Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт экономики, управления и природопользования
кафедра финансов

УТВЕРЖДАЮ
Заведующий кафедрой

_____ И.С. Ферова
подпись
«___» _____2020 г.

ДИПЛОМНАЯ РАБОТА

специальность 38.05.01 «Экономическая безопасность»

АНАЛИЗ И ОЦЕНКА ИНФОРМАЦИОННОЙ СОСТАВЛЯЮЩЕЙ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ БЮДЖЕТНОЙ ОРГАНИЗАЦИИ (НА ПРИМЕРЕ ФГБОУ ВО «СГИИ ИМ. Д. ХВОРОСТОВСКОГО»)

Научный руководитель _____ 12.06.2020 к.э.н., доцент_____ Ю.А. Назарова
подпись, дата должность, ученая степень

Выпускник _____ А.Д. Прутовых

Рецензент _____ 12.06.2020 главный экономист Ю.Д. Величкина
подпись, дата должность, ученая степень (Ф.И.О.)

Красноярск 2020

РЕФЕРАТ

Выпускная квалификационная работа по теме «Анализ и оценка информационной составляющей экономической безопасности бюджетной организации» содержит 96 страницы текстового документа, 3 иллюстрации, 16 таблиц, 5 формул, 1 приложение, 50 использованных источников.

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, БЮДЖЕТНАЯ ОРГАНИЗАЦИЯ, ИНФОРМАЦИОННЫЕ РИСКИ, ИНФОРМАЦИОННЫЕ УГРОЗЫ И УЯЗВИМОСТИ, ПЕРСОНАЛЬНЫЕ ДАННЫЕ, КОНФИДЕНЦИАЛЬНОСТЬ, ЦЕЛОСТНОСТЬ, ДОСТУПНОСТЬ.

Предмет исследования – угрозы и уязвимости информационной безопасности бюджетного учреждения на примере ФГБОУ ВО «СГИИ им. Д. Хворостовского».

Объект исследования – информационная безопасность высшего учебного заведения.

Цель данной работы: анализ и оценка информационной безопасности бюджетного учреждения, разработка рекомендаций по минимизации угроз информационной безопасности высшего учебного заведения на примере ФГБОУ ВО «СГИИ им. Д. Хворостовского».

В соответствии с целью были изучены теоретические и методические основы оценки информационной безопасности бюджетной организации, проведена оценка угроз информационной безопасности организации и рассчитан ущерб, который может повлиять на безопасность бюджетного учреждения.

ESSAY

The final qualification work on the topic “Analysis and evaluation of the information component of the economic security of a budget organization” contains 96 pages of a text document, 3 illustrations, 16 tables, 5 formulas, 1 appendix, 50 sources used.

ECONOMIC SECURITY, INFORMATION SECURITY, BUDGETARY ORGANIZATION, INFORMATION RISKS, INFORMATION THREATS AND VULNERABILITIES, PERSONAL DATA, CONFIDENTIALITY, INTEGRITY, AVAILABILITY.

The subject of the study is the threats and vulnerabilities of information security of a budgetary institution as exemplified by the Federal State Budgetary Educational Institution of Higher Education «Dmitri Hvorostovsky Siberian State Academy of Arts»

Object of study - information security of a higher educational institution.

The purpose of this work: analysis and assessment of information security of a budgetary institution, development of recommendations for minimizing threats to information security of a higher educational institution using the example of FSBEI HE «Dmitri Hvorostovsky Siberian State Academy of Arts»

In accordance with the goal, the theoretical and methodological foundations of assessing the information security of a budgetary organization were studied, an assessment of threats to the information security of the organization was carried out, and the damage that could affect the security of a budgetary institution was calculated.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Защита информации – на сегодня это одна из главных задач современного общества. Информация становится одним из ключевых элементов деятельности любой организации, может обладать ценностными характеристиками, является объектом купли и продажи. Процессы, происходящие в финансовой, промышленной, политической или социальной сфере взаимосвязаны теперь с информационными ресурсами и использованием информационных технологий.

В данное время информационные технологии – это неограниченные возможности, которые предоставляют необходимую информацию здесь и сейчас. Важная для предприятия информация должна обладать основными характеристиками: доступностью, целостностью и конфиденциальностью. Однако из-за все возрастающей сложности информационных систем и модернизирующихся информационных технологий увеличивается и число уязвимостей и потенциальных угроз, связанных с информацией.

Сегодня вопросы информационной безопасности актуальны не только для правительственных и коммерческих структур. Вопрос об обеспечении устойчивого функционирования и соответственно повышения информационной безопасности российских вузов стоит остро в связи их коммерциализацией и выходом на международную арену образования.

Из-за сложившейся ситуацией в мире, когда в условиях самоизоляции дистанционное обучение является единственным выходом, требующим при этом подключения дополнительных технико-информационных мощностей, задачи обеспечения защиты информационных ресурсов образовательного учреждения приобретают особую актуальность.

Аппаратно-программные сбои, утечка конфиденциальной информации, кража или порча оборудования - все это угрозы, которые могут нанести ущерб информационной безопасности бюджетной организации. Любое из вышеперечисленных событий является потенциально серьезной причиной остановки функционирования деятельности высшего учебного заведения в

рамках в условиях онлайн обучения, может повлечь за собой значительные финансовые убытки, стать причиной снижения престижа учебного заведения.

Объект исследования – информационная безопасность высшего учебного заведения.

Предмет исследования – угрозы и уязвимости информационной безопасности бюджетного учреждения на примере ФГБОУ ВО «СГИИ им. Д. Хворостовского».

Цель и задачи исследования. Целью данной работы является анализ и оценка информационной безопасности бюджетного учреждения, разработка рекомендаций по минимизации угроз информационной безопасности высшего учебного заведения на примере ФГБОУ ВО «СГИИ им. Д. Хворостовского».

Для достижения этой цели требуется решить следующие задачи:

1. Рассмотреть теоретические основы экономической и информационной безопасности.

2. Провести анализ методов оценки угроз информационной безопасности бюджетной организации.

3. Разработать для бюджетной организации наиболее подходящий метод оценки информационных угроз.

4. Привести характеристику образовательного учреждения, в том числе необходимо описать фонд информационно-коммуникационных средств организации.

5. Оценить угрозы и рассчитать убытки, связанные влиянием информационных угроз на безопасность бюджетного учреждения.

Методы исследования.

При решении поставленных задач использовались следующие общенаучные методы: анализ, классификация, метод оценивания, системно-структурный метод, сравнительный анализ, метод экспертных оценок.

Работа состоит из трех глав. В первой главе рассматривается теоретическая основа экономической и информационной безопасности, представлена нормативно-правовая база в области регулирования

информационной безопасности, особенности информационной безопасности бюджетных организаций.

Во второй главе приведены актуальные методы оценки рисков информационной безопасности организации, разработан наиболее подходящий метод оценки информационных угроз.

Третья глава включает в себя общую характеристику бюджетной организации «СГИИ им. Д. Хворостовского», качественный анализ оценки рисков и его количественная интерпретация, представлены контрмеры по минимизации рисков, которые обладают значительным влиянием на информационную безопасность организации.

В работе использованы научная и учебная литература, статьи в периодических изданиях и сети Интернет.

1. Теоретические основы исследования информационной составляющей экономической безопасности бюджетной организации

1.1 Экономическая безопасность предприятие: понятие, сущность, составные элементы

Экономическая безопасность – это один из наиболее актуальных и динамично развивающихся разделов науки об экономике, который дает полное представление о проблемах, рисках и угрозах, решающихся обществом на данном этапе социально-экономического и технологического развития.

Экономическая безопасность является одной из важнейших характеристик экономики. Обеспечение безопасного функционирования экономики - обязательное условие для ее конкурентной и устойчивой жизнедеятельности.

Данное понятие образовалось только в двадцатом веке в мировой экономической науке и практике. Сам термин «экономическая безопасность» ввел президент Соединенных Штатов Америки Теодор Рузвельт в 1934 г., при создании Федерального комитета по экономической безопасности, потому как осознавал необходимость определенного государственного участия в экономике страны, отказываясь от классической практики невмешательства в экономическую жизнь.

В СССР «безопасность» отождествлялась с «государственной безопасностью». Законодательно этот термин был закреплен в 1934 г.

В Российской Федерации официальное определение понятия «безопасность» определено Законом Российской Федерации «О безопасности»: «безопасность» - это состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз».

Термин «экономическая безопасность» относительно новое понятие в кругах российских органов управления экономикой. Термин допускает весьма широкую интерпретацию.

Для того чтобы понять и в полной мере осознать значение категории, нужно охарактеризовать само понятие «безопасность» и разобраться в его

сути. Нужда в защите от нежелательных внешних и радикальных внутренних угроз, а также потребность в безопасности – это основополагающая необходимость, как жизни отдельного индивидуума, так и разнообразных объединений людей, общества и государства, например.

Безопасность некоторыми исследователями рассматривается как состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, а ее осуществление формируется при помощи системы отношений различных субъектов общественной жизни, они в свою очередь держатся на силовых, правовых, технических, административных и информационных мерах.

В сегодняшних реалиях выделяется три основных уровня безопасности: общества, государства и личности. Они пересекаются с различными функциональными направлениями безопасности.

Направления представлены: внешней и внутренней безопасностью, государственной безопасностью, военной и экономической безопасностью, продовольственной и экологической безопасностью, транспортной и информационной безопасностью и так далее.

Экономическая безопасность – это одно из наиболее важнейших на сегодняшний момент направлений безопасности. В настоящее время сообщество мировых научных деятелей так и не выработало единого мнения, что конкретно подразумевать под категорией «экономическая безопасность». Часть изыскателей связывают экономическую безопасность с безопасностью международной экономической системы. Они относят к этому понятию такие моменты, как неравномерность развития экономики, увеличение задолженности, рост голода и другие аспекты всемирной нестабильности экономики.

Другие авторы считают главным приоритетом обеспечение условий, способствующих эффективному развитию определенной национальной экономики, со свободным доступом к иностранным источникам энергии и

сырья, стабильность иностранных инвестиций, а также гарантии свободного обмена различными услугами и товарами.

Некоторые ученые-исследователи определяют экономическую безопасность более локально - с точки зрения безопасности конкретного региона, отрасли, организации, личности [5].

Приведу некоторые примеры определений экономической безопасности, сформулированные учеными.

В.К. Сенчагов полагает, что суть экономической безопасности это некое состояние институтов власти и экономики, которое обеспечивает защиту интересов всей нации. Оно направлено на социальное развитие государства в целом, обеспеченность в полном объеме потенциала для обороны государства при неблагоприятных условиях развития внутренних и внешних процессов. «Экономическая безопасность - это не только защищенность национальных интересов, но и готовность, а также способность институтов власти создавать механизмы реализации и защиты этих самых интересов».

А. Колосов определяет экономическую безопасность как состояние защищенности от вредных воздействий и нанесения урона хозяйственной деятельности. По его мнению «безопасность как экономическая категория предполагает поддержание экономики на том уровне развития, который обеспечивал бы нормальную жизнедеятельность населения, в частности, его занятость, возможности дальнейшего экономического роста, поддержание в рабочем состоянии всех систем, необходимых для успешного развития и создания условий жизни населения».

С. Глазьева считает, что экономическая безопасность – «состояние экономики и производительных сил общества с точки зрения возможностей самостоятельного обеспечения устойчивого социально-экономического развития страны, поддержания необходимого уровня национальной безопасности государства, а также должного уровня конкурентоспособности национальной экономики в условиях глобальной конкуренции».

По мнению В. Панькова экономическую безопасность стоит рассматривать с позиции устойчивости и заострять внимание на поддержании определенных характеристик функционирования экономики перед лицом неблагоприятных факторов. Экономическая безопасность по его мнению – «такое состояние экономики, которое характеризуется устойчивостью, (иммунитетом) к воздействию внутренних и внешних факторов, которые способны нарушать нормальное функционирование общественного воспроизводства, подрывающих достигнутый уровень жизни населения и тем самым вызывающих повышенную социальную напряженность, а также угрозу существованию государства».

Н. Гловацкая, С. Лазуренко и Е. Бухвальд считают, что «экономическая безопасность традиционно рассматривается как важнейшая качественная характеристика экономической системы, определяющая ее способность поддерживать нормальные условия жизнедеятельности населения, устойчивое обеспечение ресурсами развития народного хозяйства, а также последовательную реализацию национально-государственных интересов России».

Академик Л. Абалкин определяет в качестве главных составных элементов экономической безопасности: устойчивость и стабильность национальной экономики; полную экономическую независимость; способность к прогрессу и саморазвитию. «Экономическую независимость» по его мнению целесообразно дополнить определенным набором факторов, устанавливающих экономическую зависимость субъектов безопасности друг от друга всех, на всех уровнях - национальном, региональном или отраслевом, на уровне организации, личности и т. д. Три элемента, которые выделил Л. Абалкин, можно определить как наиболее общие точки отсчета, универсальные критерии для полной рациональной оценки состояния экономической безопасности [5].

Экономическая безопасность на макроуровне в большинстве своем рассматривается как существенная характеристика экономической системы, определяющая способность поддерживать приемлемые условия

жизнедеятельности населения, непрерывное снабжение народного хозяйства необходимыми ресурсами, а также последовательную реализацию национально-государственных интересов.

Следует более подробно рассмотреть понятие экономической безопасности предприятия.

Предприятие является одним из основных институтов современной экономики и служит центром трансформации и перераспределения экономических ресурсов между альтернативными возможностями их использования.

Более полное определение понятия «предприятие» – это экономически обособленный субъект хозяйствования, который является звеном общественного производства в виде совокупности производительных сил, бурущую свою основу на внутреннем разделении труда кооперацию».

Понятие экономической безопасности предприятия в федеральном законе «О безопасности» четко не определено. Исследователей – экономистов по-своему интерпретировали данный термин.

По мнению Е. Олейникова «экономическая безопасность предприятия – это состояние наиболее эффективного использования корпоративных ресурсов для предотвращения угроз и для обеспечения стабильного функционирования предприятия в настоящее время и в будущем».

С. Маламедов дает следующее определение термина «экономическая безопасность»: «под экономической безопасностью предпринимательства понимается защищенность ее важнейших интересов от внешних и внутренних угроз, т.е. защита предпринимательства, ее потенциала (кадрового и интеллектуального), технологий, капитала и прибыли, защита информации, которые обеспечены системой мер различного характера (специального правового, информационно-технического, организационного, социального и экономического».

