Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КАЛИНИНГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

А. Г. Жестовский

РАЗРАБОТКА И ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ

учебно-методическое пособие по выполнению
курсового проекта для студентов специальности
10.05.03 «Информационная безопасность
автоматизированных систем»

Калининград
Издательство ФГБОУ ВО «КГТУ»
2023

УДК 004.056.57 (075)

Рецензент
доцент кафедры цифровых систем и автоматики
Института цифровых технологий
ФГБОУ ВО «Калининградский государственный технический университет»,
кандидат технических наук В. В. Капустин

Жестовский, А. Г.

Разработка и эксплуатация автоматизированных систем в защищённом исполнении: учебно-методическое пособие по выполнению курсового проекта для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» / А. Г. Жестовский. – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2024. – 87 с.

В учебно-методическом пособии изложены основные требования по выполнению курсового проекта и рекомендации по организации, выполнению и защите курсового проекта. В методических указаниях изложены требования к содержанию и оформлению курсового проекта по дисциплине «Разработка и эксплуатация автоматизированных систем в защищённом исполнении», варианты типовых заданий, указания к оформлению курсового проекта.

Пособие подготовлено в соответствии с требованиями утвержденной рабочей программы модуля «Методы и средства обеспечения информационной безопасности автоматизированных систем» 10.05.03 «Информационная безопасность автоматизированных систем».

Табл. 1, список лит. – 35 наименований

Учебно-методическое пособие рассмотрено и одобрено в качестве локального электронного методического материала на заседании кафедры ИБ ФГБОУ ВО «Калининградский государственный технический университет» 23 ноября 2023 г., протокол № 3

Учебно-методическое пособие по выполнению курсового проекта рекомендовано к использованию в учебном процессе в качестве локального электронного методического материала методической комиссией ИЦТ 28 ноября 2023 г., протокол № 11

УДК 004.056.57 (075)

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Проблема защиты информации: надежное обеспечение ее сохранности и установленного статуса использования – является одной из важнейших проблем современности.

Еще несколько лет назад обеспечение информационной безопасности могло быть эффективно решено с помощью организационных мер (выполнение режимных мероприятий, использование средств охраны и сигнализации) и отдельных программно-аппаратных средств разграничения доступа и шифрования. Этому способствовала концентрация информационных ресурсов и средств для их обработки на автономно функционирующих вычислительных центрах. Появление персональных ЭВМ, локальных и глобальных компьютерных сетей, спутниковых каналов связи, эффективных средств технической разведки и получения конфиденциальной информации существенно обострило проблему защиты информации.

Развитие информационных технологий, трансграничное их проникновение и использование во всех сферах деятельности современного человека выдвинули целый ряд новых проблем, требующих незамедлительного решения. Сегодня нет предприятий, фирм, организаций или отдельных пользователей ПЭВМ, которые бы не ставили периодически перед собой задачу защиты информации или работоспособности технических средств. Проблема информационной безопасности из разряда узкоспециальных и доступных только профессионалам становится жизненно важной для подавляющего круга населения страны. Задача защиты информации, в силу разнообразия объектов защиты, становиться комплексной.

Решение этой комплексной задачи предусматривает реализацию множества мероприятий: правовых, программно-аппаратных, криптографических, технических и организационных. Для этого необходима концепция решения проблемы проектирования, разработки, формирования и внедрения автоматизированных систем в защищенном исполнении.

Для современного развития нашего общества характерна постоянно ускоряющаяся динамика роста количества внедряемых автоматизированных систем (АС). Использование в АС новейших технологий и усложнение самих систем приводит к существенному повышению значения к разработке и дальнейшей эксплуатации АС.

Доля проектных трудозатрат в общих трудозатратах на разработку АС неуклонно повышается. В современных системах трудозатраты на проектирование сравнялись с трудозатратами на монтажные и пусконаладочные работы, зачастую превышая (в сложных комплексных системах значительно превышая) совокупные трудозатраты на все другие работы.

