорсинге [35]. На рисунке 1 приведено дерево угроз для типовой ИС.

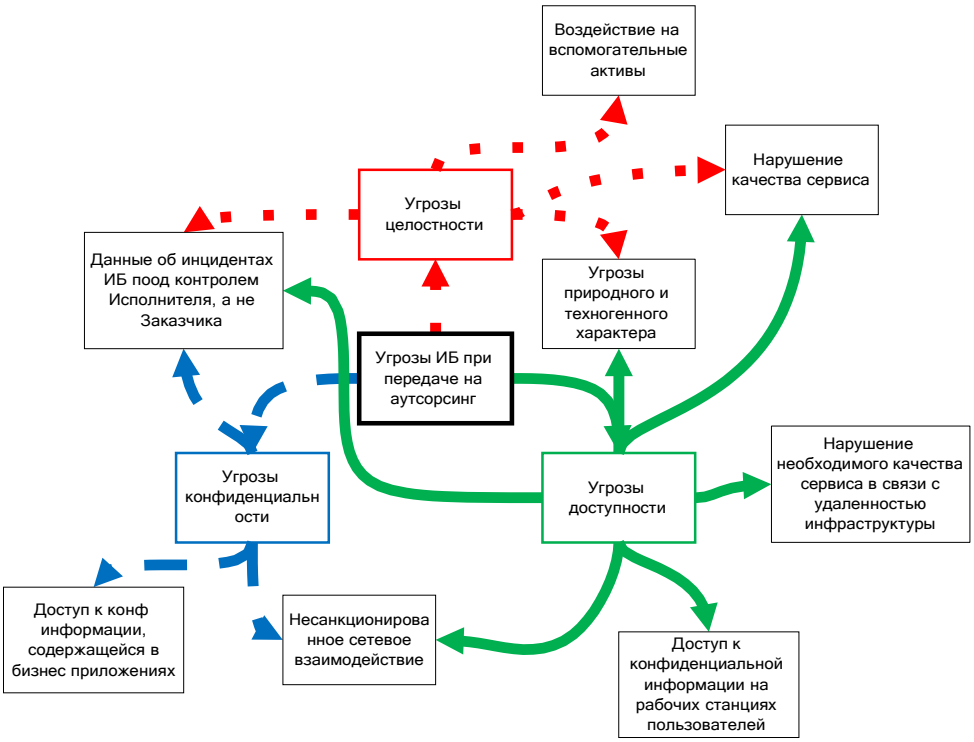

Рисунок 1 - Дерево угроз для типовой информационной системы при передаче ее на аутсорсинг [33]

Анализ дерева угроз информационной безопасности показывает, что «актуальными являются угрозы на все три свойства информации: доступность, целостность и конфиденциальность.

В связи с этим актуальным является вопрос разработки системы оценки информационной безопасности ИС в процессе и после аутсорсинга» [8].

Современными исследователями предлагается «модель информационной системы с позиции информационной безопасности, которая фиксирует основные угрозы ресурсам ИС: доступ к конфиденциальной информации на рабочих станциях пользователей, злоумышленное воздействие на вспомогательные активы, нарушение качества сервиса,

угрозы природного и техногенного характера, несанкционированное сетевое взаимодействие, доступ к данным об инцидентах ИБ под контролем аутсорсера, а не заказчика, доступ аутсорсера к конфиденциальной информации, содержащейся в бизнес-приложениях, нарушение необходимого качества сервиса в связи с удаленностью инфраструктуры. На основе модели и дерева угроз рассчитывается остаточный риск для ИС» [29].

Для «обеспечения безопасности ИС при передаче ее на аутсорсинг необходимо провести работы по минимизации рисков. Предлагается включить в эти работы: подготовку ИС к передаче на аутсорсинг, оценку уровня информационной безопасности в процессе и после аутсорсинга, а в случае его снижения уровня провести работы по восстановлению» [10].

Подготовка ИС к передаче на аутсорсинг включает «работы по защите: баз данных путем их шифрования и резервного копирования; от несанкционированной модификации файлов конфигурации и программного обеспечения ИС путем расчета контрольных сумм и их сохранения на в базе данных на отдельном носителе или рабочем месте; от несанкционированной модификации аппаратных средств ИС путем их инвентаризации и сохранения в базе данных; расчета остаточного риска для ИС и сохранения его значения в базе данных. Оценка уровня информационной безопасности в процессе аутсорсинга предполагает периодическое представление заказчику возможности проведение мониторинга состояния базы данных и ИС в целом, инвентаризации программного, аппаратного обеспечения ИС и расчет остаточного риска. Оценка уровня информационной безопасности после аутсорсинга аналогична оценке в процессе аутсорсинга. Для автоматизации процесса минимизации рисков разработаны модель, алгоритмы и программный комплекс на языке C#, который включает следующие модули: пользовательский интерфейс, агентов инвентаризации, мониторинга и аудита программного и аппаратного обеспечения, агент базы данных, агент резервного копирования, агент файлов конфигурации, агент расчета остаточного риска и ряд вспомогательных агентов» [30] .

Таким образом, в целях защиты информации, размещенной в информационной системе общего пользования должна быть обеспечена разработка мер при ее проектировании и эксплуатации, направленных на выполнение требований к безопасности этой информационной системы общего пользования.

На основании проведенного исследования можно сделать вывод, на все исследуемые объекты уделяют важное значение обеспечению информационной безопастности.

Цель обеспечения информационной безопасности в органах местного самоуправления – защита информационных ресурсов от возможного несанкционированного доступа к ним, которое может привести к нанесению ущерба органам местного самоуправления и их сотрудникам, а также ограничить возможность выполнения своих полномочий.

2 Исследование особенностей обеспечения информационной безопасности экономических субъектов

2.1 Технико-экономическая характеристика деятельности организаций

Объекты исследования: Управление культуры Администрации г.о. Сызрань, Департамент культуры Администрации г.о. Тольятти, Департамент культуры и молодежной политики Администрации г.о. Самара.

Первый объект - Управление культуры Администрации городского округа Сызрань (далее Управление) является органом Администрации городского округа Сызрань с правами юридического лица, созданного в форме муниципального казенного учреждения для исполнения организационно-управленческих функций.

Управление культуры Администрации городского округа Сызрань создано на основании Постановления Администрации города Сызрани от 21.05.1997 года №525.

Организационно правовая форма Управления- Муниципальное казенное учреждение.

В своей деятельности Управление руководствуется Конституцией Российской Федерации, федеральными конституционными законами, федеральными законами, указами и распоряжениями Президента Российской Федерации, постановлениями и распоряжениями Правительства Российской Федерации, правовыми актами Самарской области и нормативными правовыми актами органов местного самоуправления, Уставом городского округа Сызрань, а также настоящим Положением.

Местонахождение Управления: 446001, Самарская область, городской округ Сызрань, г. Сызрань, ул. Советская, 92.

Основными целями деятельности Управления являются:

– обеспечение гражданам, проживающим на территории городского округа Сызрань, возможности выбора услуг в области культуры.
– создание условий для:
  – организации досуга и обеспечения жителей городского округа Сызрань услугами организаций культуры;
  – развития местного традиционного народного художественного творчества;
  – художественного и эстетического воспитания подросткового поколения;
  – массового отдыха жителей городского округа Сызрань, в т.ч. отдыха
  детей во время каникул.
– осуществление структурно-содержательных изменений в отраслях социально-культурной сферы с целью приведения в соответствие потребностей общества в услугах культуры и ее предложений.

Структура Управления Культуры Администрации г.о. Сызрань представлена на рисунке 2.

Рисунок 2 – Структура Управления Культуры Администрации г.о. Сызрань

В сфере культуры продолжилась деятельность по расширению спектра предоставляемых населению услуг, повышению их качества и доступности для жителей и гостей городского округа, а также по развитию и реализации культурного и духовного потенциала граждан, творческой активности населения.

Деятельность учреждений культуры городского округа Сызрань в части расходования бюджетных средств осуществлялась с применением программно-целевого метода. На реализацию мероприятий ведомственной целевой программы городского округа Сызрань «Обеспечение организации деятельности муниципальных учреждений в сфере культуры и искусства городского округа Сызрань на 2020-2024 годы» в отчетном году из всех уровней бюджета направлено 455 482,9 тыс. рублей.

В Приложениях А, В и Б представлены отчеты об исполнении бюджета Управления культуры Администрации г.о. Сызрань за 2019, 2020 и 2021 год соответственно.

Основные технико-экономические показатели Управления Культуры Администрации г.о. Сызрань за 2019-2021 гг. представлены в таблице 3.

Таблица 3 - Основные технико-экономические показатели Управления Культуры Администрации г.о. Сызрань за 2019-2021 гг.

Статья	2019 год	2020 год	2021 год	Отклонения 2021/2019	
				(+/-)	%
Доходы	319,4	308,6	328,4	9,0	2,8
Расходы	306,8	322,8	334,7	27,9	9,1
Дефицит/профицит	13	-14	-6	-19	15,0

На основании представленных данных можно сделать вывод, что за исследуемый период 2019-2021 гг. происходит увеличение как доходов, так и расходов Управления Культуры Администрации г.о. Сызрань (увеличение доходов составило 2,8%, расходов – 9,1%). При опережении роста расходов над доходами отмечается увеличение дефицита бюджета (на 15%).

Следующий объект исследования - Департамент культуры Администрации г.о. Тольятти.

Основной целью деятельности департамента является реализация государственной и муниципальной культурной политики на территории городского округа Тольятти, создание условий доступности, сохранение и развитие культуры и искусства на территории городского округа Тольятти, направленных на повышение культурного уровня населения городского округа Тольятти.

В структуру департамента Администрации г.о. Тольятти входят следующие структурные подразделения:

– отдел развития отрасли культуры;
– финансово-экономический отдел;
– управление образования, культуры и искусства (рисунок 3).