Однако в экономической литературе единого мнения о сущности и содержании понятия до сих пор нет, но существуют несколько подходов к определению экономической безопасности предприятия.

Один из подходов определяет суть экономической безопасности исходя из угроз деятельности предприятия. Это мнение разделяют такие ученые-исследователи как О. Грунин, А. Кашин, В. Романюк, В. Шлыков и многие другие.

А. Козаченко, С. Лекарев, В. Пономарев объясняют понятие экономической безопасности как конкретное состояние экономической системы не ссылаясь на угрозы.

Еще один подход обосновывает экономическую безопасность с позиции обеспечения защиты информации и охраны коммерческой тайны. Это трактование характерно для российских ученых конца 20-го века, таких как А. Шаваева, В. Ярочкина [40].

Для предприятия сущность рассматриваемой категории заключается в обеспечении наилучшего использования ресурсов по защите от различных угроз и реализации условий эффективной и стабильной деятельности.

Основными задачами системы экономической безопасности различных организаций можно выделить следующие:

- обеспечение защиты законных прав и интересов организации и ее сотрудников;

- сбор и анализ данных, также осуществление прогноза развития функционирования организации;

- своевременное определение всевозможных внешних угроз безопасности для организации и ее сотрудников;

- препятствие проникновению при помощи различных технических средств в преступных целях;

- обеспечение защиты информации, составляющей служебную коммерческую тайну;

- организация охраны зданий, сооружений, территории, транспортных средств и т. д.

Составляющие экономической безопасности предприятия – это объединение основных направлений его экономической безопасности, которые отличаются друг от друга по внутреннему содержанию.

Выделяются следующие составляющие экономической безопасности организации [42]:

– финансовую;

– политико-правовую;

– интеллектуальную и кадровую;

– силовую;

– экологическую;

– технико-технологическую;

– информационную.

Следует раскрыть подробнее эти составляющие.

Финансовая безопасность рассматривает и регулирует вопросы финансово-экономической состоятельности предприятия, устойчивости к банкротству, определяет параметры платежеспособности, ликвидности и другие «денежные» характеристики.

Политико-правовая безопасность подразумевает всестороннее юридическое обеспечение деятельности предприятия, грамотную правовую работу с контрагентами и государственными структурами, решение любых других правовых вопросов.

В качестве еще одной составляющей выделяют кадровую и интеллектуальную. Данная составляющая в качестве процесса может предотвратить негативное воздействий на экономическую безопасность за счет снижения рисков и угроз, связанных с персоналом, его интеллектуальным потенциалом.

Силовая безопасность занимается режимами, охраной объектов и личной охраной руководства, противодействием преступности, взаимодействием с правоохранительными и другими государственными органами.

Экологическая составляющая предусматривает необходимость рационального потребления природных ресурсов организацией, разработку инновационных технологий предприятия, наносящих минимальный вред экологии. Такое использование должно быть ориентированно на развитии гармонии между хозяйственной деятельностью человека и требованием сохранения окружающей среды.

Технико-технологическая безопасность предполагает создание и использование такой технической базы, оборудования, основных средств производства, технологий и бизнес процессов, которые усиливают конкурентоспособность предприятия информативную защищенность от внешних и внутренних угроз.

Информационная безопасность - это не только защита собственной информации (в том числе конфиденциальной), но это и деловая разведка, информационно-аналитическая работа с внешними и внутренними субъектами. Главной целью абсолютно любой системы информационной безопасности является обеспечение прочного функционирования объекта, устранение информационных угроз - разглашения, утечки, истребления и искажения информации.

Информационная составляющая экономической безопасности предполагает такой порядок взаимообмена экономическими, социальными, научно-техническими и иными сведениями внутри организации и вовне, при котором будет гарантироваться надлежащая сохранность предоставляемой информации, и соблюдена конфиденциальность в интересах государства, общества и хозяйствующего субъекта.

1.2 Информационная безопасность организации: понятие и сущность

Современное общество сейчас смело можно назвать информационным. При помощи развития средств информационно-вычислительной техники и связи теперь позволяет собирать, хранить, обрабатывать и передавать информацию любых объемах, очень оперативно.

Благодаря информационным технологиям деятельность человека, его общение расширяются из-за использования знаний, опыта, которые были выработаны мировой цивилизацией, к которым сейчас все имеют свободный доступ. Сама экономика в настоящее время определяется и как производство материальных благ и как распространение различных информационных и технических услуг и продуктов.

Информатизация в настоящее время связана с использованием современной вычислительной техники, информационно-телекоммуникационных систем, создания информационно-телекоммуникационных сетей. Из-за этого возникает необходимость в разработке, в том числе нового программного обеспечения и применении инновационных решений в информационной сфере.

На определенном этапе развития информационной сферы создается единое безграничное информационное пространство, в котором большинство занято производством, хранением, переработкой и реализацией информации, т.е. интеллектуальным трудом, направленным на развитие мыслительного потенциала и получение знаний.

Создание информационной среды опирается на самые новые и эффективные информационные, телекоммуникационные технологии и технологии связи. Это привело к сильному распространению информационных и телекоммуникационных сетей для информационного обмена на международном уровне. Создание информационного общества это создание информационного пространства во всем мире и для всего мира.

Информационное пространство - направление деятельности человека, которое связано с созданием, переработкой и получением информации, которое

включает в себя индивидуальное и коллективное сознание; информационную базу, а также саму информацию и ее потоки.

Развитие информационных технологий влечет за собой уязвимость любого общества, так как все время появляются все новые и новые риски и угрозы, из за этого возникает необходимость постоянно их предусматривать и предотвращать. Постоянно возникающие экономические войны, которые в настоящее время становятся убыточными и очень опасными из за слияния экономик различных государств, кроме того существующий межу государствами военный конфликт может привести к реальному исчезновению всего живого на земле, война становится информационной.

Информационная война имеет основную цель – нанесение ущерба важнейшим политическим и социальным структурам, а также приводит к дестабилизации всего общества [7].

Информационная война это своего рода соперничество между государствами, реализуемое посредством оказания воздействия при помощи определенной информации на системы властно-военной инфраструктуры другого государства, на его народ в целом, на его СМИ.

Информационная преступность - проведение информационных мероприятий, носящих манипуляционный характер, на информационную сферу в противоправных целях. Одним из видов информационной преступности будет являться информационный терроризм, который проводится в политических целях.

Информационное воздействие – это воздействие, которое осуществляется с применением, так называемого информационного оружия.

Информационное оружие – это совокупность информационных, технических и других средств, технологий и различных методов, которые направлены на:

- осуществление контроля над информационной сферой врага;

- осуществление помех в работе его систем связи и информационных сетей для разрушения их работоспособности, или даже выведения из строя,

искажения содержащейся информации или целенаправленного внесения определенной вредоносной информации;

- распространение определенной целевой информации и дезинформации в системе формирования принятия решений и общественного мнения;

- влияние, оказываемое на психику и сознание государственной и военной власти, на жителей страны - врага, которые применяются для достижения ослабления или влияния различных информационных манипуляций с другой стороны.

В настоящее время из за быстрого развития информационных технологий возникает потребность в более глубоком изучении проблем информационной безопасности: различных мер защиты и средств защиты информации, изучении угроз для содержащих информацию ресурсов, уязвимостей в защитных системах.

Информационная безопасность - это состояние защищенности информационных ресурсов (информационной среды) от внутренних и внешних угроз, способных нанести ущерб интересам личности, общества, государства (национальным интересам).

Безопасность информации - защищенность информации от нежелательного (для соответствующих субъектов информационных отношений) ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования.

Из определений «информационная безопасность» и «безопасность информации» вытекает, что защита информации направлена на обеспечение безопасности информации, безопасность информации обеспечивается с помощью ее защиты.

Информационная безопасность включает[7]:

- защищенность информационной инфраструктуры, формируемой и развивающейся в интересах государства, организаций и граждан;

- информационное пространство, в котором информация используется только в определенном ракурсе и не оказывает вредного влияния при ее использовании;

- информацию, которая в полной мере обладает такими свойствами, как (получение требуемой информационной услуги за короткое время), целостность (достоверность информации, ее защита от несанкционированного доступа, искажения и разрушения), конфиденциальность (защищенность информации от неправомерного с ней ознакомления);

- структуру менеджмента в сфере экономики, системы сбора, использования, обработки и хранения информации в интересах управления организационными структурами, системы прогнозирования и анализа развития организации, системы ее управления, принятия оперативных и грамотных решений, а также осуществления координации действий при наступлении различных чрезвычайных ситуаций и введении режимов полной готовности;

- базы данных различных банков и объединений, информационные и телекоммуникационные сети, а также системы финансовых расчетов и финансового обмена.

Если рассматривать более широко понятие информационная безопасность, можно определить, что это невозможность наносить ущерб объекту безопасности, его свойствам, обусловливаемым информацией и информационной инфраструктурой (рисунок 1).

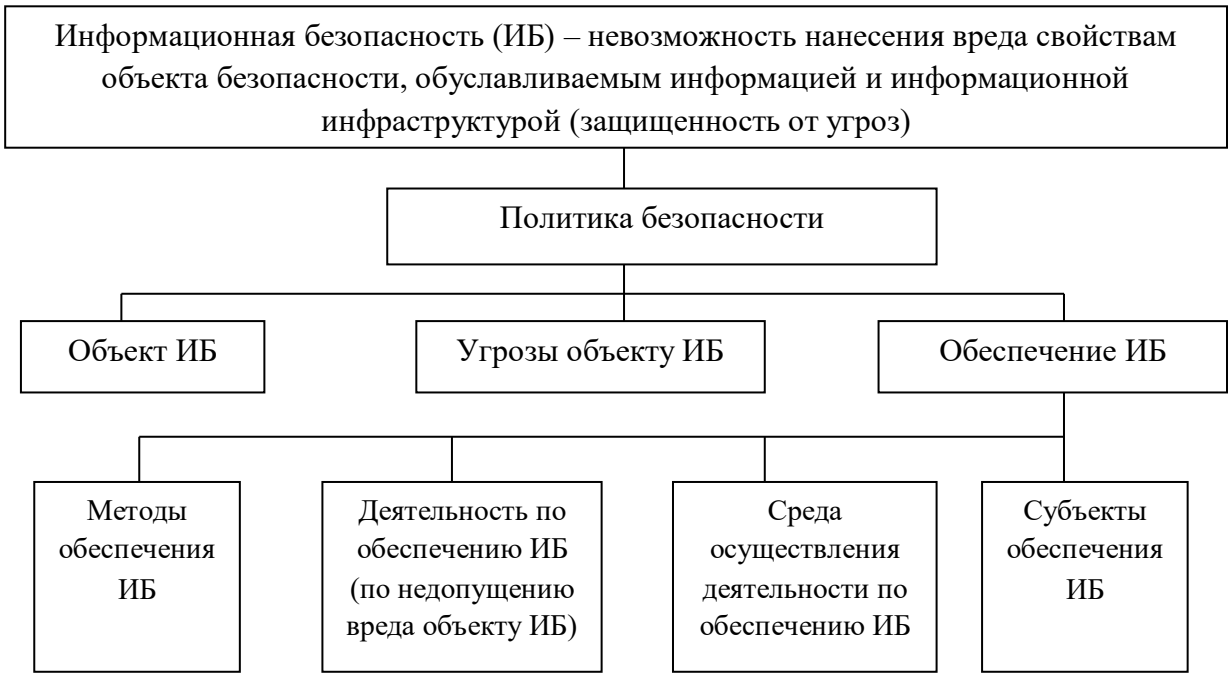

Рисунок 1 – Система понятия «Информационная безопасность»

Информационная безопасность это:

- надежность и неуязвимость работы ПК;

- полная сохранность ценных и важных данных;

- защита информации от внесения в нее искажений, изменений злоумышленниками;

- полная сохранность тайны передачи информации посредством переписки в различных системах электронной связи.

Объекты информационной безопасности в организации:

- различные информационные ресурсы, информационные базы и содержащие на них сведения, которые могут содержать коммерческую или служебную тайну и иную конфиденциальную информацию;

- системы и средства информатизации - средства информационно-коммуникационной техники, сети и системы, разнообразное программное

обеспечение, системы связи и передачи данных, технические средства сбора, обработки, хранения, передачи информации.

При функционировании какой либо организации или предприятия существует такая информация, утечка которой может повлиять на их доходность, также повлечь определенные убытки или последующее недоверие со стороны контрагентов, например. В любом государстве существует информация, которая может повлиять на снижение эффективности осуществляемой государством политики при ее раскрытии. Доступ к этой информации должен быть минимизирован и ограничен конкретным перечнем строго определенных лиц, в целях предупреждения возможности уничтожения, искажения и прочих воздействий на такую информацию. В таком случае объектом безопасности является режим доступа к такой информации, а информационная безопасность опосредована невозможностью нарушения этого режима. Как пример можно рассмотреть информационно-телекоммуникационные системы и средства связи, используемые для передачи сведений, которые составляют государственную тайну. Структура обеспечения безопасности информации включает следующие составные части:

- безопасность коммуникаций;
- компьютерная безопасность;
- безопасное программное обеспечение;
- безопасность данных.

Сочетание различных административных и технологических мер, применяемых при доступе к средствам, содержащим информацию (компьютерам), помогают обеспечить компьютерную безопасность, при сохранении ее недоступности широкому кругу лиц, конфиденциальности целостности информации [7].

Безопасность содержащихся данных обеспечивается при помощи защиты от умышленных, случайных, анонимных (неавторизованных) действий.

Предотвращение предоставления информации, которая может стать доступной в ответ на конкретный запрос анонимным (неавторизованным)

пользователям, обеспечивается соответствующими мерами для безопасности коммуникаций.

Политика безопасности – это синтез анализа возможных угроз и выбора соответствующих мер противодействия им (совокупностью определенных норм и правил поведения, используемым определенной организацией при обработке и защите информации).

1.3 Информационные угрозы: понятие, виды, способы защиты

Угроза безопасности информации – это определенное действие или событие, которое может послужить для искажения, неразрешенного использования, или даже разрушения информации, а также программного обеспечения и технических средств, ее содержащих.

Угроза — это фактор, стремящийся нарушить работу системы.

В настоящее время известен огромный перечень угроз информационной безопасности, в котором можно насчитать более двух ста видов.

Для защищаемой системы составляют не полный перечень угроз, а перечень классов угроз, определяемых по ряду базовых признаков. Это связано с тем, что описать полное множество угроз невозможно из-за большого количества факторов, влияющих на информацию.