Учитывая то обстоятельство, что работы при разработке АС выполняются в рамках жестких ограничений как по срокам ввода систем в строй, так и по стоимости (ресурсоемкости) выполняемых работ, можно сказать, что краеугольным камнем является задача оптимизации соотношения «сроки – трудозатраты/стоимость – качество». Одним из путей решения этой задачи является разумная минимизация этапов создания и объемов проектирования АС, что означает определение минимально достаточного состава проектных работ, обеспечивающих заданное качество проектируемой системы. Понятно, что в каждом конкретном случае эта задача решается по-разному. В то же время в большинстве таких решений прослеживается определенная общность подходов.

Для защиты информации, циркулирующей в АС, создают систему защиты информации, являющуюся подсистемой этой автоматизированной системы. В связи с этим следует увеличивать количество специалистов в области информационной безопасности и обучать их современным методам и средствам защиты информации.

Подготовка квалифицированного специалиста по защите информации в университетском комплексе, исходя из предъявляемых требований федерального государственного образовательного стандарта высшего образования, реализуется путем проведения специальных дисциплин, одной из которых является дисциплина «Разработка и эксплуатация автоматизированных систем в защищённом исполнении». Данная дисциплина читается студентам специальности 10.05.03 «Информационная безопасность автоматизированных систем» на 4–5 курсе.

Важной формой активизации процесса усвоения знаний при подготовке специалистов в области информационных технологий является выполнение курсовых проектов.

Курсовой проект – одна из форм учебно-исследовательской работы, ее выполнение является обязательным для всех студентов в сроки, определенные рабочим учебным планом.

Курсовой проект по дисциплине способствует формированию навыков самостоятельного научного и практического подхода к освоению учебного материала. Кроме того, курсовая проект позволяет осуществить контроль за самостоятельной работой студента и оценить, наряду с экзаменами и зачетами, подготовленность будущего специалиста.

Курсовой проект должен отвечать высоким квалификационным требованиям в отношении содержания и оформления и направлен на формирование у студентов представления о эксплуатации системы защиты информации с требованиями к грамотному применению современных технологий защиты информации.

В настоящее время в ряде вузов осуществляется подготовка бакалавров и специалистов по направлению «Информационная безопасность». В предлагаемом учебно-методическом пособии сделан акцент на обобщении материалов при построении автоматизированных систем (АС), описании подходов к проектированию, формированию, внедрению и сопровождению подсистем защиты информации (ЗИ) в составе АС. Материалы могут быть полезны при практической работе специалистам, студентам, абитуриентам, работающим в области защиты информации. Подготовленное учебное пособие призвано сформировать основы системного мышления при изучении специальных дисциплин по направлению защиты информации.

1. НАЗНАЧЕНИЕ И ЗАДАЧИ КУРСОВОГО ПРОЕКТА

Целью курсового проекта по информационной безопасности является систематизация, закрепление и углубление теоретических знаний студентов о методологии и методике аудита информационной безопасности на предприятии, определения исходных данных для проектирования системы защиты информации и собственно проектирования систем защиты информации, а также выработка у них навыков решения практических задач по защите информации.

Целью выполнения курсового проекта (работы) является практическое закрепление знаний и умений в области разработки и эксплуатации автоматизированных систем в защищенном исполнении.

Курсовой проект завершается защитой. Выполнение каждого этапа проектирования контролируется руководителем проекта.

Цели курсового проекта разнообразны: научная, познавательная, учебная, методическая.

Данные цели проявляются через следующие конкретные задачи:

- систематизация, закрепление и расширение теоретических знаний и практических умений по специальности и применение их при решении конкретных задач;
- углубление теоретических знаний в соответствии с заданной темой;
- формирование умений самостоятельно использовать справочную, техническую документацию, научно-техническую литературу;
- умение самостоятельно излагать знания, полученные в процессе самостоятельного изучения литературы, делать обстоятельные и обоснованные выводы;
- развитие творческой инициативы, самостоятельности, ответственности и организованности;
- определение уровня подготовленности студентов.

Задача курсового проекта – изучение научно-технической и справочной литературы в области информационной безопасности, приобретение студентами навыков проектирования системы защиты информации и обоснованного выбора программных средств для защиты информации для конкретного предприятия.

Курсовой проект является составной частью учебного курса и предназначен для практического закрепления и расширения полученных теоретических знаний.