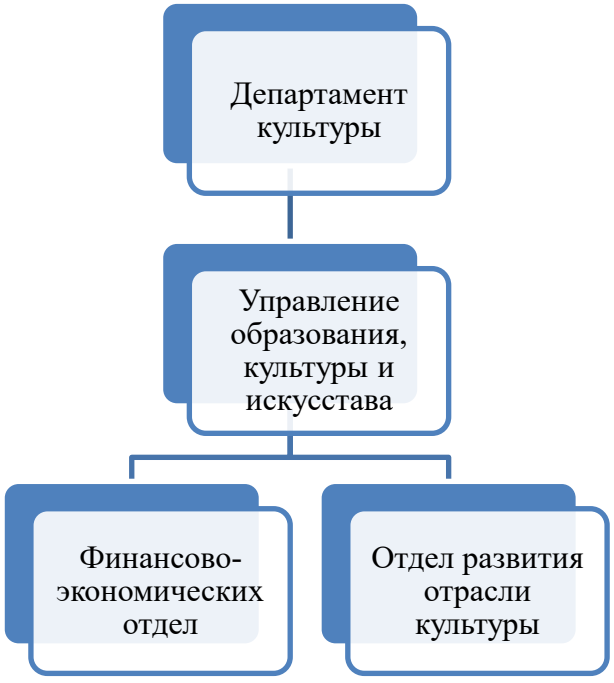

Рисунок 3 – Структура департамента культуры администрации г.о. Тольятти.

В настоящее время на территории г.о. Тольятти действует муниципальная программа «Культура Тольятти на 2019-2023 годы» - НП

«Культура» (ФП «Культурная среда», ФП «Творческие люди»), которая утвержденная постановлением администрации городского округа Тольятти от 21.09.2018 № 2799-п/1.

Целью муниципальной программы является повышение стратегической роли культуры в создании благоприятных условий для поддержки творческих инициатив, досуговой и образовательной деятельности, сохранения исторического наследия и развития культурной среды в городском округе Тольятти.

Эффективность реализации программы за 2021 год составила 99,8 % - эффективная реализация.

Основные технико-экономические показатели Департамента кульуры Администрации г.о. Тольятти за 2019-2021 гг. представлены в таблице 4.

Таблица 4 - Основные технико-экономические показатели Департамента кульуры Администрации г.о. Тольятти за 2019-2021 гг.

Статья	2019 год	2020 год	2021 год	Отклонения 2021/2019	
				(+/-)	%
Доходы	954 258	976 000	986 014	31 756	3,3
Расходы	968 214	945 471	1 038 020	69 806	7,2
Дефицит/профицит	-13 956	30 529	-52 006	-38 050	-27,3

На основании представленных данных можно сделать вывод, что за исследуемый период 2019-2021 гг. происходит увеличение как доходов, так и расходов Департамента культуры Администрации г.о. Тольятти (увеличение доходов составило 3,3%, расходов – 7,2%). При опережении роста расходов над доходами отмечается значительное увеличение дефицита бюджета (на 27,3%).

Третий объект исследования - Департамент культуры и молодежной политики Администрации г.о. Самара.

Департамент культуры и молодежной политики Администрации городского округа Самара является отраслевым (функциональным) органом Администрации городского округа Самара, осуществляющим на территории городского округа Самара единую политику в пределах имеющихся полномочий в сфере культуры и молодежной политики.

В своей деятельности Департамент руководствуется законодательством Российской Федерации, законодательством Самарской области, Уставом городского округа Самара, иными муниципальными правовыми актами городского округа Самара, а также Положением «О Департаменте культуры и молодежной политики Администрации городского округа Самара», утвержденным Решением Думы городского округа Самара от 25.07.2013 № 347.

Основными задачами Департамента являются:

- определение приоритетных направлений развития культуры, искусства и молодежной политики на территории городского округа Самара;
- осуществление единой политики городского округа Самара в области культуры, искусства и молодежной политики;
- совершенствование форм и методов работы организаций культуры и молодежных объединений, расположенных на территории городского округа Самара;
- содействие развитию на территории городского округа Самара сферы досуга и молодежной политики;
- обеспечение разнообразия культурно-досуговой деятельности на территории городского округа Самара;
- развитие и координация связей между научными организациями и учебными заведениями, осуществление научно-методической работы в сфере культуры и молодежной политики на территории городского округа Самара;

– проведение активной маркетинговой, информационной и рекламной политики, направленной на формирование и поддержку позитивного имиджа городского округа Самара в сфере деятельности Департамента.

Структура Департамента культуры и молодежной политики Администрации городского округа Самара представлена на рисунке 4.

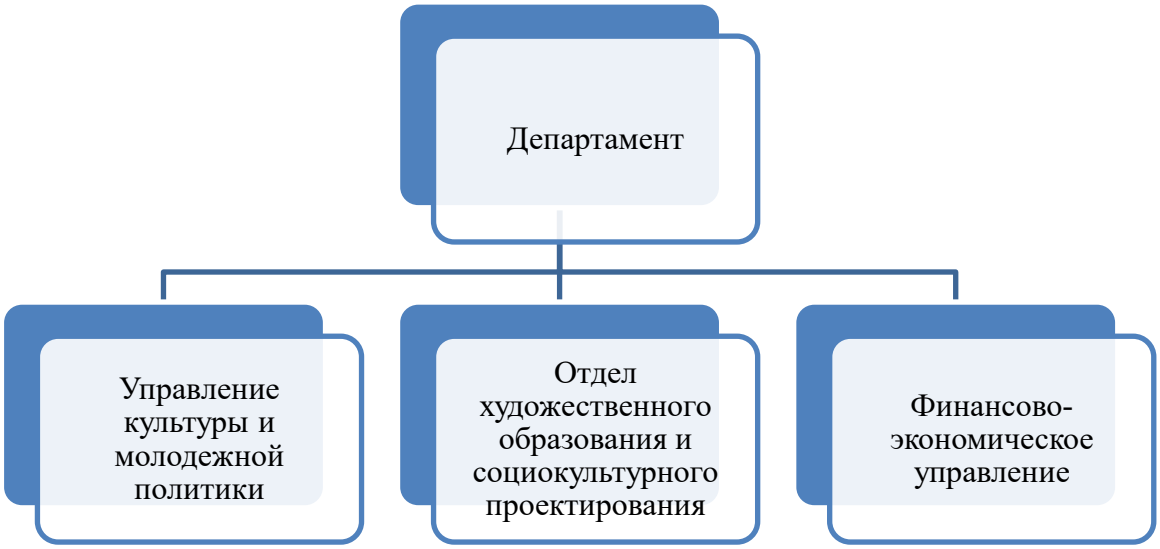

Рисунок 4 - Структура Департамента культуры и молодежной политики Администрации г.о. Самара

В сфере культуры Департаментом культуры и молодежной политики Администрации городского округа Самара реализуеются муниципальная программа городского округа Самара «Развитие культуры городского округа Самара» на 2018-2022 годы.

Цель Программы: повышение качества и доступности услуг в сфере культуры на территории городского округа Самара.

Основные технико-экономические показатели Департамента культуры и молодежной политики Администрации г.о. Самара за 2019-2021 гг. представлены в таблице 5.

Таблица 5- Основные технико-экономические показатели Департамента культуры и молодежной политики Администрации г.о. Самара за 2019-2021 гг.

Статья	2019 год	2020 год	2021 год	Отклонения 2021/2019	
				(+/-)	%
Доходы	986,4	854,2	997,3	10,9	1,1
Расходы	976,4	875,8	1 005	28,3	2,9
Дефицит/профицит	10,0	-21,6	-7,4	-17,4	17,4

На основании представленных данных можно сделать вывод, что за исследуемый период 2019-2021 гг. происходит увеличение как доходов, так и расходов Департамента культуры и молодежной политики Администрации г.о. Самара (увеличение ходохов составило 1,1%, расходов – 2,9%). При опережении роста расходов над доходами отмечается увеличение дефицита бюджета (на 17,4%).

2.2 Механизм обеспечения информационной безопасности экономических субъектов

В данном разделе исследуем механизм обеспечения информационной безопасности экономических субъектов.

Первый объект - Управление культуры Администрации г.о. Сызрань.

Обеспечением информационной безопасности Управления культуры Администрации г.о. Сызрань занимается Управление по организационной работе и информационным технологиям администрации г.о. Сызрань.

Основными задачами и функциями Управления по организационной работе и информационным технологиям администрации г.о. Сызрань являются:

– формирование и реализация политики Администрации городского округа Сызрань в области информационных и коммуникационных ресурсов и технологий, развитие телекоммуникаций и связи, координация и осуществление контроля выполнения мероприятий

информационно-телекоммуникационных технологий в Администрации;

- организация и обеспечение функционирования единой системы делопроизводства и документооборота в Администрации городского округа Сызрань; совершенствование форм и методов делопроизводства на основе применения современной электронно-вычислительной техники и программного обеспечения; методическое руководство работой по организации делопроизводства в Администрации городского округа Сызрань; контроль сроков исполнения запросов;
- организация и контроль работы по созданию и развитию автоматизированных информационных систем в Администрации городского округа Сызрань.

Средства и способы защиты информации

Антивирусная защита

Автоматизированные рабочие места и информационные системы и ресурсы Управления культуры Администрации г.о. Сызрань оборудованы сертифицированными средствами антивирусной защиты с периодичностью обновления, установленной регламентирующими документами администрации г.о. Сызрань.

В случае обнаружения вирусов и вредоносного кода сотрудники Управления культуры Администрации г.о. Сызрань обязаны незамедлительно прекратить использование автоматизированного рабочего места до момента полного удаления вирусов и вредоносного кода. При получении электронного письма, вызывающего подозрение пользователя на его содержание и вложения, необходимо удалить его не переходя по ссылкам и не открывая вложенные файлы.

Парольная защита и идентификация пользователя

В информационных системах Управления культуры Администрации г.о. Сызрань используются только персонифицированные учетные записи

пользователей, в том числе администраторов. Для идентификации пользователей в операционных системах, программном обеспечении и почтовых клиентах используются «сложные» логины и пароли, состоящие из заглавных и прописных букв, цифр и специальных символов длинной не менее 8-ми символов. Не рекомендуется в качестве паролей использовать имена близких лиц, домашних животных, даты рождения и т.п., которые могут быть легко подобраны злоумышленниками. Сотрудники Управления культуры Администрации г.о. Сызрань обязаны проводить регулярную смену паролей и не сохранять пароли в текстовых файлах на автоматизированном рабочем месте, либо иных электронных носителях, Не передавать пароли, коды доступа к техническим средствам и системам, для исключения использования учетной записи другим лицом, в случае отсутствия пользователя на рабочем месте (отпуск, временная нетрудоспособность и т.п.).