Например, можно предложить классифицировать угрозы по следующим признакам:

1. Природа возникновения: естественные угрозы (связанные с природными процессами) и искусственные (вызванные деятельностью человека).

2. Степень намерения проявления: случайные или преднамеренные

3. Источник угроз: природная среда, человек, санкционированные программно-аппаратные средства, несанкционированные программно-аппаратные средства.

4. Положение источника угроз: в пределах или вне контролируемой зоны.

5. Зависимость от активности системы: проявляются только в процессе обработки данных или в любое время.

6. Степень воздействия на систему: пассивные, активные (вносят изменения в структуру и содержание системы).

7. Этап доступа к ресурсам: на этапе доступа, после получения доступа.

8. Способ доступа к ресурсам: стандартный, нестандартный.

9. Место расположения информации: внешние носители, оперативная память, линии связи, устройства ввода-вывода.

Вне зависимости от конкретных видов угроз целесообразно связать угрозы с основными свойствами защищаемой информации.

Так, для информационных систем было предложено рассматривать три основных вида угроз.

Угроза нарушения конфиденциальности реализуется, если информация становится известной лицу, не располагающему полномочиями доступа к ней. Эта угроза имеет место в том случае, когда получен доступ к некоторой секретной информации. Нередко в данном случае используют понятие «утечка».

Угроза нарушения целостности реализуется при несанкционированном изменении данных. Когда информация преднамеренно изменена злоумышленником, считается что целостность информации в таком случае, нарушена. Целостность нарушается и в случае случайной ошибки программного или технического обеспечения. В случаях, когда изменения произведены уполномоченными на то лицами с определенной целью – они являются санкционированными.

Угроза нарушения доступности осуществляется из-за совершения преднамеренных действий, которые совершает злоумышленник или другой пользователь, блокируя доступ к определенному ресурсу информационной системы. Данное блокирование может быть временным (может быть задержка в его получении) или даже постоянным (никогда не будет найден, получен) [7].

Однако на сегодняшний день существует много различных способов защиты от множества информационных угроз.

Защита информации – это совокупность определенных мероприятий, которые направлены на функционирование важнейших составляющих информационной безопасности: ее доступности, целостности, конфиденциальности информации и ресурсов ее содержащих, а также ресурсов, которые используются для обработки, хранения и передачи данных.

Основные предметные направления защиты – это охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности.

Режим защиты информации определяется для:

- сведений, которые относятся к государственной тайне;
- конфиденциальной информации;
- персональных данных.

Система безопасности это определенный комплекс взаимодействия специальных органов и служб, использования специальных средств, методов и мероприятий, которые обеспечивают защиту интересов государства, организации, а также личности, от внешних и внутренних угроз.

Существуют определенные требования к защите информации с точки зрения системного подхода:

- осуществление более рациональных способов и методов, способствующих совершенствованию и развитию системы защиты, непрерывный контроль за состоянием этой защиты, поиск и выявление слабых или проблемных мест, а также предотвращение деятельности, содержащей признаки противоправности;
- использование всех средств защиты, имеющихся во всех структурных элементах системы экономики и на всех этапах обработки информации;
- разработка каждым структурным подразделением в пределах своей компетенции планов по защите информации в определенной организации;

- защищаются только конкретные данные, утрата которых может причинить организации определенный ущерб;

- средства защиты и ее методы должны быть надежными и препятствовать возможным путям неправомерного доступа к охраняемой секретной информации;

- эффективность защиты – средства, затраченные на осуществление защиты информации должны быть меньше чем возможные потери от осуществления информационных угроз;

- строгое разграничение полномочий и прав лиц, имеющих доступ к определенным видам информации;

- допуск к предоставлению определенных ограниченных полномочий, которые необходимы пользователю для выполнения деятельности;

- приведение к минимальному числу общих для нескольких пользователей средств, используемых для защиты информации;

- ведение строго учета случаев и попыток несанкционированного доступа к информации, носящей конфиденциальный характер;

- контроль за целостностью средств защиты информации и незамедлительное реагирование при их поломке.

Система защиты информации должна быть обеспечена с разных сторон для выполнения своей функции.

Исходя из этого система защиты информации имеет:

- различные нормативные акты, положения, инструкции, руководства - обязательные для исполнения (правовое обеспечение);

- обязательные регламенты и нормы функционирования органов и служб, которые реализуют деятельность по защите информации, методики и рекомендации, для обеспечения деятельности при выполнении своей работы (нормативно-методическое обеспечение);

- наличие определенных структурных подразделений и служб, которые осуществляют защиту информации (организационное обеспечение);

- использование различных технических устройств для защиты информации и осуществления функционирования самой системы защиты информации (аппаратное обеспечение);

- различные файлы, показатели, которые используются для решения задач, реализующих деятельность системы (информационное обеспечение);

- антивирусы и прочие программы, которые несут защитные и другие задачи (программное обеспечение);

- математические методы для различных подсчетов, которые применяются при оценке опасности возможных угроз (математическое обеспечение).

1.4 Законодательная и нормативно-правовая база в области обеспечения информационной безопасности организации

Обеспечение информационной безопасности является необходимым фактором для существования и развития любой организации.

Во многих странах на сегодняшний день существуют и на законодательном уровне утверждены национальные программы по обеспечению безопасности в сфере информационно-коммуникационных технологий. В России также утверждены и приняты на государственном и ведомственном уровнях руководящие документы, которые определяют систему информационной безопасности [17]:

- «Доктрина информационной безопасности Российской Федерации», утвержденная Президентом РФ 5 декабря 2016 г., определяет термин информационной безопасности как одну из важных составляющих национальной безопасности и рассматривает ее как «состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства» [19].

- Закон «Об информации, информационных технологиях и защите информации» № 149-ФЗ от 27.07.2006 г. регулирует отношения, которые возникающих вследствие:

1) осуществления права на поиск, получения, передачи, производства и распространения информации;

2) применения информационных технологий;

3) обеспечения защиты информации.

Кроме того в этот закон дает определение информации как сведения «о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления». Под информационной безопасностью понимается «состояние защищенности интересов (целей) организации в условиях угроз в информационной сфере». Информационная сфера трактуется как «совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение, хранение и использование информации, а также системы регулирования возникающих при этом отношений» [25].

- В Законе «О государственной тайне» № 5485-1 от 6 ноября 1997 г. регулируются отношения, возникающие из-за отнесения сведений к государственной тайне, их засекречивание или рассекречивание, а также их защиты в целях обеспечения безопасности России.

- Закон «О коммерческой тайне» N 98 - ФЗ от 29 июля 2004 г. регулирует отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации, охраной ее конфиденциальности в целях обеспечения баланса интересов обладателей информации, составляющей коммерческую тайну, и других участников регулируемых отношений, в том числе государства, на рынке товаров, работ, услуг и предупреждения недобросовестной конкуренции, а также определяет сведения, которые не могут составлять коммерческую тайну.

- Закон «О персональных данных» № 152-ФЗ от 27.07.2006 г. регулирует отношения, связанные с обработкой персональных данных, осуществляемой

государственными органами, юридическими лицами, физическими лицами с использованием средств автоматизации или без использования таких средств.

- Закон «О техническом регулировании» № 184-ФЗ от 27 декабря 2002 г. определяет такие понятия как «стандартизация», «технический регламент», «оценка соответствия» и др.; а также регламентирует положение о добровольности (рекомендуемости) применения стандарта, выводя его из разряда обязательных; данный Закон кроме того определяет «технический регламент» как «совокупность минимально необходимых, обязательных требований к процессам, продуктам, услугам и т. д. в части обеспечения безопасности их функционирования и применения» [28].

В ведущих странах мира по инициативе Международной организации по стандартизации (ISO) действуют международные и национальные стандарты нового поколения в сфере информационной безопасности, которые учитывают состояние информационных технологий в настоящее время и рассматривают практические вопросы устройства системы информационной безопасности в организациях. В настоящее время в Российской Федерации развитие современных информационно-телекоммуникационных технологий в значительной мере опережают разработку нормативной документации, регламентирующей эту сферу деятельности. Из-за этого большинство современных российских компаний стало руководствоваться международным стандартам и методическим рекомендациям, которые были разработаны в других странах. Вот некоторые из них.

1. Международный стандарт ISO/IEC 15408-1:2009 "Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model" - "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель".

В этом стандарте регламентированы общие принципы и модель оценки безопасности информационных и коммуникационных технологий, а также содержится руководство по определению специфических целей безопасности и

характеристике организации компонентов всей модели. Кроме того, в данном стандарте определяются основные понятия информационной защиты [31].

В 2013 г. Федеральной службой технического и экспортного контроля (ФСТЭК) был утвержден ГОСТ ИСО/МЭК 15408-1-2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» на основе прямого применения международного стандарта ISO/IEC 15408-1:2009.

Данный стандарт предоставляет единые требования к функциональным возможностям безопасности продуктов информационных технологий и мерам доверия, применяемым к этим продуктам при оценке безопасности, этот стандарт может быть использован для руководства при разработке, оценке или приобретении информационных продуктов, которые содержат элементы осуществления деятельности по безопасности. В ИСО/МЭК 15408 допускает применение множества различных методов оценки по отношению к свойствам безопасности продуктов информационных и коммуникационных технологий.

2. Международный стандарт ISO/IEC 27001-2013 «Information Technology. Security techniques. Information security management systems. Requirements» - «Информационные технологии. Методы обеспечения безопасности. Требования к системе управления информационной безопасностью». В данном стандарте определены требования к системе управления ИБ (СУИБ), в том числе общую методологию создания, внедрения, и оценки эффективности механизмов СУИБ. Данный стандарт - своего рода модель системы управления в системе информационной безопасности, основанной на определенном подходе к разработке, эксплуатации, анализу и мониторингу, а также сопровождению СУИБ организации. Кроме того этот стандарт приводит определенные механизмы защиты информации[31].

3. В международном стандарте ISO/IEC 27002:2013 «Information technology. Security Techniques. Code of practice for information security controls» - «Информационная технология - Методы защиты - Практическое руководство

по контролю информационной безопасности» определены основные принципы для формирования собственных стандартов информационной безопасности организации и практики управления информационной безопасностью, в том числе выбор, внедрение и управление средствами контроля, с учетом среды риска информационной безопасности организации.

Этот стандарт предназначен организаций, которые хотят:

- выбрать средства управления в процессе внедрения системы управления информационной безопасностью на основе ISO / IEC 27001;

- внедрить общепринятые средства контроля информационной безопасности;

- разработать собственные руководящие принципы управления информационной безопасностью.

4. ISO/IEC 19791:2010 «Information technology - Security techniques - Security assessment of operational systems» - «Информационные технологии. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем» - этот стандарт является расширением стандарта ISO/IEC 15408, дополняющим функциональные требования безопасности и требования доверия, относящиеся к процедурному и административному уровням информационной безопасности и рассмотрению всех этапов жизненного цикла информационных систем. Стандарт определяет структуру информационной системы на домены с различными рисками, требованиями и разной политикой безопасности, что необходимо для осуществления оценки безопасности информационных систем [31].

В целом, перечисленные ранее законы и стандарты носят регламентирующий характер и образуют нормативно правовую базу создания комплексных систем защиты информации для организаций. Вместе с тем, в них нет каких либо определенных конкретных рекомендаций к выбору требований к таким системам, наличию необходимых технических средств и организационным мерам по защите информации в организации, так как это

определяется исключительно спецификой объекта защиты информации и условиями его функционирования.

1.5 Особенности информационной безопасности бюджетной организации

Защита информации в бюджетной сфере является довольно специфической, очень важной деятельностью. Особенность ее заключается в защите информации, возникающей в процессе оказания и предоставления государственных услуг. С точки зрения оправданности тех или иных затрат, которые направленны на защиту информации существует единое мнение – траты на защиту информации всегда направлены на уменьшение возможного риска ее потери и понесенного вследствие этого ущерба.

Информационная безопасность образовательного учреждения — это функционирование информационной системы вуза в рамках действующего законодательства, обеспечивающее его независимость, целостность и устойчивое развитие, а также защищенность от воздействия внешних и внутренних угроз.

Управление информационной безопасностью образовательного учреждения должно быть основано на принципах инновационного развития. Именно оно способно сохранять динамическое равновесие, успешно реагировать посредством определенных механизмов на изменяющиеся условия, в том числе эффективно преодолевать кризисные ситуации.

Информационная безопасность должна обладать способностью быстрого реагирования на угрозы, которые нарушают стабильность и равновесие информационной системы, необходимо своевременно противостоять этим угрозам, обеспечивая эффективное и бесперебойное функционирование.

В последнее время степень информатизации учреждений образования сильно возросла. Информационной техникой в России располагают все 100% образовательных организаций. Весьма активно используются сетевые технологии: все образовательные организации имеют локальные сети, все они

должны быть подключены к информационно-телекоммуникационной сети «Интернет», в соответствии с требованиями к образовательным организациям все учебные заведения должны иметь свои вебсайты. Особенно актуально это сейчас, в условиях сложной эпидемиологической обстановки в мире, и ведения образовательного процесса исключительно посредством использования современных средств информационно-коммуникационных технологий.

Возникшая необходимость образовательных организаций использовать информационные технологии в таком объеме позволяет думать, что одним из важнейших для образовательной системы является повышение эффективности управления информационной системы образовательной организации.

В настоящее время можно говорить о резком росте сложности информационных инфраструктур, поддержание которых становится все труднее и труднее. Информационные мощности образовательных организаций увеличиваются с каждым годом, следовательно, и количество информационных данных, хранящихся в информационной системе вуза многократно, возрастает.

В рамках осуществления деятельности по обеспечению информационной безопасности вузы постоянно осуществляют:

- несанкционированный доступ к информации и передачи ее лицам, не имеющим права на доступ к ней;

- своевременное обнаружение фактов несанкционированного доступа к информации;

- предупреждение возможных негативных последствий из-за нарушения порядка доступа к информации;

- недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

- возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа;

- контроль обеспечения уровня защищенности информации, осуществляемый на постоянной основе;

- ежедневное автоматическое создание резервных копий баз данных на серверах образовательных организаций.

Кроме того, помимо ведения образовательного процесса посредством дистанционных информационных технологий, особую роль в информационной безопасности образовательных учреждений стоит отвести так называемым «госзакупкам». А именно информационной безопасности государственных информационных систем, которые создаются с учетом требований, предусмотренных Федеральным законом от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» [44].