При выполнении курсового проекта по проектированию систем информационной безопасности следует руководствоваться следующими принципами:

– система информационной безопасности является интегральной частью информационной системы компании и должна функционировать, не нарушая эксплуатационных параметров информационной системы;

– система информационной безопасности основывается на политике безопасности компании, в соответствии с которой четко определяются физические и логические границы системы;

– анализ рисков является основой проектирования и дальнейшего использования системы информационной безопасности (при вводе системы в эксплуатацию риски должны быть снижены до приемлемого, заранее определенного и утвержденного уровня).

Внедрение средств обеспечения ИБ должно быть экономически обосновано: инвестируемые в систему информационной безопасности средства должны быть адекватны тем преимуществам, которые получит компания при достижении заданного уровня информационной безопасности.

Результаты курсового проектирования представляются в виде курсового проекта, включающего пояснительную записку, файлы и мультимедийные разработки студента. Содержание курсового проекта должно свидетельствовать о достаточно высокой теоретической подготовке обучающегося, которую он должен иметь на данном курсе, и о наличии у автора (-ов) необходимых знаний по теме работы. Проект должен иметь правильно составленную библиографию, логичную структуру, обеспечивающую раскрытие темы. Должен быть написан грамотно, хорошим литературным и профессиональным языком, иметь правильно оформленный инструментальный аппарат [35].

2. ОРГАНИЗАЦИЯ И РУКОВОДСТВО ВЫПОЛНЕНИЕМ КУРСОВОГО ПРОЕКТА

2.1 Порядок выполнения курсовых проектов

Курсовой проект выполняется студентом в период семестра, когда по учебному плану изучается соответствующая дисциплина. Преподаватель осуществляет руководство и контроль выполнения курсового проекта.

Руководство со стороны преподавателя предполагает:

– определение степени подготовленности студента к написанию курсового проекта по избранной (или рекомендуемой) теме;

– оказание помощи в осмыслении тематики и содержания курсового проекта;

– выдачу рекомендаций по подбору информационных, законодательных, нормативных актов, научной и методической литературы, периодических изданий, справочных материалов и других источников;

– организацию и оказание помощи при проведении математических, и других исследований;

– консультирование по содержанию и оформлению курсового проекта;

– чтение подготовленного курсового проекта и выявление в нем недостатков и неточностей.

Выполнение предусматривает прохождение студентом процедуры проверки на объем заимствования, которую осуществляют на основании соответствующего нормативного акта университета.

Объем заимствования, в том числе содержательного, не должен превышать 50 % от общего объема пояснительной записки.

Курсовой проект представляет собой решение практической, научно-исследовательской задачи одной из актуальных проблем в области защиты информационных систем, а также в области разработки и эксплуатации автоматизированных систем в защищенном исполнении.

Законченный и оформленный в соответствии с установленными требованиями курсовой проект сдается на кафедру и передается научному руководителю, который оценивает проект и подписывает ее. К курсовому проекту студент обязан приложить заверенную личной подписью распечатку проверки текста курсового проекта в системе анализа текстов на наличие заимствований «Антиплагиат», используемой в Университете.

2.2 Выбор и утверждение темы курсового проекта

Студент выбирает тему курсового проекта из числа предложенных тем. При выборе темы курсового проекта (КП) необходимо учесть возможность дальнейшего ее развития, углубления и конкретизации, а также использования в курсовом проекте. Каждый студент выполняет индивидуальное задание, которое выдается ему преподавателем. Тема курсового проекта, ее примерное содержание обсуждаются с преподавателем курса не позднее, чем за три месяца до срока защиты первый вариант курсового проекта – не позднее, чем за один месяц до срока сдачи/защиты работы.

Студент может предложить свою тему с обоснованием целесообразности ее разработки и при согласовании с заведующим кафедрой и/или научным руководителем.

По результатам выполнения задания оформляется пояснительная записка. После проверки пояснительной записки преподавателем студент защищает выполненный курсовой проект с получением итоговой оценки.