При отсутствии пользователя информационной системы на рабочем месте по причине отпуска, временной нетрудоспособности, увольнения необходимо производить блокировку учетной записи.

Удаленный доступ

Удаленный доступ в Управлении культуры Администрации г.о. Сызрань подразумевает исключение использования средств удаленного администрирования на технических средствах и системах. В случаях удаленной технической поддержки необходимо использовать программные и технические средства, имеющие сертификат соответствия в зависимости от уровня обрабатываемой информации в информационной системе.

Использование лицензионного программного обеспечения и сертифицированных средств защиты информации

Сотрудники Управления культуры Администрации г.о. Сызрань обязаны использовать в работе только лицензионные версии операционных системы, прикладное программное обеспечение и средства защиты информации. Для защиты информационных систем и ресурсов при передаче

информации по каналам связи Управления культуры Администрации г.о. Сызрань применяются сертифицированные средства защиты информации и средства криптографической защиты информации.

Программы

Программы для защиты информации Управления культуры Администрации г.о. Сызрань включают в себя антивирусы, менеджеры паролей, приложения для резервного копирования.

Второй объект - Департамент культуры Администрации г.о. Тольятти.

Обеспечением информационной безопасности Департамента культуры Администрации г.о. Тольятти отвечает Департамент информационных технологий и связи администрации г.о. Тольятти.

Основными целями деятельности Департамента являются:

- формирование и реализация политики администрации в области информационных и коммуникационных ресурсов и технологий;
- развитие телекоммуникаций и связи;
- организация и контроль работы по анализу, созданию, развитию и эффективному использованию автоматизированных и информационных систем в администрации городского округа Тольятти, муниципальных предприятиях и учреждениях.

Средства и способы

Защита информации, обрабатываемой в локальной вычислительной сети Департамента культуры Администрации г.о. Тольятти (далее – ЛВС) реализуется комплексом программно-технических средств и организационных мероприятий, основными из которых являются:

- организация парольной защиты;
- регистрация и учет действий пользователя;
- проведение антивирусного контроля.

Рассмотрим применяемые средства и способы защиты информации более подробно.

Организация парольной защиты

Идентификация и проверка подлинности пользователя ЛВС при входе в систему осуществляется по идентификатору (персональному уникальному имени) и паролю условно-постоянного действия, дополнительно для идентификации пользователей могут применяться идентификаторы типа Рутокен, Touch Memory и др., соответствующие требованиям для управления ими с помощью СЗИ «Secret Net».

Парольная защита устанавливается на:

- запуск программы конфигурации аппаратного обеспечения средств вычислительной техники;
- процесс загрузки операционной системы;
- вход в сетевую операционную систему;
- программу - хранитель экрана;
- доступ к многопользовательским прикладным программным системам и базам данных, содержащих механизмы идентификации и подтверждения подлинности пользователей по значениям паролей.

Программно - техническое обеспечение процесса организации парольной защиты Департамента культуры Администрации г.о. Тольятти осуществляется:

- сертифицированной системой защиты от несанкционированного доступа для защиты процесса загрузки операционной системы, входа в сетевую операционную систему, программы-хранителя экрана;
- штатными средствами программы конфигурации аппаратного обеспечения;
- штатными средствами прикладных программных систем и программ управления базами данных.

Организационное обеспечение процессов генерации, использования, смены и удаления паролей осуществляют администраторы в пределах их компетенции. Пароль на программу конфигурации аппаратного обеспечения устанавливает администратор ЛВС.

Пароли выбираются пользователями ЛВС Департамента культуры Администрации г.о. Тольятти самостоятельно.

Пользователю ЛВС Департамента культуры Администрации г.о. Тольятти запрещается сообщать кому-либо свой личный пароль.

При отсутствии функционала ПО в части установки указанных выше требований к паролям, устанавливаются требования максимально к ним приближенные.

Пользователю ЛВС Департамента культуры Администрации г.о. Тольятти запрещается:

- до идентификации и аутентификации начинать обработку конфиденциальной информации в ЛВС;
- записывать свои пароли в очевидных местах, внутренности ящика стола, на мониторе, на обратной стороне клавиатуры и т.д.;
- хранить пароли в записанном виде на отдельных листах бумаги;
- сообщать свои пароли посторонним лицам;
- произносить свой пароль вслух;
- использовать общие пароли совместно с другими коллегами по работе;
- предпринимать какие-либо действия по получению (раскрытию) паролей других пользователей.

Смена пароля должна проводиться не реже чем 1 раз в 90 календарных дней.

Число совершенных подряд неудачных попыток ввода пароля не должно превышать 10.

В случае отсутствия технической возможности установки пароля пользователем ЛВС самостоятельно, установка пароля производится при участии администраторов.

О случаях компрометации пароля пользователи ЛВС Департамента культуры Администрации г.о. Тольятти обязаны немедленно сообщать администраторам. Администраторы должны незамедлительно принять меры

для предотвращения утечки информации (блокировка учетной записи пользователя АС, просмотр системных журналов, выявление фактов НСД и т.д.).

К событиям, связанным с компрометацией паролей, относятся:

- разглашение паролей пользователями ЛВС или визуальное ознакомление с паролем посторонними лицами;
- регистрация пользователя АС во время его отсутствия;
- утрата устройств идентификации пользователей ЛВС АПК;
- использование устройств идентификации посторонними лицами без контроля со стороны владельца.

По всем фактам компрометации паролей проводится служебное расследование.

Регистрация и учет действий пользователей

Для контроля за действиями пользователей ЛВС осуществляется регистрация событий происходящих на СВТ Администрации и АПК. Программно - техническое обеспечение данного процесса осуществляется подсистемами регистрации и учета (аудита) средств защиты информации, сетевой операционной системы и прикладных программных систем.

Регистрации подлежат события связанные с обеспечением безопасности информации, такие как: вход (выход) пользователя в систему (из системы), изменение полномочий пользователя, запуск (завершение) программ, предназначенных для обработки защищаемой информации, доступ к защищаемым информационным ресурсам, вывод информации на машинные носители информаци, факты попыток несанкционированного доступа.

Регистрация действий пользователей осуществляется в специальных электронных журналах. Копии электронных журналов должны хранится не менее 1 года со дня внесения в них последней записи.

Доступ к электронным журналам Департамента культуры Администрации г.о. Тольятти организован таким образом, чтобы исключить возможность внесения изменений (удаления записей) пользователями ЛВС.

Электронные журналы используются при разборе конфликтных ситуаций, для проверки правильности (корректности) работы программных и технических средств, а также при определении попыток несанкционированного доступа.

При длительном бездействии (неактивности) пользователя ЛВС производится блокирование в информационной системе сеанса работы пользователя по истечению времени, заданного в параметрах настроек - не более 10 минут, для возобновления сеанса работы пользователю необходимо повторно пройти аутентификацию по паролю.

Если пользователю необходимо отойти на некоторое время и не завершать свой сеанс, можно заблокировать компьютер, выполнив следующие действия:

– использовать «горячие клавиши» - нажать комбинацию клавиш <Ctrl> + <Alt> + <Del>;

– далее, в появившемся на экране окне, нажать кнопку «Блокировка».

При возобновлении сеанса работы пользователя необходимо набрать пароль пользователя ЛВС.

Порядок проведения антивирусного контроля

Для предотвращения частичного или полного уничтожения или изменения информации, циркулирующей в средств управления средствами антивирусной защиты осуществляется Администратором ЛВС от воздействия вредоносных программ – «закладок» и других компьютерных вирусов на коппьютеры устанавливаются антивирусные средства.

К использованию допускаются только лицензионные антивирусные средства, имеющие сертификат соответствия требованиям по безопасности информации ФСТЭК России. Департамент культуры Администрации г.о. Тольятти использует антивирус «Лаборатория Касперского».

Установка средств управления средствами антивирусной защиты осуществляется Администратором ЛВС в соответствии с технической документацией на используемые средства защиты от вредоносного программного обеспечения.

Установка и настройка клиентских частей средств антивирусной защиты на серверах и автоматизированных рабочих местах (далее – АРМ) сотрудников осуществляется Администратором средств управления средствами антивирусной защиты осуществляется Администратором ЛВС.

На всех серверах и АРМ работников Департамента культуры Администрации г.о. Тольятти используются настройки средств защиты от вредоносных программ, позволяющие:

- осуществлять автоматическую антивирусную проверку и «лечение» файлов в момент попытки записи или считывания файла;
- проверять каталоги и файлы по расписанию (с учетом нагрузки на сервер).

Работникам запрещается отключать средства антивирусной защиты и самостоятельно вносить изменения в настройки антивирусного программного обеспечения.

Актуализация антивирусных баз, администрирование и управление компонентами подсистемы антивирусной защиты выполняются централизованно. Обновление антивирусных баз с использованием доступа в сеть Интернет разрешено только с использованием средств криптографической защиты информации, имеющими сертификат соответствия ФСБ России и ФСТЭК России.

Полная антивирусная проверка рабочих станций и серверов Департамента культуры Администрации г.о. Тольятти осуществляется не реже 1 раза в неделю. Администратор ЛВС обязан проводить постоянный контроль результатов проверки и в случае обнаружения вирусной активности докладывать ответственному за информационную безопасность ЛВС.

В случае обнаружения высокой активности вредоносного программного обеспечения осуществляется переход в режим усиленного контроля с ежедневной антивирусной проверкой. Режим усиленного антивирусного контроля необходимо отменять только после определения и локализации каналов реализации угроз информационной безопасности, через которые возможно распространение данного вредоносного программного обеспечения.

Обновление антивирусных баз должно осуществляться ежедневно.

При использовании рабочих станций в сети «Интернет» сотрудники Департамента культуры Администрации г.о. Тольятти соблюдают следующие меры безопасности:

- при осуществлении почтового обмена необходимо исключать открытие сообщений, полученных от неизвестных адресатов или имеющих признаки массовой рассылки (тема письма содержит информацию рекламного характера, предложения дополнительного дохода, просьбы о помощи и другие варианты, рассчитанные на проявление интереса к содержанию сообщения). Сообщения, содержащие указанные выше признаки, необходимо удалять без предварительного прочтения;
- исключить загрузку программного обеспечения, видео или фотоматериалов, а также других материалов, использование которых не требуется для исполнения служебных обязанностей;
- при появлении в окне браузера сообщений, призывающих перейти по указанной ссылке, их необходимо закрывать. При случайном нажатии на такую ссылку необходимо оперативно закрыть открывающуюся страницу.