Согласно положениям ч. 9 ст. 24.1 федерального закона № 44-ФЗ «оператор электронной площадки, оператор специализированной электронной площадки обязаны обеспечить конфиденциальность информации об участнике такой закупки, направившем указанные информацию и электронные документы». Так же согласно ч. 12 ст. 24.1 того же закона «информация и документы, связанные с проведением электронных процедур, закрытых электронных процедур и полученные или направленные оператором электронной площадки хранятся в соответствии с требованиями, установленными в соответствии с ч. 2 настоящей статьи» [44].

Существует ряд угроз, которые могут навредить информационной безопасности образовательного учреждения в области закупок товаров, работ, услуг для государственных и муниципальных нужд.

Во-первых, потенциальную угрозу несут сами сотрудники. Они могут случайно и намеренно передать сведения об участии организации в торгах конкурентным организациям. Таким образом, известной окажется очень важная информация, например, цена заявки на участие в конкурсе. Это впоследствии может негативно сказаться на организации, сведения которой стали доступны третьим лицам.

Вторая группа угроз - конкуренты. Любая информация об участии в какой-либо закупке может дать определенное преимущество сторонним

организациям. И чем больше деталей они знают, тем больше у них преимуществ.

Если речь идет о тендерах на крупные суммы, не стоит недооценивать возможную недобросовестную конкуренцию с вовлечением “третьих лиц“ для оказания давления на организацию. И цель таких действий проста - ограничить участие в торгах.

Третья группа – контролирующие и надзорные органы. Был такой пример, когда против одного из чиновников организации государственного заказчика проводили расследование по подозрению в коррупции. Нередкой практикой в подобных делах является следственная проверка основных подрядчиков, в том числе обыски с изъятием компьютеров и необходимой документации.

В четвертую группу угроз входят общественные организации, активисты, средства массовой информации. Некоторые из представителей данных категорий желают сделать себе имя на создании провокационных историй, участником которых вряд ли хотела бы стать любая организация, которая ценит свою деловую репутацию и имидж.

Вышеперечисленные риски вполне реальны. И существует прямая закономерность – чем выше стоимость контрактов, за которые соревнуется организация на рынке «госзакупок», тем выше вероятность того, что найдутся те, кто будет мешать в их получении.

Вопрос реализации политики информационной безопасности в образовательных организациях остаётся актуальным, так как информационные системы охватывают новые сферы образовательной деятельности, а безопасность и защита информации всегда нуждается в доработке, контроле и постоянном мониторинге.

2. Методы и средства обеспечения информационной составляющей экономической безопасности бюджетных организаций

2.1 Методика определения уровня защищенности персональных данных в информационных системах персональных данных

В образовательных организациях обработка персональных данных осуществляется с использованием информационных систем. Для соответствия законодательству Российской Федерации в области защиты персональных данных необходимо обеспечивать их безопасность.

В соответствии с требованиями Закона о персональных данных выбор мер для защиты осуществляется в соответствии с устанавливаемым уровнем защищенности для каждой из информационных систем. Порядок установления такого уровня определен в Требованиях к защите персональных данных при их обработке в информационных системах персональных данных, которые утверждены Постановлением Правительства Российской Федерации от 01.11.2012 № 1119.

Уровень защищенности данных при их обработке зависит от категории, количества обрабатываемых субъектов, определенного типа актуальных угроз безопасности.

Существуют разные категории данных, подлежащих обработке.

Специальными называются те персональные данные, которые касаются расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, личной жизни субъектов.

Существует еще категория биометрических персональных данных. Это такие сведения, которые характеризуют физиологические и биологические особенности субъекта персональных данных, на их основании можно установить личность, оператором они используются для идентификации субъекта персональных данных.

Также персональные данные могут быть общедоступными. Они находятся в общедоступных источниках.

Еще персональные данные могут носить статус иных, если данные которые обрабатываются информационной системой не относятся ни к специальным, ни к биометрическим или общедоступным.

По типу информационная система может быть обрабатывающей персональные данные сотрудников либо обрабатывающей персональные данные субъектов, которые не являются таковыми.

По количеству обрабатываемых субъектов требованиями к защите при их обработке определенно два значения:

1) обработка персональных данных менее 100 000 субъектов;

2) обработка персональных данных более 100 000 субъектов.

Также для установления уровня защищенности персональных данных следует учитывать тип актуальных угроз, наносящих вред информационной системе.

Существуют следующие типы актуальных угроз:

1) угрозы 1-го типа связанны с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, которое используется информационной системой;

2) угрозы 2-го типа связанны с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе;

3) угрозы 3-го типа не связанны с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении.

Установление уровня защищенности для каждой информационной системы осуществляется в соответствии с «Требованиями к защите персональных данных…», ниже представлен пошаговый алгоритм его определения.

Первый шаг состоит в необходимости установить категории персональных данных, обрабатываемых в информационных системах. Мы

определяем, какие персональные данные отнесем к специальным, какие - к биометрическим, какие - к общедоступным, а какие, вообще - к иным

Второй шаг - это определение типа субъектов персональных данных. На данном этапе необходимо установить является субъект сотрудником образовательной организации или нет. Если в информационных системах одновременно обрабатываются данные сотрудников образовательной организации и субъектов, не являющихся работниками данного учреждения, то устанавливается тип «Субъект персональных данных, не являющийся сотрудником образовательной организации».

Третьим шагом необходимо определить количество обрабатываемых субъектов. Следует проанализировать обрабатываемое количество субъектов и по результатам получить контрольное значение.

Для выполнения четвертого шага необходимо определить актуальные угрозы безопасности персональных данных, в том числе нужно определить актуальность угроз недекларированных возможностей в прикладном и системном программном обеспечении. В зависимости от этого мы получим одно из следующих значений: 1 тип угроз; 2 тип угроз; 3 тип угроз.

По результатам проведенной аналитической работы определяются уровни защищенности персональных данных в информационной системе. Это все фиксируются Актом установления уровня защищенности персональных данных в информационной системе персональных данных.

2.2 Методы и инструментальные средства анализа и управления рисками информационной безопасности

В соответствии с международным стандартом ISO 27002, анализ угроз - основная задача при определении защищенности уровня информационной безопасности, начальная точка при поддержании эффективного управления системой информационной защиты. Риск же в общем смысле – есть наличие возможности понести негативные последствия в материальном или каком-либо другом виде.

На начальном этапе анализа рисков необходимо обоснование требований, которые предъявляются к уровню защиты информации. На рисунке 2 представлено два основных подхода к организации режима информационной безопасности: минимальные требования и повышенные (рисунок 2).

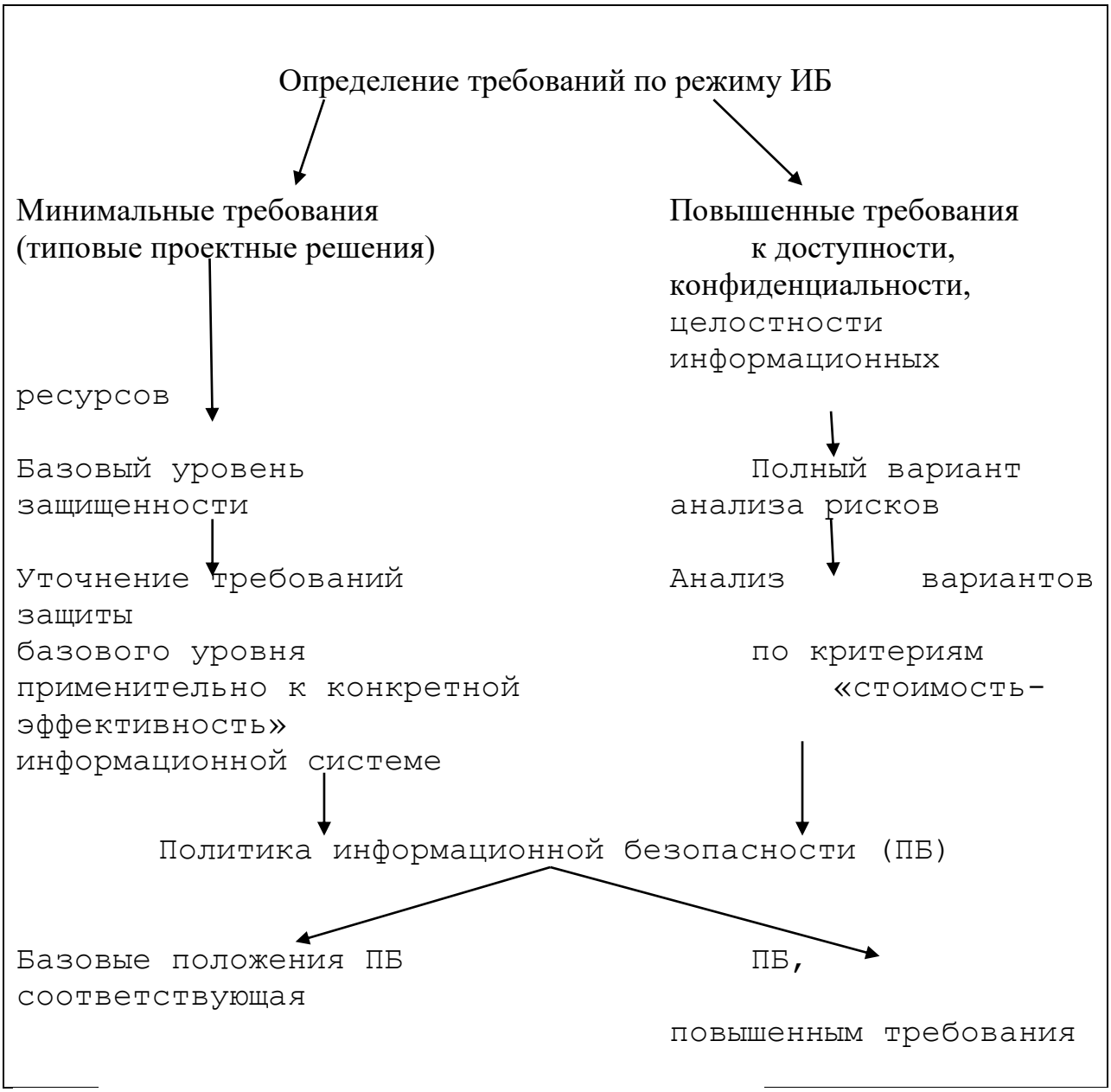

Рисунок 2 – Подходы к организации режима ИБ

При минимальных требованиях рассматривается типовой набор наиболее вероятных угроз, они должны быть нейтрализованы стандартными контрмерами, при этом вероятности их осуществления и уязвимость ресурсов не учитываются.

Повышенные требования устанавливаются в том случае, если угрозы могут привести к очень тяжелым последствиям, следует осуществлять полный набор мероприятий по организации режима информационной безопасности. При этом должны выполняться следующие работы по анализу рисков [17]:

а) определение ценности ресурсов, отнесение их к определенным категориям;

б) определение полного набора угроз;

в) расчет вероятностей угроз;

г) выявление уязвимостей ресурсов;

д) определение потенциального злоумышленника;

е) оценка потенциального ущерба при осуществлении угроз.

На этапе управления рисками определяются возможные подходы к их управлению. Данная информация представлена в таблице 1.

Таблица 1 - Управление информационными рисками

Типы управления риском	Основные мероприятия
Уменьшение риска	Введение контрмер может привести к снижению негативных последствий значимого уровня
Уклонение от риска	Особенностью данного направления является снижение степени влияния риска путем изменения природы или характера угроз, локализация риска, совместное управление риском. Одной из возможных причин уклонения от риска может быть отсутствие варианта реакции компании, способного понизить вероятность наступления или степень негативных последствий.
Изменение характера риска	Компенсация риска (страхование или распределение ущерба между партнерами).
Принятие риска	Отсутствие каких-либо действий, направленных на снижение вероятности и последствий реализации. Причина, по которой используют данный метод, - значительное превышение стоимости работ по снижению влияния риска на компанию по сравнению с последствиями реализации негативного события.

Имеется два основных подхода к измерению риска: по двум и по трем факторам. В первом случае риск – это произведение вероятности неблагоприятного события и тяжести ущерба:

$$R = P \text{соб.} \times r, \quad (1)$$

где R - риск,

P соб. - вероятность наступления неблагоприятного события, вызванного действием угрозы,

r - цена ущерба.

Если режиму предъявлены повышенные требования защиты информации, вероятность наступления неблагоприятного события рассчитывается следующим образом (трех факторная оценка):

$$R = P \text{угр.} \times P \text{уязв.} \times r\,, \qquad (2)$$

где R - риск,

P угр. - вероятность возникновения угрозы;

P уязв. - вероятность успешной реализации угрозы через уязвимость

r - цена ущерба.

Данные выражения можно рассматривать как математические формулы. Однако эти переменные сложно оценить в количественном выражении, они в большей степени отвечают за качественную оценку.

Существует несколько подходов для определения качественной шкалы. Самый распространенный из них – табличный способ с балльной системой оценивания. В таблице 2 приведен пример такого способа оценки риска по трем факторам: вероятность угрозы, вероятность уязвимости, цена ущерба. Угрозы и уязвимости задаются по трех уровневой, ущерб - по пяти уровневой шкалам. Переменные - угрозы и уязвимости - заданы следующим образом: низкая (Н), средняя (С), высокая (В); аналогично определяется цена ущерба r (пренебрежимая, незначительная и т.д.). Риск R принимает одно из следующих 9-ти значений: 0 - отсутствие риска; 1- риском можно пренебречь; 2 - риск очень мал; 3 - незначительный риск; 4 - допустимый риск; 5 - средний риск; 6 - высокий риск; 7 - критический риск; 8 - недопустимый риск.

Такие таблицы используются как в «бумажных» вариантах, так и программных продуктах, которые как раз и предназначены для анализа рисков.

Таблица 2 - Трехфакторная оценка риска

Цена ущерба	Вероятность угрозы								
	низкая			средняя			высокая		
	Вероятность уязвимости			Вероятность уязвимости			Вероятность уязвимости		
	Н	С	В	Н	С	В	Н	С	В
Пренебрежимая	0	1	2	1	2	3	2	3	4
Незначительная	1	2	3	2	3	4	3	4	5
Умеренная	2	3	4	3	4	5	4	5	6
Серьезная	3	4	5	4	5	6	5	6	7
Критическая	4	5	6	5	6	7	6	7	8

Оценка вероятностей угроз и уязвимостей осуществляется с помощью одного из следующих методов:

- метод экспертных оценок (метод поиска результата, полученного на основании использования персонального мнения эксперта или коллективного мнения группы экспертов);

- обработка статистических данных (собираются данные о произошедших событиях, об их частоте, последствиях);

- анкетирование и разного вида опросники (составляется список вопросов, касающихся нужной темы, производится опрос сотрудников, данные собираются, анализ полученных ответов).