Список типовых тем приведен **в приложении А.**

При выборе темы курсового проекта необходимо учитывать следующие условия:

- соответствие темы курсового проекта содержанию дисциплины, по которой выполняется курсовой проект; актуальность проблемы;
- наличие специальной литературы и возможность получения фактических данных, необходимых для анализа;
- собственные научные интересы и способности обучающегося;
- преемственность исследований, начатых в предыдущих курсовых проектах (работах) и в период учебных практик;
- исключение по возможности дублирования (дословного совпадения формулировок) тем курсовых проектов, выполняемых обучающимися учебной группы.

Также при самостоятельном определении темы студенту требуется учесть свой опыт в выбранной сфере, наличие соответствующих знаний и навыков, а также имеющихся знаний по предполагаемой тематике.

Обучающиеся могут выполнять групповые курсовые проекты (от 2 до 3 студентов в группе). Состав групп утверждается заведующим кафедрой с учетом действующей нормативов планирования учебной нагрузки.

По всем текущим вопросам проводятся регулярные консультации. Студенту следует периодически информировать руководителя о ходе выполнения курсового проекта, консультироваться по вызывающим затруднения или сомнения теоретическим и практическим вопросам, обязательно ставить в известность о возможных проблемах в выполнении проекта и его содержания. Изменение выбранной ранее темы курсового проекта допускается при согласовании с преподавателем этого вопроса.

Курсовой проект предусматривает **следующие этапы:**

1). Подготовка к выполнению курсового проекта заключается в изучении литературы по выбранной проблеме, сборе исходных данных по рассматриваемым проблемам. На этом этапе изучаются цели функционирования объекта проектирования, состояние защиты, уязвимости, Студент собирает, обобщает и систематизирует материалы, необходимые для разработки предложений, определяет задачи проектирования. Полученные материалы используются во введении и аналитической части проекта.

2). Разработка темы. На основе собранных и обобщенных материалов формулируются способы решения задач и разрабатываются алгоритмы решения задач, определяется специфика и порядок их реализации, реализуются предложенные решения, обосновывается эффективность разработки, исследований, решений.

3). Оформление курсового проекта.

При этом выполняется:

– систематизация материалов курсового проекта;

– отбор материала для оформления содержательной части проекта и составление структуры ее изложения, подготовка необходимого иллюстративного материала и т. д.;

– определение направлений и основного содержания предложений, выявление необходимости дополнительного сбора материалов; формирование чернового варианта разработки в целом;

– сбор дополнительных материалов, детальная разработка и обоснование выдвинутых предложений;

– уточнение аналитической и исследовательской части проекта;

– редактирование и окончательное оформление отобранного материала;

– оформление иллюстративного материала.

В **приложении Б** приведены характеристики предметной области при разработке и эксплуатации автоматизированных систем в защищенном исполнении в различных организациях.

4). Заключительным этапом подготовки курсового проекта к защите является предъявление ее преподавателю. К этому моменту курсовой проект должен быть подписан студентом.

3. СТРУКТУРА И СОДЕРЖАНИЕ КУРСОВОГО ПРОЕКТА

Основным требованием, предъявляемым к содержанию курсовых проектов, является их актуальность, направленность на решение конкретных задач разработки, внедрения и оценки эксплуатационных параметров автоматизированных систем в защищённом исполнении с использованием достижений науки и техники, а также их основным направлением будущей деятельности специалиста.

Внутреннее содержание курсового проекта должно свидетельствовать о достаточно высокой теоретической подготовке студента, которую он должен иметь на данном курсе. Проект должен иметь правильно составленную библиографию, логичную структуру, обеспечивающую раскрытие темы. Должен быть написан грамотно, хорошим литературным и профессиональным языком, иметь правильно оформленный инструментальный аппарат.

Минимальный объем курсового проекта 20 печатных тысяч знаков, 25 страниц (шрифт 14 пт., полуторный интервал, отступ 1,27).

Курсовой проект имеет свою структуру, сохранение которой обязательно и содержит следующие элементы:

- титульный лист;
- содержание (оглавление);
- введение;

– основную часть;
– заключение;
– список использованных источников;
– приложения.