Программы

Программы для защиты информации Департамента культуры Администрации г.о. Тольятти включают в себя антивирусы, антишпионы, менеджеры паролей, приложения для резервного копирования.

Третий объект - Департамент культуры и молодежной политики Администрации г.о. Самара.

Обеспечением информационной безопасности Департамента культуры и молодежной политики Администрации г.о. Самара занимается Управление информационных ресурсов и технологий администрации г.о. Самара.

Управление информационных ресурсов и технологий Аппарата Администрации городского округа Самара является отраслевым (функциональным) органом Администрации городского округа Самара, через который Администрация городского округа Самара осуществляет свои полномочия в сфере информационных технологий, связи и телекоммуникаций, информационной безопасности и координацию в соответствии с действующим законодательством деятельности отраслевых (функциональных) органов Администрации городского округа Самара в данной сфере.

Задачи и функции Управления информационных ресурсов и технологий Аппарата Администрации городского округа Самара утвержденныраспоряжением Администрации городского округа Самара от 03.10.2018 № 40-р.

Основные задачи:

- обеспечение информационного взаимодействия отраслевых (функциональных) органов Администрации городского округа Самара;
- развитие информационной инфраструктуры – разработка, согласование и реализация организационно-технических мероприятий по внедрению информационных технологий, формированию единого информационного пространства в Администрации городского округа Самара;
- организация функционирования и развития телекоммуникационной инфраструктуры и информационных ресурсов Администрации городского округа Самара;

- обеспечение информационной безопасности в отраслевых (функциональных) органах Администрации городского округа Самара;
- обеспечение внедрения и функционирования автоматизированной системы электронного делопроизводства и управления документооборотом Администрации городского округа Самара (далее – СЭД), организация работ по ее развитию и поддержанию в актуальном состоянии;
- обеспечение централизованного руководства процессами, проектами и объектами информатизации отраслевых (функциональных) органов Администрации городского округа Самара;
- организация и координация работ по развитию в городском округе Самара информационного общества и формированию электронного муниципалитета;
- создание условий для обеспечения жителей городского округа Самара услугами связи в пределах предоставленных полномочий.
- участие в развитии и расширении сети почтовой связи на территории городского округа Самара;
- оказание содействия организациям связи в решении вопросов обеспечения жителей городского округа Самара услугами связи.

Средства и способы защиты информации

Основными средствами и способами защиты информации в Департаменте культуры и молодежной политики Администрации г.о. Самара являются:

- комплексная антивирусная защита информационных систем Департамента;
- обработка персональных данных и информации ограниченного распространения;
- управление сетями Департамента;
- управление логическим доступом к ресурсам Департамента;

– управление средствами криптографической защиты и их ключевыми системами;
– использование сотрудниками Департамента сети Интернет и корпоративной электронной почты;
– парольная политика;
– межсетевое взаимодействие информационных систем Департамента;
– управление физическим доступом сотрудников в помещения Депратамента;
– аудит событий информационной безопасности.

Программы

Программы для защиты информации Департамента культуры и молодежной политики Администрации г.о. Самара включают в себя антивирусы, антишпионы, менеджеры паролей, приложения для резервного копирования, межсетевые экраны.

Итоги анализа механизма обеспечения информационной безопасности экономических субъектов представлены в таблице 6.

Таблица 6 - Итоги анализа механизма обеспечения информационной безопасности экономических субъектов

Параметры исследования	Управление культуры Администрации г.о. Сызрань	Департамент культуры Администрации г.о. Тольятти	Департамент культуры и молодежной политики Администрации г.о. Самара
Ответственный за информационную безопасность (IT-аутсорсер)	Управление по организационной работе и информационным технологиям администрации г.о. Сызрань	Департамент информационных технологий и связи администрации г.о. Тольятти	Управление информационных ресурсов и технологий администрации г.о. Самара

Продолжение таблицы 6

Параметры исследования	Управление культуры Администрации г.о. Сызрань	Департамент культуры Администрации г.о. Тольятти	Департамент культуры и молодежной политики Администрации г.о. Самара
Средства и способы защиты информации	Антивирусная защита Парольная защита и идентификация пользователя Использование лицензионного программного обеспечения и сертифицированных средств защиты информации	- организация парольной защиты; - регистрация и учет действий пользователя; - проведение антивирусного контроля.	комплексная антивирусная защита ИС; обработка персональных данных и информации ограниченного распространения; управление сетями;; использование сотрудниками сети Интернет и корпоративной электронной почты; парольная политика; межсетевое взаимодействие информационных систем; управление физическим доступом сотрудников в помещения; аудит событий информационной безопасности.
Программы длязащиты информации	антивирусы, менеджеры паролей, приложения для резервного копирования.	антивирусы, антишпионы, менеджеры паролей, приложения для резервного копирования	антивирусы, антишпионы, менеджеры паролей, приложения для резервного копирования, межсетевые экраны.
Основные риски /угрозы	угрозы нарушения конфиденциальности информации; угрозы нарушения целостности информации; угрозы нарушения доступности информации	угрозы нарушения конфиденциальности информации; угрозы нарушения целостности информации; угрозы нарушения доступности информации	угрозы нарушения конфиденциальности информации; угрозы нарушения целостности информации; угрозы нарушения доступности информации.

На основании изложенных данных можно сделать вывод, на все исследуемые объекты уделяют важное значение обеспечению информационной безопастности.

Цель обеспечения информационной безопасности в органах местного самоуправления – защита информационных ресурсов от возможного несанкционированного доступа к ним, которое может привести к нанесению ущерба органам местного самоуправления и их сотрудникам, а также ограничить возможность выполнения своих полномочий.

Для достижения поставленной цели в органах местного самоуправления решаются следующие задачи:

- «анализ и оценка актуальных угроз и нарушителей информационной безопасности;
- оценка рисков информационной безопасности;
- внедрение организационных, программно-аппаратных и технических мер защиты информации;
- создание условий для оперативного реагирования на угрозы информационной безопасности» [13].

2.3 Оценка эффективности IT-аутсорсинга информационной безопасности экономических субъектов

Организация работ с целью обеспечения информационной безопасности - непрерывный процесс любого экоомического субъекта.

Анализ информационной безопасности экономических субъектов в рамках исследования проводился по методике, предложенной Т.А. Рудаковой и А.С. Бондаренко [26].

Ее суть состоит в том, что анализ эффективности информацилнной безопасности экономических субъектов проводится по определенным этапам (рисунок 5).

Рисунок 5 - Алгоритм оценки эффективности информационной безопасности экономических субъектов

Характеристика систем обеспечения информационной безопасности каждого экономического субъекта-объекта исследования была подробно исследована в предыдущем пункте.

Анализ существующих рисков и угроз.

Возможные риски и угрозы информационной безопасности также были исследованы в предыдущем пункте. На основе анализа можно сделать вывод, что в качестве возможных угроз нарушения информационной безопасности во всех рассматриваемых экономических субъектах можно выделить три основных группы угроз:

- «угрозы нарушения конфиденциальности информации;
- угрозы нарушения целостности информации;
- угрозы нарушения доступности информации» [14].

На третьем этапе был определен уровень информационной безопасности экономических субъектов.

Уровень информационной безопасности экономических субъектов рассчитывался по методике Ильяшенко С.Н., который предлагает при

определении уровня информационной безопасности использовать ряд коэффициентов:

«Коэффициент полноты информации (Кпл) — определяется как отношение объема информации, которая необходима для принятия обоснованного решения, ко всему объему информации, имеющемуся у лица, принимающего решения.

$$Кпл=Инеобх./И, \quad (1)$$

где Кпл – коэффициент полноты информации;

Инеобх. - объем информации, которая необходима для принятия обоснованного решения;

И – весь объем информации, имеющийся у лица, принимающего решения.

Коэффициент точности информации (Кт) — определяется как отношение релевантной информации к общему объему информации, имеющемуся в распоряжении субъекта.

$$Кт=Ирел./И, \quad (2)$$

где Кт – коэффициент точности информации;

Ирел. - объем релевантной информации;

И – весь объем информации, имеющийся у лица, принимающего решения.

Коэффициент противоречивости информации (Кпр) — определяется как отношение количества независимых свидетельств в пользу принятия управленческого решения к общему количеству независимых свидетельств в суммарном объеме релевантной информации. Объем оцениваемой информации может быть определен в станицах текста (формата А4), в

количестве символов в текстовом файле, в весе данного файла (Кбайт, Мбайт).

$$Кпр=НСупр./ НС, \quad (3)$$

где Кпр – коэффициент противоречивости информации;

НС - независимые свидетельства в пользу принятия управленческого решения;

НС – общее количество независимых свидетельств» [8] .

Общий уровень информационной безопасности «рассчитывается как произведение данных коэффициентов:

$$Ки = Кпл \times Кт \times Кпр. \quad (4)$$

где Ки – общий уровень информационной безопасности;

Кпл – коэффициент полноты информации;

Кт – коэффициент точности информации;

Кпр – коэффициент противоречивости информации.

Коэффициент уровня информационной безопасности в данном случае принимает числовое значение от 0 до 1 (таблица 7).

Данная методика является ограниченной в применении в связи с трудностями в точном выделении из всей имеющейся информации данных, необходимых для принятия управленческих решений» [12].

Таблица 7 – Определение уровня информационной безпасности

Значение коэффициента	Уровень
$Ки \geq 0,7$	Высокий
$0,3 \leq Ки < 0,7$	Средний
$Ки < 0,3$	Низкий

Таблица 8 – Расчет уровня информационной безопасности экономических субъектов

Коэффициенты	Управление культуры Администрации г.о. Сызрань	Департамент культуры Администрации г.о. Тольятти	Департамент культуры и молодежной политики Администрации г.о. Самара
Коэффициент полноты информации (Кпл)	0,78	0,71	0,82
Коэффициент точности информации (Кт)	0,88	0,86	0,98
Коэффициент противоречивости информации (Кпр)	0,72	0,86	0,89
Общий уровень информационной безопасности	0,49	0,53	0,72

Общий уровень информационной безопаснойсти представлен на рисунке 6.