Актуальные стандарты и опубликованные в открытой печати корпоративные документы, что относятся к сфере информационной безопасности, носят рекомендательный характер, содержать лишь общие положения по созданию методик оценки уровня защищенности информационной безопасности, а также управлению информационными рисками. Следовательно, задачей каждой компании является разработка собственной методики или же это делает специализированная организация. Эти методики должны учитывать особенности и специфику деятельности предприятия, своеобразность применения информационных технологий и другое.

Анализ рисков можно проводить с помощью «бумажных» методик или же специализированными инструментальными средствами. О первых было упомянуто ранее, поэтому следует более подробно рассмотреть программные обеспечения (далее - ПО), занимающиеся оценкой рисков организации.

Американская компания RiskWatch Inc. разработала методологию анализа и управления рисками RiskWatch. Данное программное обеспечение предназначено для идентификации и оценки уровней угроз, обнаружения уязвимостей, оценки на соответствие требований нормативной базы, прогнозирование размеров возможных потерь и разработки контрмер, позволяющих предотвратить в будущем наступление негативных последствий вследствие реализации актуальных для предприятия угроз. Разработанная методика осуществляет количественный анализ рисков, он позволяет принимать более обоснованные решения по вопросам обеспечения безопасности. Критерием оценки и управления рисками при этом используются ожидаемые годовые потери - Annual Loss Expectancy (ALE) и оценка возврата (окупаемости) инвестиций - Returnon Investment (ROI).

Для выявления возможных уязвимостей используется опросник, который включает более 600 вопросов. С помощью них определяется частота возникновения выделенных угроз, степень уязвимости и ценность ресурсов. Все это используется в дальнейшем для расчета эффекта от внедрения средств защиты. Существуют специализированные версии для правительственных структур и предприятий различных отраслей промышленности, в которых базы знаний по ресурсам, угрозам и контрмерам регулярно обновляются.

Но данный метод не учитывает организационные и административные уровни защиты, анализ осуществляется только на программно-техническом уровне, следовательно, метод не учитывает все аспекты комплексной защиты информации.

Программное обеспечение CRAMM разработано в Великобритании, является наиболее распространенным в использовании при оценке информационной безопасности организации, так как использует комплексный

подход в оценке. На сегодня имеется до 10 версий данной программы: рассчитана на требования армии, государственных учреждений, финансовых структур, частных организаций. Анализ рисков данной программы состоит их 3 последовательных этапов (рисунок 3). Набор исходных данных определяется отдельно для каждого из этапов - последовательность мероприятий, анкеты для проведения опросов, списки проверки и набор выходных документов (отчетов).

На первом этапе осуществляется непосредственно описание самой информационной системы, определяются ее функции, выделяются категории пользователей и персонал, который будет принимать участие в исследовании; происходит идентификация ресурсов информационной системы и определяется их ценность; выявляются все угрозы, уязвимости и оценивается их уровень.

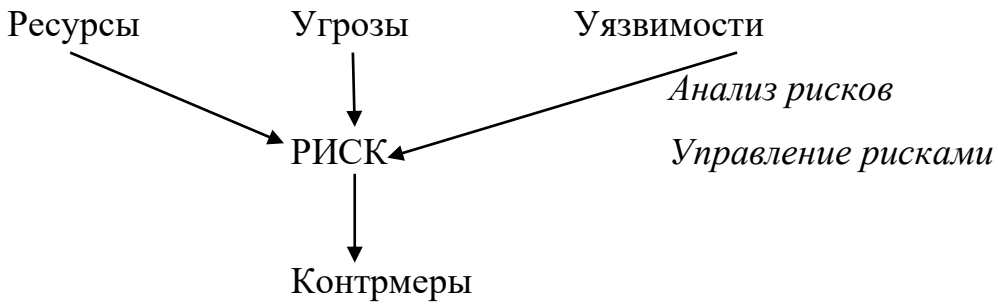

Рисунок 3 - Этапы оценки рисков по методу CRAMM

На втором этапе производится оценка риска с помощью упрощенных методов или осуществляется полный анализ на основе полученных оценок угроз и уязвимостей.

На третьем этапе выбирают целесообразные меры противодействия угрозам. ПО CRAMM обладает обширным каталогом ресурсов (физических, программных и информационных), классов угроз и контрмер, видов возможного материального и нематериального ущерба. Оценка угроз и уязвимостей производится с помощью экспертов или используются результаты исследования косвенных факторов.

Данное ПО детально осуществляет оценку угроз и уязвимостей предлагает контрмеры из собственной обширной базы данных. Однако оценка

рисков является качественной и очень приблизительной, а процесс формирования выходных документов очень трудоемок - общий объем отчета составляет сотни страниц.

Еще один способ, который позволяет построить комплексную систему защиты информации на предприятии, разработан компанией Microsoft. Данная методика включает в себя модель управления рисками информационной безопасности организации. Весь цикл управления рисками можно разделить на четыре основных стадии:

1. Оценка рисков. Здесь происходит планирование сбора данных, обсуждение ключевых условий успешной реализации и подготовка рекомендаций, осуществляется непосредственный сбор информации о рисках и его документирование, описывается последовательность действий по качественной и количественной оценке рисков

2. Поддержка принятия решений. Данная стадия включает в себя определение функциональных требований, выбор подходящих элементов контроля, их проверку на соответствие на соответствие функциональным требованиям, осуществляется оценка снижения рисков, идентифицируются наиболее экономически эффективные решения по минимизации рисков.

3. Реализация контроля. На данном этапе используются элементы контроля, которые могут снизить информационной риск, происходит поиск целостного подхода и осуществляется организация многоуровневой защиты.

4. Оценка эффективности программы включает в себя анализ эффективности процесса управления рисками, проверку выбранных элементов контроля на соответствие необходимому уровню защиты. На этой стадии разрабатываются целые системы показателей рисков, оценивается эффективность программы управления рисками, и выявляются возможности ее улучшения.

Если обобщить, в данной методике на начальном этапе рискам присваивают значения в соответствии со шкалой: «высокий», «существенный», «умеренный» и «незначительный». После выявляются наиболее существенные

риски, производится подсчет финансовых показателей, при необходимости, только потом, при необходимости, проводится количественная оценка – расчет ожидаемого годового ущерба (ALE).

Стоит также отметить программное обеспечение «Microsoft Security Assessment Tool (MSAT)», оно позволяет «оценить уязвимости в ИТ-средах, предоставить список расставленных по приоритетам проблем и список рекомендаций по минимизации этих угроз».

Анализа информационной инфраструктуры происходит с помощью опросника, в котором около 200 вопросов, «охватывающих инфраструктуру, приложения, операции и персонал». Часть вопросов предназначена для определения бизнес-модели компании, на основе полученных ответов создается «профиль бизнес-риска (BRP)». С помощью другой части вопросов составляется список защитных мер, внедренных организацией с течением времени. В комплексе эти меры образуют уровни защиты, а сумма уровней, которая образует объединенную систему глубокой защиты, называется «индексом глубокой защиты (DiDI)». Два этих показателя сравнивают - BPR и DiDI, чтобы проанализировать распределение угроз по областям оценки рисков – инфраструктуре, приложениям, операциям и людям.

В результате анализа предоставляется общая информация о состоянии системы защиты информации предприятия, однако более глубокий анализ конкретных технологий или процессов описываемое средство не осуществляет.

Российская консалтинговая компания в области безопасности информации Digital Security разработала на основе международных и российских стандартов (ISO 15408, ISO 27002, ISO 27001 и др.) два программных продукта - «Гриф» и «Кондор», они позволяют оценить информационные риски организации, учитывая специфику российских реалий.

Анализ рисков с помощью ПО ГРИФ осуществляется путем построения модели информационной системы организации. Для этого анализируются следующая информация:

- весь список ресурсов, на которых хранится ценная информация;

- сетевые группы, в которых находятся ресурсы системы (т.е. физические связи ресурсов друг с другом);

- отделы, к которым относятся ресурсы;

- виды ценной информации и наносимый ущерб для каждого вида;

- бизнес-процессы и информация, которая в них участвует;

- группы пользователей, имеющих доступ к ценной информации;

- класс группы пользователей;

- доступ группы пользователей к информации и его характеристики (вид и права);

- средства защиты информации и рабочего места группы пользователей.

На основе введенных данных происходит построение модели информационной системы, угроз, уязвимостей, злоумышленника, на их основе проводится анализ уровня защищенности каждого вида информации.

Для произведение комплексной оценки вероятностей угроз, уязвимостей и средств защиты вводится шкала от 0 до 100%. С помощью экспертом определяются весовые коэффициенты и ущерб (в рублях или уровнях) по каждому ресурсу и виду информации. Затем рассчитывается риск воздействия угроз (угрозы конфиденциальности, целостности и отказа в обслуживании) для каждого ресурса, каждого вида информации и каждого типа нарушителя. Значение уровня риска варьируется в интервале от 0 до 1.

Также существует раздел - «Политика безопасности», способный оценить эффективность вводимых организационных мер. В нем содержатся вопросы, которые связаны с поведением сотрудников на работе и ряд иных вопросов, затрагивающих эту тему. Ответы на эти вопросы могут влиять на веса средств защиты и изменяют значение риска реализации угроз.

КОНДОР включает в себя систему ГРИФ. Это система разработки и управления политикой безопасности информационной системы. Она описывает такие аспекты управления информационной безопасности, как:

- политика безопасности;

- организационные методы обеспечения информационной безопасности;

- управление ресурсами;
- пользователи информационной системы;
- физическая безопасность;
- управление коммуникациями и процессами;
- контроль доступа;
- приобретение, разработка и сопровождение информационных систем;
- управление инцидентами информационной безопасности;
- управление непрерывностью ведения бизнеса;
- соответствие системы требованиям.

Данное ПО базируется на международных стандартах управления информационной безопасностью и позволяет проанализировать систему на соответствие данным стандартам.

После того, как опрос был полностью осуществлен, и все ответы введены, для дальнейшего анализа в программном обеспечении предусмотрен модуль управления контрмерами. В нем можно идентифицировать, какие положения стандартов были организацией не выполнены. После определения конкретных контрмер можно увидеть соотношение стоимости данных контрмер и величины, на которую изменилось значение критичности невыполненных требований.

Вышеперечисленные программные продукты анализа и управления рисками не обладают достаточной наглядностью («прозрачностью»), имеют в основном качественный характер и сводятся к формальной проверке выполнения или невыполнения требований стандартов информационной безопасности.

Количественная оценка ущерба, который вызван воздействием угроз на информационные и материальные ресурсы, плохо освещена, как правило, оценка этих ресурсов производится только по качественной шкале.

Адаптация методик анализа информационных рисков и их управление к специфике образовательных учреждений, является открытым вопросом для обсуждения. Бизнес-процессы, протекающие в вузе, структура

информационных ресурсов значительно отличаются от характерных процессов для обычной организации. Требуется изучение учебного учреждения в качестве объекта защиты, выявление основных источников его угроз, уязвимостей, защищаемых ценностей и разработки соответствующих методик анализа и управления рисками, предназначенных для повышения информационной безопасности.

2.3 Методика оценки рисков информационной безопасности бюджетной организации

Сегодня перед каждым предприятием, комплексно подходящим к вопросу безопасности своей организации, в том числе и информационной, встает вопрос об организации качественной системы защиты информации. Эффективность защиты зависит от подхода к ее организации и правильного выбора методов расчета рисков информационной безопасности.

В данное время очень важно иметь полное преставление о состоянии информационной безопасности организации, это необходимо для ее бесперебойного функционирования.

Отличительной чертой любого предприятия, осуществляющего свою работу в условиях дистанционного режима, является чувствительность к информационной безопасности, потребность в надежной защите аппаратно-программного комплекса с целью обеспечения непрерывности функционирования ключевых процессов, что просто обязывает руководителей организации создавать и поддерживать эффективную систему информационной безопасности.

Существует множество методик оценки и обработки рисков, которые применимы к любой информационной системе. Однако для грамотного построения системы защиты требуется большой объем информации о реализованных атаках, а также о попытках их реализации. Такая информация подлежит программному анализу с целью выявления наиболее актуальных угроз информационной безопасности. Но не всегда есть возможность

реализовать такое на практике, ввиду ограниченности временных и финансовых ресурсов. Это актуально и для бюджетной организации, так как оценка информационных рисков и угроз является важно, но не ключевой задачей ее функционирования, не всегда вуз обладает достаточным количеством временных или финансовых ресурсов для комплексной и глубокой оценки информационной безопасности.

Данный метод предлагает качественную оценку рисков информационной системы организации с расчетом материального ущерба в случае реализации угроз Он не требует финансовых затрат, большого количества времени и специальной профессиональной подготовки для интерпретации результатов, следовательно является простым в использовании и «прозрачным».

Расчет рисков основывается на совокупности способов и методов определения и оценки рисков, предложенных рядом международных и российских стандартов в сфере информационной безопасности.

Существует несколько ключевых документов, в которых прописаны требования к методам обработки и оценки рисков – серия международных стандартов ISO 27000. На основе их разработаны национальные стандарты, позволяющие составить собственную методику оценки рисков информационной безопасности исходя из специфики предприятия.

Процесс расчета рисков информационной безопасности актуален на всех этапах работы системы защиты информации. Исходя из данных документов, можно выделить следующее:

- в процессе оценки рисков должны быть установлены критерии приемлемости риска и критерии для оценки рисков безопасности;

- должна быть произведена идентификация рисков, направленных на такие основные свойства информационных ресурсов (конфиденциальность, целостность и доступность);

- в процессе анализа рисков должна быть произведена оценка потенциальных потерь в случае реализации риска;

- должна быть оценена вероятность реализации рисков и определена их величина;

- при осуществлении оценки должно быть произведено сопоставление рисков с установленными критериями, а также определен вектор приоритетных направлений по их обработке.

Существует множество методов по оценке рисков информационной безопасности. Это, например, идентификация риска, анализ последствий его реализации, оценка эффективности существующих средств управления, количественная или качественная оценка уровня рисков, смешанная оценка вероятностных характеристик риска [38].