Рисунок 6 - Общий уровень информационной безопаснойсти экономических субъектов

На основании рассчитанных данных можно сделать вывод, что лишь в Департаменте культуры и молодежной политики Администрации г.о. Самара

общий уровень информационной безопасности может быть оценен как высокий (0,72), а в Управлении культуры Администрации г.о. Сызрань и Департаменте культуры Администрации г.о. Тольятти уровень информационной безопасности – среднй (0,49 и 0,53 соответственно).

Поэтому для повышения уровня информационной безопасности данным экономическим субъектам рекомендуется применение IT-аутсорсинга как инструмента обеспечения информационной безопасности экономических субъектов.

Выявленные проблемы и пути их решения представлены в таблице 9.

Таблица 9 – Выявленные проблемы и пути их решения

Проблемы	Пути решения
1. Высокий уровень угроз: - угрозы нарушения конфиденциальности информации; - угрозы нарушения целостности информации; - угрозы нарушения доступности информации	Снижение уровня угроз
2. Недостаточный (средний) уровень информационной безопасности	Повышение уровня информационной безопасности

Мероприятия, направленные на решение выявленных проблем, будут рассмотрены в следующей главе.

Таким образом, на основании рассчитанных данных можно сделать вывод, что лишь в Департаменте культуры и молодежной политики Администрации г.о. Самара общий уровень информационной безопасности может быть оценен как высокий (0,72), а в Управлении культуры Администрации г.о. Сызрань и Департаменте культуры Администрации г.о.

Тольятти уровень информационной безопасности – средний (0,49 и 0,53 соответственно).

Поэтому для повышения уровня информационной безопасности данным экономическим субъектам рекомендуется применение IT-аутсорсинга как инструмента обеспечения информационной безопасности экономических субъектов.

Нна основании проведенного анализа обеспечения информационной безопасности Управления культуры Администрации г.о. Сызрань можно сделать вывод, что данный бизнес-процесс уже выведен на аутсорсинг: обеспечением информационной безопасности Управления культуры Администрации г.о. Сызрань занимается Управление по организационной работе и информационным технологиям администрации г.о. Сызрань.

Однако, анализ Положения Управления по организационной работе и информационным технологиям администрации г.о. Сызрань позволяет сделать вывод, что обеспечению информационной безопасности Управления культуры Администрации г.о. Сызрань должного внимания не уделяется.

Также по результатам анализа обеспечения информационной безопасности Управления культуры Администрации г.о. Сызрань был выявлен ряд проблем, основными из которых стали:

– высокий уровень угроз информационной безопасности;

– недостаточный (средний) уровень информационной безопасности.

Именно поэтому необходимо разработать мероприятия по совершенствованию IT-аутсорсинга Управления культуры Администрации г.о. Сызрань.

3 Внедрение IT-аутсорсинга как инстумента обеспечения информационной безопасности Управления культуры Администрации г.о. Сызрань

3.1 Разработка мероприятий по совершенствованию IT-аутсорсинга

На основании проведенного анализа обеспечения информационной безопасности Управления культуры Администрации г.о. Сызрань можно сделать вывод, что данный бизнес-процесс уже выведен на аутсорсинг: обеспечением информационной безопасности Управления культуры Администрации г.о. Сызрань занимается Управление по организационной работе и информационным технологиям администрации г.о. Сызрань.

Однако, анализ Положения Управления по организационной работе и информационным технологиям администрации г.о. Сызрань позволяет сделать вывод, что обеспечению информационной безопасности Управления культуры Администрации г.о. Сызрань должного внимания не уделяется.

Также по результатам анализа обеспечения информационной безопасности Управления культуры Администрации г.о. Сызрань был выявлен ряд проблем, основными из которых стали:

– высокий уровень угроз информационной безопасности;

– недостаточный (средний) уровень информационной безопасности.

Именно поэтому необходимо разработать мероприятия по совершенствованию IT-аутсорсинга Управления культуры Администрации г.о. Сызрань.

Анализ опыта муниципальных образований в сфере IT-аутсорсинга (в частности, г.о. Самара) позволяет сделать вывод, что IT – аутсорсинг как инструмент обеспечения информационной безопасности экономических субъектов может быть достаточно эффективным при использовании системы информационной безопасности.

Дерево решений для внедрения IT-аутсорсинга как инстумента обеспечения информационной безопасности Управления культуры Администрации г.о. Сызрань представлено на рисунке 7.

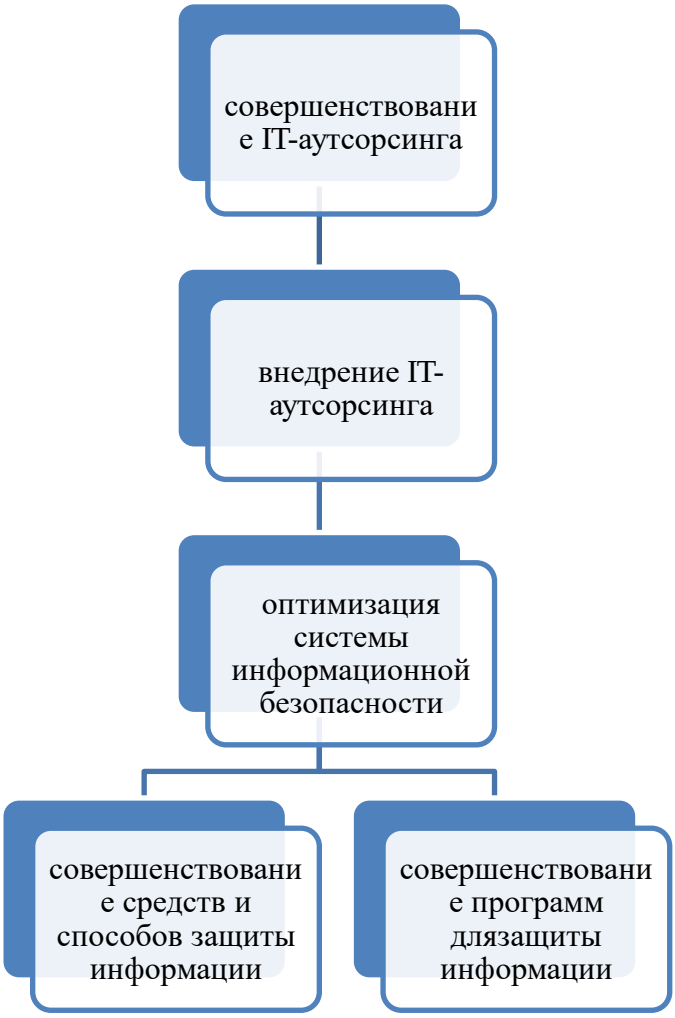

Рисунок 7 - Дерево решений для внедрения IT-аутсорсинга как инстумента обеспечения информационной безопасности Управления культуры Администрации г.о. Сызрань

Реализация предложенных мероприятий будет осуществляться с использованием метода проектов.

Цель проекта – совершенствование IT-аутсорсинга как инстумента обеспечения информационной безопасности Управления культуры Администрации г.о. Сызрань

Задачи проекта:

– внедрение IT-аутсорсинга как инстумента обеспечения информационной безопасности Управления культуры Администрации г.о. Сызрань;
– оптимизация системы информационной безопасности Управления культуры Администрации г.о. Сызрань.

Как уже было отмечено, Управление по организационной работе и информационным технологиям администрации г.о. Сызрань, который в настоящее время осуществляет IT-аутсорсинг информационной безопасности Управления культуры администрации г.о. Сызрань, обеспечению информационной безопасности Управления культуры Администрации г.о. Сызрань должного внимания не уделяет.

Именно поэтому все бизнес-процессы, позволяющие обеспечить информационную безопасность Управления культуры администрации г.о. Сызрань, рекомендуется передать на внешний аутсорс.

В современном понимании аутсорсинг - это «передача не являющихся основными функций организации сторонним исполнителям. К причинам, лежащим в основе такого рода управленческих решений, как правило, относятся:

– снижение затрат посредством передачи вспомогательных функций сторонним организациям;
– высвобождение ресурсов для исполнения основных функций организации;
– отсутствие достаточного опыта в той или иной сфере деятельности» [1].

Внедрение IT-аутсорсинга как инстумента обеспечения информационной безопасности Управления культуры Администрации г.о. Сызрань предлагается за счет передачи на аутсорсинг всех бизнес-процессов по обеспечению информационной безопасности с целью защиты информационных ресурсов от возможного несанкционированного доступа к ним, которое может привести к нанесению ущерба Управлению культуры

Администрации г.о. Сызрань и его сотрудникам, государственным органам и учреждениям Самарской области, а также ограничить возможность выполнения Управлением своих полномочий.

Оптимизация системы информационной безопасности Управления культуры Администрации г.о. Сызрань предполагает построение системы обеспечения информационной безопасности (СОИБ) с использованием модели Деминга и заключается в цикличном выполнении следующей группы процессов (рисунок 8):

- планирование СОИБ;
- реализация СОИБ;
- проверка СОИБ;
- совершенствование СОИБ.