Выбор метода оценки рисков должен основываться на следующих факторах:

- временные, финансовые, информационные ресурсы;

- степень неопределенности оценки рисков ИБ;

- наличие либо отсутствие возможности получение количественных оценок выходных данных, где таковыми могут являться мнения, решения, перечни, а также рекомендации, в зависимости от метода и этапа оценки.

В соответствии с ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» ценные активы организации условно можно разделить на основные и вспомогательные [30].

Основные активы:

1) процессы, связанные с деятельностью, в результате которой создается услуга, представляющая интерес для потребителя;

2) конфиденциальная информация, сведения, являющиеся предметом собственности, подлежащие защите от нарушения конфиденциальности, целостности и доступности, в соответствии с требованиями правовых документов и требованиями владельца информации, вне зависимости от формы представления.

Вспомогательные активы:

1) аппаратно-программный комплекс – совокупность технических и программных средств, которые предназначенных для выполнения взаимосвязанных функций по обработке информации ограниченного распространения, включающая в себя активную аппаратуру обработки данных, стационарную аппаратуру, периферийные обрабатывающие устройства, операционные системы и прикладное программное обеспечение;

2) носители данных – носитель для хранения данных, включая электронный носитель и аналоговый;

3) сеть – совокупность телекоммуникационных устройств, используемых для соединения нескольких физически удаленных друг от друга сегментов информационной системы;

4) персонал – все субъекты, имеющие легитимный доступ в пределы контролируемой зоны;

5) место функционирования организации – пределы контролируемой зоны, в которой функционирует информационная система.

Первоначально необходимо определить ценность активов (далее – ЦН) организации, в данном случае рассматривается четыре балльная система оценки ценности активов где:

«1» - реализация риска, направленного на конфиденциальность, целостность и/или доступность актива не будет иметь последствий, как для организации в целом, так и внутренней деятельности, в частности;

«2» – реализация риска, направленного на конфиденциальность, целостность и/или доступность актива приведет к незначительным потерям для организации, в условиях, когда восстановление прежнего состояния системы возможно без остановки деятельности.

«3» – реализация риска, направленного на конфиденциальность, целостность и/или доступность актива приведет к значительным финансовым потерям и/или окажет существенное негативное влияние на престиж организации, в условиях, когда восстановление прежнего состояния системы возможно, но требует больших временных и/или финансовых ресурсов

«4» – реализация риска, направленного на конфиденциальность, целостность и/ или доступность актива может привести к полной остановке деятельности, большим финансовым потерям и/или окажет значительное негативное влияние на престиж организации.

Данные о проведенной оценке активов оформляются в таблицу.

Таблица 3 - Шкала ценности активов

Идентификатор актива	Активы организации	Конфиденциальность	Целостность	Доступность	Ценность актива

Следующим шагом является определение степени уязвимости каждого из ценных активов организации (далее – СУ).

В рамках работы будет рассмотрен выборочный ряд угроз ИБ, актуальных для организации, с ID в соответствии с банком угроз ФСТЭК.

В таблице 4 представляется результат оценки уязвимости актива для перечня угроз, где

«1» – низкая уязвимость по отношению к конфиденциальности, целостности и/или доступности ценного актива организации,

«2» – средняя степень уязвимости,

«3» – высокая степень уязвимости.

Таблица 4 - Степень уязвимости актива

Угрозы ИБ	Ценные активы организации

Последним этапом перед расчетом рисков информационной безопасности является оценка вероятности реализации угроз ИБ (далее – В), определенных ранее и представленных в таблице 4. Проведенная оценка вероятности предоставляется в таблице 5,

где «1» – угроза существует, но не встречалась в рассматриваемой сфере,

«2» – угроза возникает в рассматриваемой сфере 2–3 раза в год,

«3» – угроза была реализована в рассматриваемой системе,

«4» – угроза возникает 2–3 раза в год в рассматриваемой системе.

Таблица 5 - Вероятность реализации угроз

ID угроз	Вероятность угрозы

Общий уровень риска ИБ для каждого из ценных активов организации рассчитывается по формуле, в таблице 6 представляется итог проведенной оценки.

$$Р = ЦН \times СУ \times В \quad (3)$$

Приемлемым риском считается риск, чье числовое значение находится в промежутке от 1 до 10, такой риск считается незначительным, и обработка такого риска не требуется.

Средний риск, чье числовое значение находится в диапазоне от 11 до 21, рекомендован к обработке с целью его минимизации.

Высокий риск, чье числовое значение находится в диапазоне от 22 до 64, данный риск считается существенным, обрабатывается в обязательном порядке, так как представляет большую угрозу для деятельности всей организации.

Таблица 6 - Оценка рисков ИБ

Ценный актив организации	ID угрозы	ЦН	СУ	В	Р	Значение оценки риска

После расчета уровня риска проводится анализ, из представленного перечня выбираются наиболее высокие риски, для них предлагаются возможные контрмеры, которые оформляются также в таблицу для наглядности.

Таблица 7 - Рекомендованные контрмеры

Ценный актив организации	Угрозы	Риск	Планируемые контрмеры

Для того, чтобы более четко представить, насколько сильно та или иная угроза влияет на организацию, следует провести анализ и определить финансовый ущерб, который может причинить угроза, риск которой является на высоком уровне, сравнить со стоимостью тех мер, которые будут осуществлены в качестве мероприятий по укреплению уровня безопасности и сделать выводы о целесообразности тех или иных мер, которые необходимо будет ввести.

3. Анализ состояния информационной составляющей экономической безопасности ФГБОУ ВО «СГИИ имени Д. Хворостовского», разработка предложений по оптимизации информационной инфраструктуры

3.1 Характеристика ФГБОУ ВО «СГИИ имени Д. Хворостовского»

Федеральное государственное бюджетное образовательное учреждение «Сибирский государственный институт искусств имени Д. Хворостовского» (далее – СГИИ имени Д. Хворостовского, институт, вуз) – федеральный государственный вуз; большой образовательный, творческий, научный и методический центр в области музыкального, художественного, хореографического и театрального искусства на территории Российской Федерации.

Вуз образован в 1978 году. Вначале в его структуру входили три направления: музыкальное, театральное, художественное. В 1987 году художественный факультет был реорганизован в – Красноярский государственный художественный институт (КГХИ).

В 2000 году институт получает статус академии – Красноярская государственная академия музыки и театра (КГАМиТ). Далее в 2015 году Министерство культуры Российской Федерации вернуло вузу историческое наименование: Красноярский государственный институт искусств (КГИИ). В 2017 году вуз реорганизован посредством присоединения к нему Красноярского государственного художественного института и образованием художественного факультета КГИИ. В 2018 году КГИИ переименован ФГБОУ ВО «Сибирский государственный институт искусств имени Дмитрия Хворостовского» (СГИИ) [33].

Сейчас деятельность института в области образования осуществляется, как и в самом начале его существования, тремя факультетами для всех уровней подготовки специалистов среднего профессионального, высшего образования (бакалавриат, специалитет, магистратура), а также подготовки кадров высшей квалификации (аспирантура, ассистентура-стажировка).

Вуз осуществляет образовательную деятельность в рамках системы непрерывного образования (от учеников школ до специалистов высшей квалификации). В 1991 г. в институте образовано отделение довузовской подготовки, в 1994 году отделение преобразовано в музыкальный лицей. На базе которого была открыта 12-я Красноярская гимназия «Музыки и театра», которая в свою очередь стала в 2004 г. музыкальным колледжем в составе СГИИ (КГАМиТ).

В настоящее время около 65 % педагогов вуза имеют различные ученые степени (кандидата и доктора наук), ученые/почетные звания (доцента, профессора/заслуженный, народный), удостоены различных правительственных наград. Многие педагоги организовали творческие школы в своем индивидуальном направлении искусства.

За многие годы институт выпустил более четырех тысяч специалистов для учреждений культуры и искусства России (филармонии, театры, концертные коллективы, художественные и дизайнерские студии и мастерские, учебные заведения разного уровня (вузы, ссузы, детские школы искусств)). Выпускники СГИИ после его окончания осуществляют свою трудовую деятельность во многих городах России и мира. Наиболее известные выпускники института – скульптор Даши Намдаков, оперный певец мирового уровня – народный артист Российской Федерации Дмитрий Хворостовский.

Огромной известностью в России и в мире пользуются созданные на базе СГИИ хоровой ансамбль солистов «Тебе поемъ», а так же Красноярский камерный оркестр.

Вуз довольно активно осуществляет профориентационную деятельность с ДШИ и ссузами культуры и искусства, а также другими музыкальными и художественными организациями в реализующими свою деятельность в области образования в таких городах как Москва, Санкт-Петербург, многие города Сибири и Урала.

На базе института постоянно проводятся фестивали, конкурсы, научные конференции различного уровня (региональные, межрегиональные,

всероссийские, международные и др.), которые на сегодняшний день являются частью культурной жизни Сибири и всей России: (Международный музыкально-театральный конкурс-фестиваль «Надежда», Международный художественный симпозиум по керамике, Международный конкурс скрипачей Виктора Третьякова, Всероссийский конкурс по фортепиано среди студентов различных специальностей «Енисей-KLAVIER», Международный конкурс-фестиваль баянистов, аккордеонистов и гармонистов «Кубок Сибири», Международный фестиваль и конкурс дирижеров академических хоров средних и высших учебных заведений «Весенние хоровые капеллы», Всероссийский конкурс «Symphoniacusinteger», Открытый сибирский конкурс «Мелос сибирской поэзии», Международные научные конференции «Искусство глазами молодых», «Художественная культура России»). Основная цель реализуемых на базе института мероприятий в области искусства – поиск и помощь в выбранном профессиональном направлении самых талантливых, обучающихся и выпускников, развитие их потенциала, возникновение у них интереса к Российскому искусству и культуре [33].

На основе международных соглашений проходят интерпленэры вместе с художниками из Франции, Германии, Англии, Индии, Японии, Бангладеш. Кроме того, периодически институт организует различные выездные мероприятия творческой направленности: педагоги института проводят лекции, мастер-классы в Индии (по местам К. Рериха), в университетах г. Турку (Финляндия), г. Варшава, г. Краков (Польша), колледж г. Онеонта (штат Нью-Йорк), принимают участие в международном фестивале «Италия – Сибирь». С 2001 по 2016 год вместе с Международной академией И.С. Баха при помощи Министерства культуры Красноярского края институт организовал и провел на своей базе фестиваль «Бахакадемия». Студенты СГИИ ежегодно активно участвуют в музыкальных фестивалях в Англии, Германии, Греции, Франции, Сербии, Чехии, а также других странах. Педагоги института постоянно участвуют в работе жюри различных международных конкурсов Европы и других стран мира.

Между вузом и многими организациями в области культуры и искусства заключены и реализуются договоры о сотрудничестве: Казахская национальная консерватория имени Курмангазы (Казахстан), Комплекс «Музыкальный колледж – музыкальная школа – интернат для одаренных детей» (Павлодар, Казахстан), Таджикский государственный институт культуры и искусств им. М. Турсунзаде (Таджикистан), Центр международных программ Министерства образования и науки Республики Таджикистан, Каршинский государственный университет (Узбекистан), Академия музыки г. Краков, Ляонинский университет науки и технологий (Институт архитектуры и художественного дизайна), Педагогический университет Внутренней Монголии (Китай), Педагогический университет г. Чуньцинь, Харбинский институт дизайна и искусств Харбинского университета, Хулуньбуирский институт (Китай), музыкально-хореографический колледж им. Гончисумлыы (Монголия), Ванадзорский государственный университет имени Ованеса Туманяна (Армения), Белорусская государственная академия искусств (Беларусь), Кыргызский государственный университет культуры и искусства им. Б. Бейшеналиевой (Кыргызстан), Белорусский государственный университет культуры и искусств (Республика Беларусь), Университет UşakUniversity (Турция).

Материально-техническое обеспечение института на основании федерального закона «Об образовании в Российской Федерации» № 273 понятие средства обучения и воспитания включает в себя: «различные приборы и оборудование, в том числе и спортивный инвентарь, инструменты (в том числе музыкальные), учебно-наглядные пособия, компьютеры, информационно-телекоммуникационные сети, аппаратно-программные и аудиовизуальные средства, печатные и электронные образовательные и информационные ресурсы и иные материальные объекты, необходимые для организации образовательной деятельности».

В соответствии с этим перечнем в средства, которые применяются в процессе обучения и воспитания в институте включены:

1. Специфическое оборудование и инвентарь, необходимые при реализации образовательного процесса: спортивный инвентарь и спортивное оборудование, различные музыкальные инструменты, гончарное оборудование (печи для обжига, муфельные печи, пресс для тиснения, канифольный шкаф), оборудование для использования в области художественного искусства (станок литографский, скульптурный станок), а также иное материальное и техническое оборудование для оснащения учебных корпусов вуза, спортивного зала и других служебных помещений, используемых для образовательного процесса.

2. Учебные и другие учебно-наглядные пособия: учебные и учебно-методические пособия, дидактические материалы, гипсовые наглядные учебные пособия и др.

3. Информационно-коммуникационное оборудование: компьютеры, информационно-телекоммуникационные сети, фото- и видеоаппаратура, веб-камеры, проекторы, экраны и пр.

4. Электронные и печатные образовательные и информационные ресурсы.

Кафедры и факультеты в полном объеме оснащены учебными аудиториями для лекционных групповых, а также индивидуальных занятий, в том числе имеющими мультимедийные системы, которые могут воспроизводить графические, аудио-, видео- материалы. Вуз имеет все необходимый парк инструментов, которые требуются для реализации всех направлений подготовки и специальностей для индивидуальных и групповых занятий.

Кроме того, в вузе есть 3 компьютерных класса с мультимедийным оборудованием и выходом в Интернет. Библиотека института в своей структуре имеет фонотеку на 156 посадочных места, а также другие аудитории и помещения для индивидуального просмотра видеозаписей и прослушивания аудиозаписей, кабинки для звукорежиссеров, 2 студии звукозаписи.

В настоящее время в своей собственности институт имеет более 250 компьютеров с выходом в информационно-телекоммуникационную сеть

«Интернет», одновременный доступ к которым имеют 90 обучающихся и 166 сотрудников.