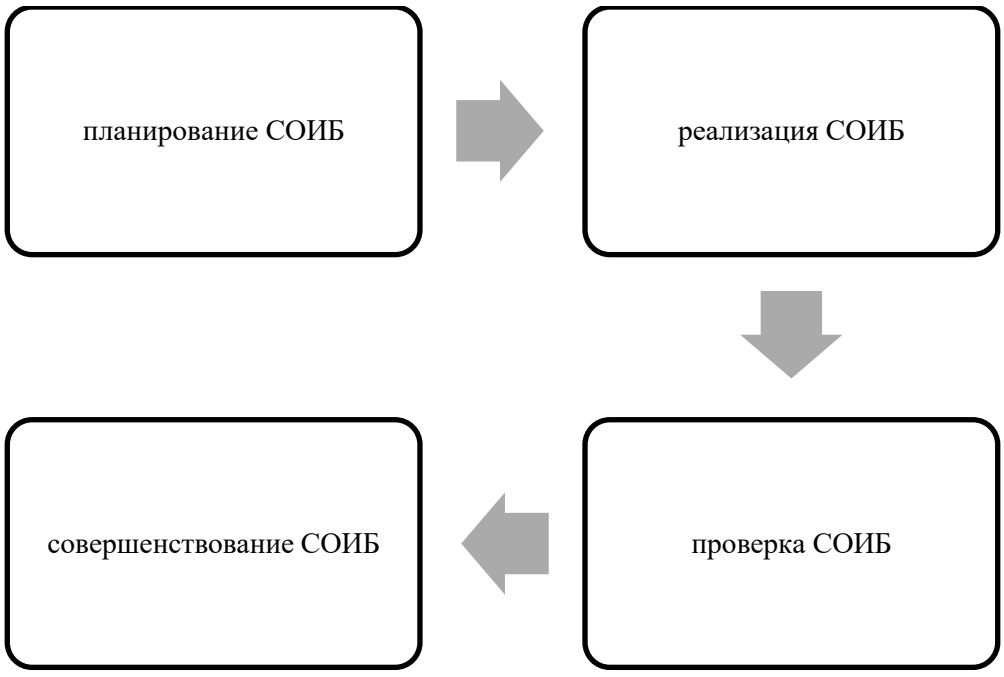

Рисунок 8 – Основные этапы оптимизации системы информационной безопасности Управления культуры Администрации г.о. Сызрань

На этапе планирования СОИБ в Управлении культуры Администрации г.о. Сызрань необходимо провести следующие работы:

– анализ требований законодательства РФ и нормативных правовых документов РФ в области обеспечения информационной безопасности;
– определение и распределение ролей сотрудников Управления культуры в области обеспечения информационной безопасности;
– анализ и оценка рисков информационной безопасности:
– идентификация информационных, программных и физических ресурсов Управления культуры;
– определение потенциальных нарушителей информационной безопасности для Управления культуры (модель нарушителя);
– определение значимых для Управления культуры угроз информационной безопасности (модель угроз информационной безопасности);
– оценка вероятности возникновения угроз информационной безопасности;
– оценка степени влияния угроз информационной безопасности на деятельность Управления культуры;
– оценка рисков нарушения информационной безопасности в Управлении культуры;
– рассмотрение различных вариантов применения средств защиты информации, в целях минимизации выявленных рисков информационной безопасности;
– оценка затрат на реализацию средств защиты.

На этапе реализации СОИБ в Управлении культуры необходимо провести следующие работы:

– внедрение внутренних распорядительных документов, регламентирующих требования к системе обеспечения информационной безопасности в технологических процессах Управлении культуры;

– внедрение и конфигурирование программных, программно-аппаратных и технических средств защиты информации;
– внедрение процедур управления инцидентами информационной безопасности;
– повышение осведомленности сотрудников Управления культуры в вопросах обеспечения информационной безопасности.
– обеспечение непрерывности функционирования информационных систем Управления культуры и возможности восстановления их после сбоя.

На этапе проверки СОИБ в Управления культуры необходимо провести следующие работы:

– контроль корректности и бесперебойности функционирования программных, программно-аппаратных и технических средств защиты информации;
– контроль исполнения сотрудниками Управления культуры внутренних документов Управления культуры, регламентирующих вопросы обеспечения информационной безопасности.
– проведение оценки соответствия системы обеспечения информационной безопасности требованиям к защите информационных ресурсов Управления культуры, установленных законодательством РФ и региональными нормативно-правовыми актами.

На этапе совершенствования СОИБ в Управлении культуры Администрации г.о. Сызрань необходимо провести следующие работы:

– анализ результатов проверки СОИБ;
– внесение оперативных изменений в состав и конфигурацию средств защиты информации;
– внесение изменений в документы, регламентирующие деятельность по обеспечению информационной безопасности;
– разработка планов по тактическим улучшениям СОИБ.

Так, оптимизация системы информационной безопасности Управления культуры Администрации г.о. Сызрань предполагает построение системы обеспечения информационной безопасности (СОИБ) посредством проведения следующих мероприятий:

– совершенствование средств и способов защиты информации;
– совершенствование программ длязащиты информации.

Данные мероприятия предполагают постановку и решение следующих задач:

– разработка и внедрение комплексной антивирусной защиты информационных систем Управления культуры администрации г.о. Сызрань;
– обработка персональных данных и информации ограниченного распространения;
– управление сетями Управления культуры;
– управление логическим доступом к ресурсам Управления культуры;
– управление средствами криптографической защиты и их ключевыми системами;
– использование сотрудниками Управления культуры сети Интернет и корпоративной электронной почты с защитными механизмами;
– парольная политика;
– межсетевое взаимодействие информационных систем Управления культуры;
– управление физическим доступом сотрудников в помещения Управления культуры;
– аудит событий информационной безопасности.

Учитывая, что в настоящее время Управление по организационной работе и информационным технологиям администрации г.о. Сызрань, выполняющее функционал по обеспечению информационной безопасности, уделяет незначительное внимание работам по информационной безопасности, а также сложность проектных работ и высокие требования к

квалификации персонала, который будет выполнять данный функционал, данный вид работ предлагается перевести на аутсорсинг.

Для реализации данного мероприятия потребуются следующие виды ресурсов:

- интеллектуальные ресурсы. Требуется привлечение сотрудников Управления культуры Администрации г.о. Сызрань и IT-аутсорсера, который будет выполнять работы по обеспечению информационной безопасности;
- финансовые ресурсы. Финансирование предусматривается за счет муниципального бюджета г.о. Сызрань;
- организационные ресурсы. Реализацию проекта предполагается осуществлять путем создания команды проекта во главе с проект-менеджером (IT-аутсорсером);
- управленческие ресурсы. Руководство разработкой и осуществлением проекта должно быть возложено на проект-менеджера;
- профессиональные ресурсы, сотрудники Управления культуры Администрации г.о. Сызрань, а также руководитель проекта - IT-аутсорсер, который будет выполнять работы по обеспечению информационной безопасности Управления культуры.

Основные этапы проекта, их наименование, дата начала, длительность и дата завершения представлены в таблице 10.

Таблица 10 - Основные этапы проекта по внедрению IT-аутсорсинга как инстумента обеспечения информационной безопасности Управления культуры Администрации г.о. Сызрань

Этапы	Начало	Длительность	Окончание
Постановка целей проекта	01.04.2023	8	09.04.2023
Определение функций компании IT-аутсорсера	10.04.2023	5	15.04.2023
Поиск и отбор IT-аутсорсера, заключение договора	16.04.2023	18	04.05.2023
Построение системы взаимодействия	05.05.2023	9	14.05.2023
Работа по обеспечению информационной безопасности Управления культуры	15.05.2023	230	31.12.2023
Оценка эффективности проекта	01.01.2024	1	02.01.2024

План-график проектных мероприятий представлен на рисунке 9.

Рисунок 9 - План-график проектных мероприятий

Расчет затрат на совершенствование IT-аутсорсинга Управления культуры администрации г.о. Сызрань и расчет экономической эффективности предложенных мероприятий представим ниже.

3.2 Расчет затрат на совершенствование IT-аутсорсинга

В рамках реализации мероприятий, направленных на совершенствование IT-аутсорсинга Управления культуры администрации г.о. Сызрань предполагается ряд работ, требующих опредененных затрат.

В качестве компании-аутсорсера была выбрана компания 1BITcloud, которая не только является официальным партнером 1С по предоставлению во временное пользование программ на технологической платформе 1С:Предприятие 8, но и обеспечивает системное администрирование и поддержку IT-инфраструктуры без отпуска и выходных.

При выборе компании-аутсорсера учитывались следующие показатели:

- возможность круглосуточной защиты и администрирования IT-инфраструктуры деятельности компании;
- предоставление комплексной поддержкки;
- стоимость услуг.

Кроме того, выбранная компания-IT-аутсорсер обеспечивает следующий спектр услуг:

- NDA (соглашение о неразглашении). Заключение соглашения для предотвращения утечки любой конфиденциальной информации: от коммерческой тайны до персональных данных;
- обеспечение антивирусной защиты. Защита серверов и рабочих станций пользователей от вредоносных программ, а также очистка от вирусов в случае заражения;
- резервное копирование данных. Обеспечение резервного копирования и восстановления информации при необходимости;
- система хранения доступов. Создание, модификация и удаление учетных записей и групп пользователей

Так, расходы на внедрение IT-аутсорсинга как инструмента обеспчения информационной безопасности Управления культуры будут состоять из следующих статей:

– автоматизированное рабочее место;

– принтер\сканер\МФУ;

– серверная операционная система на базе Microsoft;

– управляемый коммутатор\маршрутизатор\Wi-Fi точка;

– видеорегистратор;

– IP камера видеонаблюдения;

– телефонная станция IP;

– сетевое хранилище данных;

– СКУД (система контроля удаленного доступа);

– считыватель СКУД.

Статьи затрат и их величина представлены в таблице 11.

Таблица 11 - Статьи затрат и их величина на внедрение IT-аутсорсинга как инструмента обеспчения информационной безопасности Управления культуры администрации г.о. Сызрань

Статья затрат	цена за ед., в месяц	Количество	Сумма
Автоматизированное рабочее место	640	12	7 680
Принтер\сканер\МФУ	400	6	2 400
Серверная операционная система на базе Microsoft	2 400	1	2 400
Управляемый коммутатор\маршрутизатор\Wi-Fi точка	400	1	400
Видеорегистратор	2 000	12	24 000
IP камера видеонаблюдения	400	12	4 800
Телефонная станция IP	2 400	1	2 400
Сетевое хранилище	2 400	1	2 400
СКУД	2 000	1	2 000
считыватель СКУД	400	1	400
ИТОГО			48 880

Таким образом, затраты в месяц на IT-аутсорсинг составят 48 880 руб.

Заключение договора сроком более, чем на 6 месчцев (договор планируется заключить до конца 2023 года) предполагает предоставление

скидки 10%. Так, расходы в месяц составят 43 992 руб., расходы в год – 527 904 руб.

Расходы также включают в себя круглосуточную техническую поддержку.

В следующем раделе произведем расчет экономической эффективности предложенных мероприятий.

3.3 Экономическая эффективность предложенных мероприятий

Оценка эффективности «организации информационной безопасности предполагает оценку общего уровня затрат (материальных, трудовых, финансовых) на построение системы информационной безопасности и оценку достигаемого эффекта. Грамотное распределение ресурсов в целях обеспечения информационной безопасности приводит к повышению уровня информационной безопасности» [6].