Значительная часть учебной литературы и наглядно-дидактических пособий и материалов оцифровывается и хранится в электронной форме для использования на занятиях при помощи информационно-телекоммуникационных технологий, аппаратно-программного и аудиовизуального оборудования. Для этого все корпуса института оснащены аудиториями с мультимедиа-проекторами, а также компьютерные аудитории.

В институте действует студенческий медиацентр, в котором осуществляется доступ к видеозаписывающему оборудованию. Кроме того, институт имеет колоссальную базу печатных изданий, полностью обеспечивающей учебно-методической литературой все образовательные программы, реализуемые институтом. Доступ ко всей учебной литературе и другим печатным изданиям осуществляется библиотекой вуза, читальными залами, а также посредством использования электронных библиотечных комплексов. Работники института в своей трудовой деятельности постоянно используют электронные образовательные и информационные ресурсы.

Вуз имеет все необходимое оборудование и средства, которые применяются для проведения мероприятий культурно-массового характера (микшерные пульты, проекторы, акустические системы, радиосистемы, усилители мощности, звуковоспроизводящая аппаратура, световая система, ноутбуки, компьютеры, переносные и стационарные экраны многофункционального направления).

Использование находящейся в собственности института материально-технической базы необходимо для создания условий, способствующих всестороннему развитию студентов, в том числе организации их внеучебной деятельности (досуга), созданию различных творческих коллективов и объединений.

Огромное внимание в СГИИ им. Дмитрия Хворостовского уделяется вопросам соответствия института уровню информационно –

коммуникационных технологий, соответствующему современным реалиям. Таблица 8 содержит информацию об оснащенности вуза соответствующим оборудованием.

Таблица 8 - Доступ к информационно-телекоммуникационным сетям

Наименование	Всего	В том числе используемых в учебных целях	
		Всего	Из них доступных для использования обучающимися в свободное от основных занятий время
Персональные компьютеры – всего	256	200	90
Из них: ноутбуки и другие портативные персональные компьютеры (кроме планшетных)	55	55	43
планшетные компьютеры	2	2	0
находящиеся в составе локальных вычислительных сетей	256	200	90
имеющие доступ к Интернету	256	200	90
имеющие доступ к Интернет-порталу организации	256	200	90
Серверы	9		
Мультимедийные проекторы	16		
Интерактивные доски	3		
Устройства выполняющие операции печати, сканирования, копирования	100		
Телевизоры и плазменные панели	26		
Максимальная скорость доступа к Интернету	15 Мбит/сек		
Максимальная скорость фиксированного беспроводного доступа к Интернету (WiFi)	10 Мбит/сек		
Количество выделенных каналов	3		

Для профессиональной ориентации выпускников вуза в настоящих условиях информатизации общества, а также помощи в развитии их компетентности в сфере информационных коммуникаций, институтом осуществляется деятельность по следующим направлениям:

- доступ к телекоммуникационным, образовательным, научным и творческим информационным ресурсам для педагогов, сотрудников и студентов вуза;

- обучение педагогических работников и студентов института информационным технологиям и современным технологиям обучения, а также создание условий, необходимых для такого обучения;

- непрерывное наращивание объема финансирования, направленного для решения проблемы информатизации посредством использования различных источников финансирования (субсидии на исполнение государственного задания, средства от приносящей доход деятельности, различные программы развития, гранты и пр.).

В реализации этих направлений помогает комплексная информатизация основных и вспомогательных процессов, осуществляемая в вузе на всех уровнях (образовательных и структурных). Непрерывно развивается информационная образовательная среда, которая реализуется на современном уровне как обучения, так и управления всем процессом образования и его качеством (начиная от приемной кампании (набора студентов) и рекламы образовательных услуг до составления и осуществления образовательных программ).

Все лекционные аудитории, компьютерные классы, кафедры, деканаты, вспомогательные службы и структурные подразделения, расположенные в трех корпусах института, объединены в единую защищенную локальную сеть, все компьютеры института оснащены доступом в интернет.

Во всех корпусах института располагаются лекционные аудитории, которые оснащены специализированным мультимедийным и акустическим, проекционным, плазменным, интерактивным оборудованием, для наглядного проведения занятий, а также компьютерные классы, оснащенные всем необходимым техническим оборудованием и лицензионным программным обеспечением.

Все программное обеспечение вуза включает в себя программы и пакеты программ коммерческого использования, свободного ПО, учебных версий программ. Это операционные системы, офисные программы, справочно-правовые системы, бухгалтерские программы, программные пакеты САПР для

архитекторов и дизайнеров (AutoCAD, ArchiCad), программы для 3D моделирования, обработки растровой и векторной графики, издательской деятельности и верстки, видеомонтажа, анимации, обработки звука (3dsMax, CorelDraw, Photoshop, Illustrator, InDesign, FlashProfessional, DreamWeaver, AfterEffects, PremierePro, Auditionи.т.д.), программы набора нотного текста Finale, программы секвенсоры:SteinbergCubase, PresonusStudioOne и т. д.

В образовательном процессе педагогами и студентами института широко используются компьютерные программы по различным тематикам и даже дисциплинам, профессиональные пакеты программ, электронные версии справочников, словарей, энциклопедий, электронные учебные пособия и методические рекомендации, электронные каталоги и электронные библиотечные системы. Полный перечень программного обеспечения, имеющегося в институте, представлен в таблице 9.

Таблица 9 - Наличие программного обеспечения

Наименование ПО	Количество лицензий (количество рабочих мест)
ОС Windows Server	5
ОСWindowsXP, Vista,7,8,10	250
Autocad	125, учебная версия
ArchiCAD	учебная версия
Консультант Плюс	сетевая
1С:Бухгалтерия	22
1С:Зарплата и кадры	22
1С:Трактиръ	5
Электронная библиотека	сетевая
ПКГРАНДСмета	2
Adobe Master Collection	29
Adobe Design Premium	10
3dsMax	125, учебная версия
CorelDraw	19
Abbyy Fine Reader	15
MS Office	216
АнтивирусКасперского	279
WinRAR	60

Окончание таблицы

Наименование ПО	Количество лицензий (количество рабочих мест)
Business Studio	1
Программное обеспечение Лаборатория MmisLab	сетевая
Finale	18
Teletronix® LA-2A Classic Leveler Collection	1
NativeInstruments KOMPLETE	3
Celemonymelodyne edition Full version	1
Pgmusic Band-in-box and RealBandMegaPAK	2
MeldaProductionMTotalBundle	2
PropellerheadsReason	2
SteinbergCubase	4
Sony Sound Forge Professional	2
Presonus Studio One 2 Professional	4
PresonusVocALign Project	1
Sony Vegas	1
MERCURY NATIVE	1
Лингафонный кабинет «Аудиториум»	сетевая
АИБСAbsotheque Unicode (со встроенными модулями «веб-модуль OPAC» и «Книгообеспеченность»), программный комплекс «Либер. Электронная библиотека», модуль «Поиск одной строкой для электронного каталога AbsOPACUnicode», модуль «SecView к программному комплексу «Либер. Электронная библиотека».	сетевая

В соответствии с требованиями действующего законодательства Российской Федерации к образовательным организациям всех видов и уровней, а также для быстрого и оперативного доступа к информации о деятельности института и его структурных подразделений, в институте функционирует сайт.

Целями его работы являются:

- соблюдение действующего законодательства Российской Федерации в области образования;

- представление вуза в информационно-коммуникационной сети Интернет;

- формирование имиджа вуза;

- предоставление доступа к информационной базе института для поступающих (абитуриентов), студентов, а также работников вуза;

- реализация обеспечения доступности информации деятельности института и ее открытости.

3.2 Выявление проблем и определение уровня защищенности информационной безопасности организации

В соответствие с Федеральным законом «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27.07.2006 информация, содержащаяся в данном пункте, запрещена для отрытого доступа, так как содержит конфиденциальные сведения

ЗАКЛЮЧЕНИЕ

В соответствие с Федеральным законом «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27.07.2006 информация, содержащаяся в заключении, запрещена для отрытого доступа, так как содержит конфиденциальные сведения

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ГОСТ ИСО/МЭК 15408-1-2012 Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1: Введение и общая модель. – Введ. 15 нояб. 2012. – Москва : Стандартинформ, 2014.

2. Об обеспечении безопасности персональных данных ФГБОУ ВО «СГИИ им. Д. Хворостовского»: положение от 26 нояб. 2018 г. – Красноярск: ФГБОУ ВО «СГИИ им. Д. Хворостовского», 2018.

3. Об обработке персональных данных ФГБОУ ВО «СГИИ имени Д. Хворостовского: положение от 26 нояб. 2018 г. – Красноярск: ФГБОУ ВО «СГИИ им. Д. Хворостовского», 2018.

4. Политика Сибирского государственного института искусств имени Д. Хворостовского в отношении обработки персональных данных: политика от 26 нояб. 2018 г. - Красноярск: ФГБОУ ВО «СГИИ им. Д. Хворостовского», 2018.

5. Экономическая безопасность: учебно-методическое пособие / В. К. Крутиков, Т. В. Дорожкина, О. И. Костина, М. В. Якунина. – Калуга : Эйдос, 2017.

6. Манахова, И. В. Экономическая безопасность : учебник / И. В. Манахова. – Саратов : Саратовский социально-экономический институт (филиал) РЭУ им. Г.В. Плеханова, 2019.

7. Вострецова, Е. В. Основы информационной безопасности : учебное пособие для студентов ВУЗов / Е. В. Вострецова. – Екатеринбург : Изд-во Урал. ун-та, 2019.

8. Матвеева, В. А. Информационная безопасность : учебно-методическое пособие / В. А. Матвеева. – Нижний Новгород : Изд-во Нижегород. ун-та, 2017.

9. Ясенева, В. Н. Информационная безопасность : учебное пособие / В. Н. Ясенева. – Нижний Новгород : Изд-во Нижегород. гос. ун-та им. Н. И. Лобачевского, 2017.

10. Шубинский, М. И. Информационная безопасность для работников бюджетной сферы : учебное пособие / М. И. Шубинский. – Санкт-Петербург : НИУ ИТМО, 2017.

11. Саматов, К.М. Персональные данные работников организации и их защита : учебное пособие / К. М. Саматов. – Екатеринбург : Издательские решения, 2016.

12. Персональные данные в государственных информационных ресурсах : научные доклады / М. Брауде-Золотарев, В. Негородов, Е. Сербина, И. Волошкин. – Москва : Дело, 2016.

13. Защита персональных данных в организации : монография / М. Ю. Рытов, В. И. Аверченков, Т. Р. Гайнулин. – Брянск : Брянск. гос. техн. ун-т, 2016.

14. Новая парадигма защиты и управления персональными данными в Российской Федерации и зарубежных странах в условиях развития систем обработки данных в сети Интернет : монография / А. С. Дупан (Гутникова) [и др.]. – Москва : НИУ ВШЭ, 2016.

15. Плетнев, П. В. Алгоритмы и методики оценки угроз информационной безопасности в сетях и системах телекоммуникаций : дис. … канд. техн. наук : 05.12.13 / Плетнев Павел Валерьевич. – Новосибирск, 2017.

16. Глухов, Н. И. Оценка информационных рисков хозяйствующих субъектов : дис. … канд. экон. наук : 08.00.05 / Глухов Николай Иванович. – Иркутск, 2009.

17. Кудрявцева, Р. Т. Управление информационными рисками с использованием технологий когнитивного моделирования (на примере высшего учебного заведения) : дис. … канд. техн. наук : 05.13.19 / Кудрявцева Рима Тимиршаиховна. – Уфа, 2008.

18. Шестерин, А. А. Совершенствование системы обеспечения информационной безопасности как составляющей экономической безопасности кредитных организаций : дис. … канд. экон. наук : 08.00.05 / Шестерин Александр Александрович. – Москва, 2010.

19. Доктрина информационной безопасности Российской Федерации [Электронный ресурс] : Указ Президента Российской Федерации от 5 дек. 2016 г. № 646 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_208191/4dbff9722e14f63a309bce4c2ad3d12cc2e85f10/

20. Уголовный кодекс Российской Федерации [Электронный ресурс] : федер. закон от 13.06.1996 № 63-ФЗ ред. от 07.04.2020 // Справочная правовая система «КонсультантПлюс». - Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_10699/

21. Гражданский кодекс Российской Федерации. Ч 1 [Электронный ресурс] : федер. закон от 30 ноября 1994 года № 51-ФЗ ред. от 16.12.2019 // Справочная правовая система «КонсультантПлюс». - Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_5142/

22. Трудовой кодекс Российской Федерации [Электронный ресурс] : федер. закон от 30.12.2001 № 197-ФЗ ред. от 24.04.2020 // Справочная правовая система «КонсультантПлюс». - Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_34683/

23. Кодекс Российской Федерации об административных правонарушениях [Электронный ресурс] : федер. закон от 30.12.2001 № 195-ФЗ ред. от 24.04.2020 // Справочная правовая система «КонсультантПлюс». - Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_34661/

24. О персональных данных [Электронный ресурс] : федер. закон от 27.07.2006 № 152-ФЗ ред. от 31.12.2017 // Справочная правовая система «КонсультантПлюс». - Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/

25. Об информации, информационных технологиях и защите информации [Электронный ресурс] : федер. закон от 27.07.2006 № 149-ФЗ ред. от 03.04.2020 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

26. О государственной тайне [Электронный ресурс] : закон от 21.07.1993 № 5485-1 ред. от 29.07.2018 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/

27. О коммерческой тайне [Электронный ресурс] : федерльный закон от 29.07.2004 № 98-ФЗ ред. от 18.04.2018 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/

28. О техническом регулировании [Электронный ресурс] : федер. закон от 27.12.2002 № 184-ФЗ ред. от 28.11.2018 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_40241/

29. О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд [Электронный ресурс] : федер. закон от 05.04.2013 № 44-ФЗ ред. от 24.04.2020 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_144624/

30. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности [Электронный ресурс]: нац. стандарт Российской Федерации введ. 01.12.2011 // Электронный фонд правовой и нормативно-технической документации «КонсорциумКодекс». – Режим доступа: http://docs.cntd.ru/document/gost-r-iso-mek-27005-2010

31. Официальный сайт Международной организации по стандартизации [Электронный ресурс]. – Режим доступа: https://www.iso.org/ru/home.html

32. Банк данных угроз безопасности федеральной службы по техническому и экспортному контролю [Электронный ресурс] : банк данных угроз безопасности информации содержит сведения об основных угрозах безопасности информации и уязвимостях критически важных объектов. - Режим доступа: https://bdu.fstec.ru

33. Официальный сайт Сибирского федерального института искусств имени Дмитрия Хворостовского [Электронный ресурс]. - Режим доступа: http://kgii.ru

34. Руйга, И. Р. Экономическая безопасность [Электронный ресурс] : учебно-методическое пособие / И. Р. Руйга. – Электрон. дан. - Красноярск : Сиб. федер. ун-т, 2017. - Режим доступа: https://bik.sfu-kras.ru/

35. Макашова В. Н., Чусавитина Г. Н. Модернизация ИТ-инфраструктуры образовательных учреждений в целях обеспечения информационной безопасности [Электронный ресурс] / В. Н. Макашова, Г. Н. Чусавитина // Научная электронная библиотека «eLIBRERY.RU». – 2014. – Режим доступа: https://www.elibrary.ru/item.asp?id=23020685

36. Мандрица И. В., Мандрица О. В., Соловьева И. В., Петренко В. И. Методика технико-экономического обоснования принимаемых решений по повышению информационной безопасности бюджетных организаций [Электронный ресурс] / И. В. Мандрица, О. В. Мандрица, И. В. Соловьева, В. И Петренко // Научная электронная библиотека «eLIBRERY.RU». – 2017. – Режим доступа: https://www.elibrary.ru/item.asp?id=29952439

37. Баранова, Е. К. Методика анализа и оценки рисков информационной безопасности [Электронный ресурс] / Е. К. Баранова // Научная электронная библиотека «КиберЛенинка». – 2015. – Режим доступа: https://cyberleninka.ru/article/n/metodiki-analiza-i-otsenki-riskov-informatsionnoy-bezopasnosti/viewer

38. Ильченко Л. М., Брагина Е. К., Егоров И. Э., Зайцев С. И. Расчет рисков информационной безопасности телекоммуникационного предприятия [Электронный ресурс] / Л. М. Ильченко, Е. К. Брагина, И. Э. Егоров, С. И. Зайцев // Научная электронная библиотека «eLIBRERY.RU». – 2018. – Режим доступа: https://www.elibrary.ru/item.asp?id=32880002

39. Шиляев, С. Методика оценки рисков информационной безопасности [Электронный ресурс] / С. Шиляев // Электронный журнал «Контур». – 2015. – Режим доступа: https://kontur.ru/articles/1691

40. Морунов, В. В. Экономическая безопасность как экономическая категория / В. В. Морунов // Экономические науки. - 2011. - № 83. – С. 53 – 55.

41. Киселева И. А., Симонович Н. Е., Косенко И. С. Экономическая безопасность предприятия: особенности, виды, критерии оценки / И. А. Киселева, Н. Е. Симонович, И. С. Косенко // Вестник ВГУИП. – 2018. - Т. 80, № 3. С. 415 – 423.

42. Ермолаев, Д. В. Составляющие экономической безопасности предприятия / Д. В. Ермолаев // Ученые записки Орловского гос. ун-та. Серия : гуманитарные и социальные науки. - 2011. - № 4. – С. 15 – 17.

43. Батова, В. Н. Обеспечение экономической безопасности бюджетных учреждений высшего профессионального образования в новых условиях финансирования / В. Н. Батова // Финансовая аналитика: проблемы и решения. – 2013. - № 24 (162). – С. 35 – 50.

44. Ануфриев, С. С. Информационная безопасность, и проблемы повышения эффективности системы государственных закупок / С. С. Ануфриев // Актуальные вопросы экономических наук. – 2013. - № 29-1. С. 71 – 80.

45. Плетнев, П. В., Белов, В. М. Методика оценки рисков информационной безопасности на предприятиях малого и среднего бизнеса / П. В. Плетнев, В. М. Белов // Доклады Томского государственного ун-та систем управления и радиоэлектроники. - 2016. – № 1-2. – С. 83 – 86.

46. Пугин, В. В., Губарева, О. Ю. Обзор методик анализа рисков информационной безопасности информационной системы предприятия / В. В. Пугин, О. Ю. Губарева // Т-СОММ: Телекоммуникации и транспорт. - 2016. – Т. 6, № 6. – С. 54 – 57.

47. Хорев, П. Б., Ларионов, И. П. Особенности разработки методики оценки информационной безопасности предприятия для экспертных систем / П. Б. Хорев, И. П. Ларионов // Современная наука: актуальные проблемы и пути их решения. - 2017. - № 9. – С. 14 – 19.

48. Надеждин, Е. Н., Шептуховский, В. А. Методика оценивания рисков информационной безопасности в вычислительных сетях образовательных

учреждений / Е. Н. Надеждин, В. А. Шептуховский // Педагогическая информатика. - 2016. - № 4. – С. 84 – 92.

49. Ажмухамедов, И. М., Ханжина, Т. Б. Оценка экономической эффективности мер по обеспечению информационной безопасности / И. М. Ажмухамедов, Т. Б. Ханжина // Вестник Астрах. гос. техн. ун-та. Серия: Экономика. - 2016. - № 1. С. 185 – 190.

50. Егоров, М. А. Методика аудита информационной безопасности в современных условиях / М. А. Егоров // Вестник науки и образования. Ч. 2. - 2019. - № 11 (65). – С. 34 – 37.

ПРИЛОЖЕНИЕ А

Виды ответственности

Таблица - Таблица 11 - Виды ответственности за нарушение закона о персональных данных

Вид ответственности	Нарушение	Санкция	Норма
Административная	Неправомерный отказ в предоставлении гражданину и (или) организации информации, предоставление которой предусмотрено законом, несвоевременное ее предоставление либо предоставление заведомо недостоверной информации	Административный штраф на должностных лиц в размере от 5 тыс. до 10 тыс. руб.	Ст. 5.39 КоАП РФ
	Обработка персональных данных в случаях, не предусмотренных законом, либо обработка, несовместимая с целями сбора персональных данных	Предупреждение или административный штраф: на граждан – от 1 тыс. до 3 тыс. руб.; на должностных лиц – от 5 тыс. до 10 тыс. руб.; на юридических лиц – от 30 тыс. до 50 тыс. руб.	Ч. 1 ст. 13.11 КоАП РФ
	Обработка персональных данных без письменного согласия субъекта, когда это необходимо, либо обработка данных с нарушением требований к составу сведений, включаемых в такое согласие	Административный штраф: на граждан – от 3 тыс. до 5 тыс. руб.; на должностных лиц – от 10 тыс. до 20 тыс. руб.; на юридических лиц – от 15 тыс. до 75 тыс. руб.	Часть 2 ст. 13.11 КоАП РФ
	Невыполнение оператором обязанности по опубликованию или обеспечению иным образом неограниченного доступа к политике обработки персональных данных	Предупреждение или административный штраф: на граждан – от 700 до 1 тыс. руб.; на должностных лиц – от 3 тыс. до 6 тыс. руб.; на индивидуальных предпринимателей – от 5 тыс. до 10 тыс. руб.; на юридических лиц – от 15 тыс. до 30 тыс. руб.	Ч. 3 ст. 13.11 КоАП РФ
	Невыполнение оператором обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных	Предупреждение или административный штраф: на граждан – от 1 тыс. до 2 тыс. руб.; на должностных лиц – от 4 тыс. до 6 тыс. руб.;	Ч. 4 ст. 13.11 КоАП РФ

Продолжение таблицы

Вид ответственности	Нарушение	Санкция	Норма
		на юридических лиц – от 20 тыс. до 40 тыс. руб.	
	Невыполнение оператором в установленные сроки требования субъекта персональных данных или его представителя либо Роскомнадзора об уточнении персональных данных, их блокировании или уничтожении (если данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки)	Предупреждение или административный штраф: на граждан – от 1 тыс. до 2 тыс. руб.; на должностных лиц – от 4 тыс. до 10 тыс. руб.; на индивидуальных предпринимателей – от 10 тыс. до 20 тыс. руб.; на юридических лиц – от 25 тыс. до 45 тыс. руб.	Ч. 5 ст. 13.11 КоАП РФ
	Невыполнение оператором при обработке персональных данных без использования средств автоматизации обязанности по соблюдению условий, обеспечивающих их сохранность и исключающих несанкционированный к ним доступ, если это повлекло неправомерный или случайный доступ к данным, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия в отношении них	Административный штраф: на граждан – от 700 до 2 тыс. руб.; на должностных лиц – от 4 тыс. до 10 тыс. руб.; на индивидуальных предпринимателей – от 10 тыс. до 20 тыс. руб.; на юридических лиц – от 25 тыс. до 50 тыс. руб.	Ч. 6 ст. 13.11 КоАП РФ
	Невыполнение оператором, являющимся государственным или муниципальным органом, обязанности по обезличиванию персональных данных либо несоблюдение установленных для этого требований или методов	Предупреждение или наложение административного штрафа на должностных лиц в размере от 3 тыс. до 6 тыс. руб.	Ч. 7 ст. 13.11 КоАП РФ
	Непредставление или несвоевременное представление в государственный или иной уполномоченный орган сведений, представление которых предусмотрено законом либо предоставление таких сведений в неполном объеме или в искаженном виде	Административный штраф: на граждан – от 100 до 300 руб.; на должностных лиц – от 300 до 500 руб.; на юридических лиц – от 3 тыс. до 5 тыс. руб.	Ст. 19.7 КоАП РФ
	Невыполнение оператором при сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", предусмотренной законодательством Российской Федерации в области персональных данных обязанности по обеспечению записи, систематизации, накопления, хранения, уточнения (обновления, изменения) или извлечения персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации	Административный штраф: - на граждан в размере от тридцати тысяч до пятидесяти тысяч рублей; - на должностных лиц - от ста тысяч до двухсот тысяч рублей; - на юридических лиц - от одного миллиона до шести миллионов рублей.	Ч. 8 ст. 13.11 КоАП РФ
	Повторное совершение административного правонарушения, предусмотренного частью 8	Административный штраф: - на граждан в размере от	Ч. 9 ст. 13.11

Продолжение таблицы

Вид ответственности	Нарушение	Санкция	Норма
	настоящей статьи	пятидесяти тысяч до ста тысяч рублей; - на должностных лиц - от пятисот тысяч до восьмисот тысяч рублей; - на юридических лиц - от шести миллионов до восемнадцати миллионов рублей.	КоАП РФ
Уголовная	Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или СМИ	Штраф до 200 тыс. руб., либо обязательные работы на срок до 360 часов, либо исправительные работы на срок до одного года, либо принудительные работы на срок до двух лет (с лишением права занимать определенные должности на срок до трех лет или без такового), либо арест на срок до четырех месяцев, либо лишение свободы на срок до двух лет (с лишением права занимать определенные должности на срок до трех лет)	Ст. 137 УК РФ
	То же деяние, совершенное с использованием служебного положения	Штраф от 100 тыс. до 300 тыс. руб., либо лишение права занимать определенные должности на срок от двух до пяти лет, либо принудительные работы на срок до четырех лет (с лишением права занимать определенные должности на срок до пяти лет или без такового), либо арест на срок до шести месяцев, либо лишение свободы на срок до четырех лет (с лишением права занимать определенные должности на срок до пяти лет)	
	Незаконное публичное распространение информации, указывающей на личность лица, не достигшего 16 лет, по уголовному делу, либо информации, содержащей описание полученных им в связи с преступлением физических или нравственных страданий	Штраф от 100 тыс. до 300 тыс. руб., либо лишение права занимать определенные должности на срок от трех до пяти лет, либо принудительные работы на срок до пяти лет (с лишением права занимать определенные должности на срок до шести лет или без такового), либо арест на срок до шести месяцев, либо лишение свободы на срок до пяти лет (с лишением права занимать определенные должности на срок до шести лет)	

Окончание таблицы

Вид ответственности	Нарушение	Санкция	Норма
	Неправомерный отказ должностного лица в предоставлении документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление ему неполной или заведомо ложной информации, если это причинило вред правам и законным интересам граждан	Штраф до 200 тыс. руб., либо лишение права занимать определенные должности на срок от двух до пяти лет	Ст. 140 УК РФ
	Неправомерный доступ к охраняемой законом компьютерной информации, если это повлекло ее уничтожение, блокирование, модификацию либо копирование	Штраф до 200 тыс. руб., либо исправительные работы на срок до одного года, либо ограничение свободы на срок до двух лет, либо принудительные работы на срок до двух лет, либо лишение свободы на тот же срок	Ст. 272 УК РФ
Гражданско-правовая	Причинение лицу убытков в результате нарушения правил обработки его персональных данных. Под убытками при этом понимаются: расходы, которые лицо произвело или должно будет произвести для восстановления нарушенного права; утрата или повреждение его имущества; неполученные доходы, которые лицо получило бы, не будь его право нарушено.	Возмещение убытков	Ст. 15 ГК РФ
	Причинение гражданину морального вреда (нравственных страданий) вследствие нарушения правил обработки персональных данных	Компенсация морального вреда (независимо от возмещения имущественного вреда и понесенных субъектом убытков)	Ст. 24 закона «О персональных данных», ст. 151 ГК РФ
Дисциплинарная	Разглашение одним работником персональных данных другого, если они стали известны ему в связи с исполнением трудовых обязанностей	Увольнение	Подпункт "в" п. 6 ч. 1 ст. 81 ТК РФ
	Иные нарушения в области персональных данных при их обработке	Замечание или выговор	Ст. 90, ст. 192 ТК РФ
Материальная	Лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных работника	Материальная ответственность	СТ. 90 ТК РФ

Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт экономики, управления и природопользования
кафедра финансов

УТВЕРЖДАЮ
Заведующий кафедрой
_____ И.С. Ферова
подпись
«_17_» __06___ 2020 г.

ДИПЛОМНАЯ РАБОТА

специальность 38.05.01 «Экономическая безопасность»

АНАЛИЗ И ОЦЕНКА ИНФОРМАЦИОННОЙ СОСТАВЛЯЮЩЕЙ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ БЮДЖЕТНОЙ ОРГАНИЗАЦИИ (НА ПРИМЕРЕ ФГБОУ ВО «СГИИ ИМ. Д. ХВОРОСТОВСКОГО»)

Научный
руководитель _____ 12.06.2020 к.э.н., доцент_____ Ю.А. Назарова
подпись, дата должность, ученая степень

Выпускник _____ 12.06.2020 А.Д. Прутовых

Рецензент _____ 12.06.2020 главный экономист Ю.Д. Величкина
подпись, дата должность, ученая степень (Ф.И.О.)

Красноярск 2020