Как уже было отмечено, в рамках реализации мероприятий, направленных на совершенствование IT-аутсорсинга Управления культуры администрации г.о. Сызрань предполагается ряд работ, требующих опредененных затрат.

Учитывая сложность работ и необходимый высокий уровень квалификации сотрудников, позволяющих обеспечить необходимый уровень информационной безопасности, все работы было предложено перевести на аутсорсинг.

Заключение договора сроком более, чем на 6 месчцев (договор планируется заключить до конца 2023 года) предполагает предоставление скидки 10%. Так, расходы в месяц составят 43 992 руб., расходы в год – 527 904 руб. Расходы также включают в себя круглосуточную техническую поддержку.

Рассмотрим еще один вариант совершенствования IT-аутсорсинга Управления культуры администрации г.о. Сызрань – введение в штат

Управления по организационной работе и информационным технологиям администрации г.о. Сызрань дополнительного сотрудника, который бы занимался исключительно обеспечением информационной безопасности.

Анализ рынка труда г.о. Сызрань (сайт https://syzran.jobcareer.ru/zarplata/) позволяет сделать вывод, что на начало 2023 года средняя заработная плата IT-специалиста в г. Сызрань – 55 000 рублей. Однако, помимо заработной платы работодатель обязан уплачивать за сотрудников страховые взносы.

Масштабные нововведения по страховым взносам - 2023 связаны с такими серьезными мероприятиями, как:

– объединение ПФР и ФСС;

– введение единого налогового платежа (ЕНП).

В результате в законодательстве о страховых взносах с 2023 года появятся такие понятия, как «единый тариф», «единая предельная база».

В 2023 году величина предельной базы поднялась с 1 565 000 до 1 917 000 рублей.

«Единый тариф» составляет 30% в рамках единой предельной величины базы; 15,1% - сверх предельной базы.

Сравнение расходов на введение в штат IT-специалиста и аутсорсера представлено в таблице 12.

Таблица 12- Сравнение расходов на введение в штат IT-специалиста и аутсорсера

Расходы	аутсорсер	штатный сотрудник
расходы на оплату труда, в месяц	43 992	55 000
расходы на оплату труда, в год	527 904	660 000
страховые взносы (единый тариф, 30%)	0	198 000
Итого расходы, в год	527 904	858 000

Экономия на перевод услуг на ауосорсинг составит: 858 000 - 527 904 = 330 096 тыс.руб. в год.

Таким образом, представленные данные наглядно демонстрируют целесообразность передачи работ по обеспечению информационной безопасности на IT-аутсорсинг. Кроме того, заключение договора на аутсорс предполагает круглосуточную техническую поддержку и отсутствие рисков из-за болезни или увольнения штатного сотрудника.

Годовой экономический эффект - это показатель, характеризующий уменьшение общей совокупности затрат, связанных с производством годового объема продукции предприятия.

Годовой экономический эффект составит : 858 000 - 527 904 = 330 096 тыс.руб. в год.

Согласно опыту конкурирующих компаний, внедрение IT-аутсорсинга как инструмента обеспечения экономической безопасности экономических субъектов позволит увеличить доходы на 20%.

Планируемые доходы составят 328,4*1,2*1000 = 394 080 тыс.руб.

Эффективность рассчитывается по формуле:

$$Э = \frac{Р}{З} * 100\%, \quad (6)$$

где Р - результат,

З –затраты.

Эффективность составит:

$$Э = \frac{394\ 080}{527904} * 100\% = 75\%$$

Для определения простого срока окупаемости инвестиций (PP) используется формула:

$$PP = IC / CF, \quad (7)$$

где PP – простой срок окупаемости;

IC – сумма инвестиций в проект;

CF – планируемая ежегодная прибыль.

PP = 527 904/394 080=1,34 года.

Рассчитанные данные позволяют сделать вывод, что введение IT-аутсорсинга как инструмента обепечения информационной безопасности в Управлении культуры администрации г.о. Сызрань будет экономически целесообразно.

Таким образом, анализ опыта муниципальных образований в сфере IT-аутсорсинга (в частности, г.о. Самара) позволяет сделать вывод, что IT – аутсорсинг как инструмент обеспечения информационной безопасности экономических субъектов может быть достаточно эффективным при использовании системы информационной безопасности.

Учитывая сложность работ и необходимый высокий уровень квалификации сотрудников, позволяющих обеспечить необходимый уровень информационной безопасности, все работы было предложено перевести на аутсорсинг.

В качестве компании-аутсорсера была выбрана компания 1BITcloud, которая не только является официальным партнером 1С по предоставлению во временное пользование программ на технологической платформе 1С:Предприятие 8, но и обеспечивает системное администрирование и поддержку IT-инфраструктуры без отпуска и выходных.

Годовой экономический эффект составит : 858 000 - 527 904 = 330 096 тыс.руб. в год.

Кроме того, согласно опыту конкурирующих компаний, внедрение IT-аутсорсинга как инструмента обеспечения экономической безопасности экономических субъектов позволит увеличить доходы на 20%.

Планируемые доходы составят 328,4*1,2*1000 = 394 080 тыс.руб.

Эффективность составит 75%, срок окупаемости инвестиций – 1,34 года.

Рассчитанные данные позволяют сделать вывод, что введение IT-аутсорсинга как инструмента обепечения информационной безопасности в Управлении культуры администрации г.о. Сызрань будет экономически целесообразно.

Заключение

Информационная безопасность предприятия связана с обеспечением необходимого уровня защиты информации. Поэтому информационная безопасность должна контролироваться, должны разрабатываться меры по управлению рисками, формироваться стандарты по управлению защитой информации. В процессе обеспечения информационной безопасности следует уделять внимание формальным методам защиты информации. В основе заложена стандартизация. Ее цель направлена на доверие, реализацию мер по защите данных от вероятных рисков, снижение угроз.

Немаловажную роль в формировании системы экономической безопасности играет профессиональный опыт руководителя службы экономической безопасности и уровень технической оснащенности предприятия. Однако основная сложность построения системы экономической безопасности заключается в ее зависимости от человеческого фактора. Сложно достичь желаемого результата, если работники не осознают значимости и потребности мероприятий для поддержания экономической безопасности.

Особенностью и одновременно сложностью системы экономической безопасности является ее зависимость от человеческого фактора. Даже при компетентном руководителе службы безопасности успеха предприятие может добиться тогда, когда каждый сотрудник осознаёт значимость и потребность во внедряемых мерах экономической безопасности.

В целях защиты информации, размещенной в информационной системе общего пользования должна быть обеспечена разработка мер при ее проектировании и эксплуатации, направленных на выполнение требований к безопасности этой информационной системы общего пользования.

На основании проведенного исследования можно сделать вывод, на все исследуемые объекты уделяют важное значение обеспечению информационной безопастности.

Цель обеспечения информационной безопасности в органах местного самоуправления – защита информационных ресурсов от возможного несанкционированного доступа к ним, которое может привести к нанесению ущерба органам местного самоуправления и их сотрудникам, а также ограничить возможность выполнения своих полномочий.

Для достижения поставленной цели в органах местного самоуправления решаются следующие задачи:

- «анализ и оценка актуальных угроз и нарушителей информационной безопасности;
- оценка рисков информационной безопасности;
- внедрение организационных, программно-аппаратных и технических мер защиты информации;
- создание условий для оперативного реагирования на угрозы информационной безопасности» [13].

На основании проведенного анализа обеспечения информационной безопасности Управления культуры Администрации г.о. Сызрань можно сделать вывод, что данный бизнес-процесс уже выведен на аутсорсинг: обеспечением информационной безопасности Управления культуры Администрации г.о. Сызрань занимается Управление по организационной работе и информационным технологиям администрации г.о. Сызрань.

Однако, анализ Положения Управления по организационной работе и информационным технологиям администрации г.о. Сызрань позволяет сделать вывод, что обеспечению информационной безопасности Управления культуры Администрации г.о. Сызрань должного внимания не уделяется.

Также по результатам анализа обеспечения информационной безопасности Управления культуры Администрации г.о. Сызрань был выявлен ряд проблем, основными из которых стали:

- высокий уровень угроз информационной безопасности;
- недостаточный (средний) уровень информационной безопасности.

Именно поэтому необходимо разработать мероприятия по совершенствованию IT-аутсорсинга Управления культуры Администрации г.о. Сызрань.

Анализ опыта муниципальных образований в сфере IT-аутсорсинга (в частности, г.о. Самара) позволяет сделать вывод, что IT – аутсорсинг как инструмент обеспечения информационной безопасности экономических субъектов может быть достаточно эффективным при использовании системы информационной безопасности.

Учитывая сложность работ и необходимый высокий уровень квалификации сотрудников, позволяющих обеспечить необходимый уровень информационной безопасности, все работы было предложено перевести на аутсорсинг.

В качестве компании-аутсорсера была выбрана компания 1BITcloud, которая не только является официальным партнером 1С по предоставлению во временное пользование программ на технологической платформе 1С:Предприятие 8, но и обеспечивает системное администрирование и поддержку IT-инфраструктуры без отпуска и выходных.

Годовой экономический эффект составит : 858 000 - 527 904 = 330 096 тыс.руб. в год.

Кроме того, согласно опыту конкурирующих компаний, внедрение IT-аутсорсинга как инструмента обеспечения экономической безопасности экономических субъектов позволит увеличить доходы на 20%.

Планируемые доходы составят 328,4*1,2*1000 = 394 080 тыс.руб.

Эффективность составит 75%, срок окупаемости инвестиций – 1,34 года.

Рассчитанные данные позволяют сделать вывод, что введение IT-аутсорсинга как инструмента обепечения информационной безопасности в Управлении культуры администрации г.о. Сызрань будет экономически целесообразно.

Список используемой литературы и используемых источников

1. Аникин Б.А., Рудая И.Л. Аутсорсинг и аутстаффинг, Высокие технологии менеджмента. М.: Инфра-М, 2019. 320 с.

2. Богачев В.И., Шевченко М.Н., Денисенко И.А. Обеспечение экономической безопасности в деятельности международных интеграционных образований // The Mechanism of Economic and Legal National Security: Experience, Problems and Prospects Materials of scientific-practical conference. Лондон, 2018. С. 20-29.

3. Богачев В.И., Шевченко М.Н., Рипка А.Н. и др. Теневая экономика: сущность, опасные тенденции расширения её масштабов, организация мер безопасности. Луганск, 2019. 314 с.

4. Гильмиярова М. Р. Концептуально-понятийные основы развития аутсорсинга // Экономика, право и управление. 2019. №2. С. 3-12

5. Денисенко И.А., Пономарев А.А. Устойчивое развитие в системе экономической безопасности на примере предприятий оптовой и розничной торговли // Направления повышения эффективности управленческой деятельности органов государственной власти и местного самоуправления. Сборник материалов I Международной научно-практической конференции. 2018. С. 64-68.

6. Джобава Р.Г. Методы оценки экономической целесообразности использования аутсорсинга // Гуманизация образования.2019. №7. С.37-41.

7. Егорова М.В. Финансовая безопасность предприятия и ее угрозы и влияние на экономическую безопасность предприятия // Социально-экономические проблемы в современной России. Сборник научных трудов преподавателей и магистрантов. М., 2019. С. 62-65.

8. Ильяшенко С. Н. Составляющие экономической безопасности предприятия и подходы к их оценке [Электронный ресурс]. — Режим доступа: https://docplayer.ru/47237310-Sostavlyayushchie-ekonomicheskoy-

bezopasnosti-predpriyatiya-i-podhody-k-ih-ocenke-ilyashenko-s-n.html (дата обращения: 07.06.22).

9. Использование ИТ-аутсорсинга для обеспечения экономической безопасности предприятия / В. Ю. Щеглов, А. О. Скворцов // Известия высших учебных заведений. Поволжский регион. Экономические науки. 2018. № 2 (8). С. 29-34.

10. Кавчук Д.А., Тумоян Е.П., Астафьев Г.А. Интеллектуальный подход к анализу рисков и уязвимостей информационных систем // Известия ЮФУ. Технические науки. 2018. № 12 (149). С. 79- 86.

11. Кириллова А. Аутсорсинг и аутстаффинг как новые технологии менеджмента // Финансовая жизнь, 2019. - № 1. – С. 55-58.

12. Козаченко А. В. Экономическая безопасность предприятия: сущность и механизм обеспечения: [монография] / А. В. Козаченко, В. П. Пономарьов, О. М. Ляшенко. К. : Либра, 2019. С. 87.

13. Курбанов А.Х. Методика оценки целесообразности использования аутсорсинга // Современные проблемы науки и образования. 2019. № 1. С. 110-114.

14. Кузнецов В.М. Аутсорсинг: новое слово в управление // ЭКО: Экономика и организация промышленного производства. 2015. №6. С.79-86.

15. Круглов В.Н., Доценко Д.В. Экономическая безопасность: Аудит и финансовый анализ, 2019. №4. С. 415-426.

16. Луцкая Н.В. Аутсорсинг и инсорсинг как взаимодополняющие инструменты менеджмента для формирования оптимальной организационной структуры предприятия // Организатор производства. 2019. №2. С.41-57.

17. Луцкая Н.В. Аутсорсинг: уровни предоставляемых услуг и модели взаимодействия сторон // Компетентность . 2018. №2 (133). С. 30-36.

18. Маркеева Г. А., Михнева С. Г. История возникновения и этапы развития аутсорсинга // Известия высших учебных заведений. Поволжский регион. Экономические науки. 2019. №1. С. 106-116.

19. Механизмы управления экономической безопасностью / Ю. Г. Лысенко, С. Г. Мищенко, Р. А. Руденский, А. А. Спиридонов ; под ред. Ю. Г. Лысенко. Донецк : ДонНУ, 2019. 178 с.

20. Минасьян М. аутсорсинг в практике американских компаний // Инвестиции в России. 2018. №10 (165). С. 27-37.

21. Муфтахутдинова Х.Р. Аутсорсинг как инфраструктурный элемент развития внешнеторговой деятельности промышленного предприятия // Социально-экономическое управление: теория и практика. 2019. №1 (21). С.10-15.

22. Николаев В. Облачные технологии как инструмент ИТ-аутсорсинга / В. Николаев // Директор по безопасности. 2019. № 2.

23. Овакимян Г. С. Современные методы повышения конкурентоспособности предприятия: бенчмаркинг и аутсорсинг // Экономика и управление: проблемы и решения. 2018. № 7.

24. Охотский Е.В. Участие России в международном антикоррупционном сотрудничестве // Вопросы государственного и муниципального управления. 2019. № 1. С. 211-228.

25. Попов И.С., Березин В.В. Аутсорсинг как способ повышения эффективности бизнеса в современной экономике // Вестник академии. 2018. №4. С. 116-117.

26. Райзберг Б. А., Лозовский Л. Ш., Стародубцева Е. Б. Современный экономический словарь. 5-е изд., перераб. и доп. — М.: ИНФРА-М, 2019. 495 с.

27. Рудакова Т.А., Бондаренко А.С. Инструментарий оценки информационной составляющей экономической безопасности предприятия // Бизнес и экономическая безопасность. Лизинг. 2019 г. №6. С. 47-55.

28. Указ Президента РФ от 13.05.2017 N 208 "О Стратегии экономической безопасности Российской Федерации на период до 2030 года"

29. Цыбулин А.М. Архитектура автоматизированной системы управления информационной безопасностью предприятия // Известия ЮФУ. Технические науки. 2019. № 12 (125). С. 58-64.

30. Черняк В.З. Управление предпринимательскими рисками в системе экономической безопасности. Теоретический аспект // ЮНИТИ-ДАНА, Закон и право, 2019. С. 78.

31. Шлыков В.В. Комплексное обеспечение экономической безопасности предприятия. СПб.: Алетейя, 2019. 167 с.

32. Шульженко Л.Е., Денисенко И.А., Потапкин А.В. Тенденции развития зарубежной налоговой политики // Научный Вестник ГОУ ЛНР «Луганский национальный аграрный университет». 2019. № 5. С. 508-527.

33. Authorization. Types and methods of authentication. — Access mode: http://life-prog.ru/view_programmer.php?id=159&page=16, free (accessed: Identification and authentication. Access mode: http://www.itsec.ru/articles2/Inf_security/id-i-aut/, free (accessed: 28.05.2022).

34. Gutmann P. The Subterranean Economy // Financial Analysts Journal. 1977. № 34. P. 20.

35. Michael H. David, L. John, V. 19 deadly sins that threaten the security of programs:studies. manual / X. Michael, David. L, John. in Moscow: DMK Press, 2016. 228s.

36. Managing vulnerability. Access mode: http://securitymicrotest.ru/resheniya/information-security-anagement/vulnerability-management/, free(accessed: 28.05.2022).

37. Fingar P. Dot. Cloud. Oblachnyye vychisleniya - biznes-platforma XXI veka [Cloud computing is the business platform of the 21st century.] // M.: Akvamarinovaya kniga, 2011. 256 p.

Приложение А

Отчет об исполнении бюджета Управления культуры Администрации г.о. Сызрань за 2019 год

Таблица А.1 - Отчет об исполнении бюджета Управления культуры Администрации г.о. Сызрань за 2019 год

Наименование главного распорядителя средств бюджета, раздела, подраздела, целевой статьи, вида расходов бюджета городского округа	Утвержденный план		Кассовое исполнение		% исполнения	
	Всего	В том числе средства выше-стоящих бюджетов	Всего	В том числе средства выше-стоящих бюджетов	Всего	В том числе средства выше-стоящих бюджетов
Управленияе культуры Администрации г.о. Сызрань	976 323	377 780	968 214	370 683	99,2	98,1
Мероприятия на обеспечение деятельности органов местного самоуправления в сфере культуры	164		164		100,0	
Закупка товаров, работ и услуг для обеспечения государственных (муниципальных) нужд	164		164		100,0	
Иные закупки товаров, работ и услуг для обеспечения государственных (муниципальных) нужд	164		164		100,0	

Приложение Б

Отчет об исполнении бюджета за Управления культуры Администрации г.о. Сызрань 2020 год

Таблица Б.1 - Отчет об исполнении бюджета Управления культуры Администрации г.о. Сызрань за 2019 год

Наименование главного распорядителя средств бюджета, раздела, подраздела, целевой статьи, вида расходов бюджета городского округа	Утвержденный план		Кассовое исполнение		% исполнения	
	Всего	В том числе средства выше-стоящих бюджетов	Всего	В том числе средства выше-стоящих бюджетов	Всего	В том числе средства выше-стоящих бюджетов
Управление культуры Администрации г.о. Сызрань	1 012 781	88 714	945 471	27 529	93,4	31,0
Мероприятия в установленной сфере деятельности	10		10		100,0	
Мероприятия в установленной сфере деятельности	15 199		15 198		100,0	
Мероприятия на обеспечение деятельности органов местного самоуправления в сфере культуры	15 199		15 198		100,0	
Закупка товаров, работ и услуг для обеспечения государственных (муниципальных) нужд	15 199		15 198		100,0	
Иные закупки товаров, работ и услуг для обеспечения государственных (муниципальных) нужд	15 199		15 198		100,0	

Приложение В

Отчет об исполнении бюджета Управления культуры Администрации г.о. Сызрань за 2021 год

Таблица В.1 - Отчет об исполнении бюджета Управления культуры Администрации г.о. Сызрань за 2019 год

Наименование главного распорядителя средств бюджета, раздела, подраздела, целевой статьи, вида расходов бюджета городского округа	Утвержденный план		Кассовое исполнение		% исполнения	
	Всего	В том числе средства выше-стоящих бюджетов	Всего	В том числе средства выше-стоящих бюджетов	Всего	В том числе средства выше-стоящих бюджетов
Управления культуры Администрации г.о. Сызрань	1 040 597	55 063	1 038 020	55 000	99,8	99,9
Мероприятия в установленной сфере деятельности	74		74		100,0	
Мероприятия на обеспечение деятельности органов местного самоуправления в сфере культуры	74		74		100,0	
Закупка товаров, работ и услуг для обеспечения государственных (муниципальных) нужд	74		74		100,0	
Иные закупки товаров, работ и услуг для обеспечения государственных (муниципальных) нужд	74		74		100,0	