Титульный лист курсового проекта содержит следующие элементы **(приложение В)**:

– полное наименование вышестоящего органа (Федеральное Агентство по рыболовству);

– университета (федеральное государственное бюджетное образовательное учреждение высшего образования «Калининградский государственный технический университет» либо ФГБОУ ВО «КГТУ»);

– института (Институт цифровых технологий);

– кафедры («Информационная безопасность»);

– название дисциплины («Разработка и эксплуатация автоматизированных систем в защищённом исполнении»);

– модуля («Методы и средства обеспечения информационной безопасности автоматизированных систем»);

– название темы курсового проекта (проекта);

– сведения об исполнителе (Ф.И.О. обучающегося, группа, подпись);

– сведения о научном руководителе (Ф.И.О., ученая степень, ученое звание);

– наименование места и год выполнения.

Содержание (Оглавление) включает в порядке следования все основные разделы и подразделы (параграфы, при этом знак § не ставится) курсового проекта, начиная с введения и заканчивая списком использованных источников и литературы или приложением, с указанием страниц, на которых они начинаются **(приложение Г)**.

Параграфы являются заголовками подразделов и пунктов, начинаются с абзацного отступа, печатаются с прописной буквы вразрядку, не подчеркивая без точки в конце (ГОСТ 7.32−2001) [21]. Если заголовок включает несколько предложений, их разделяют точками. Переносы слов в заголовках не допускаются.

Все заголовки отделяются от основного текста и других заголовков одной пустой строкой.

Каждая глава начинается с нового листа (страницы).

Главы и параграфы работы следует нумеровать арабскими цифрами. Главы должны иметь порядковую нумерацию в пределах всего текста (за исключе-

нием приложений). Номер параграфа включает номер главы и порядковый номер параграфа, разделенные точкой (например, *1.1, 1.2, 1.3* и т. д.). После номера главы, параграфа, пункта и подпункта в тексте точку не ставят. Заголовки третьего уровня в работе не используются (**приложение Д**).

Слово «СОДЕРЖАНИЕ» пишется прописными буквами, располагается по центру. Каждую запись содержания оформляют как отдельный абзац, выровненный «по ширине».

Номера страниц выровнены по правому краю поля и соединяют с наименованием структурного элемента или раздела отчёта посредством отточия.

Обозначения подразделов приводят после абзацного отступа, равного двум знакам, относительно обозначения разделов. Обозначения пунктов приводят после абзацного отступа, равного четырём знакам относительно обозначения разделов. При необходимости продолжение записи заголовка раздела, подраздела или пункта на второй (последующей) строке выполняют, начиная от уровня начала этого заголовка на первой строке.

Принятые в проекте малораспространенные условные обозначения, сокращения, символы, единицы и специфические термины необходимо представлять в виде отдельного списка. Если сокращения, условные обозначения, символы, единицы и термины повторяются в проекте не менее трех раз, отдельный список не составляют, а расшифровку дают непосредственно в тексте при первом упоминании.

Введение. В этой части обосновывается *актуальность* исследуемой в курсовом проекте проблемы, дается краткий *анализ изученности проблемы*, на основании которой определяется *объект исследования, предмет исследования, цель исследования*, используемые *методы исследования*, формулируются *задачи курсового проекта*, обозначается структура проекта.

Приводятся сведения о назначении в области применения разрабатываемой системы информационной безопасности. Анализируются современное состояние и тенденции развития информационной безопасности информационных систем.

При разработке введения рекомендуется показать:

– развитие технологий защиты информации в предметной области;

– роль и возможности современного программного обеспечения;

– значимость использования систем защиты данных, информационных систем и компьютерных сетей в определённой предметной области;

– значимость и актуальность подготовки специалистов в области защиты информации автоматизированных систем и компьютерных сетей;

– возможности и важность модернизации защиты компьютерных сетей;

– необходимость в разработке сегодня технической документации и рекомендаций по обслуживанию, модернизации компьютерных сетей и информа-

ционных систем.

Введение не нумеруется. Слово «ВВЕДЕНИЕ» пишется прописными буквами без точки в конце и центрируется.

Актуальность темы исследования определяется обоснованием теоретической и практической важности выбранной для исследования проблемы. Актуальность базируется на результатах анализа степени изученности проблемы в отечественной и зарубежной литературе. Освещение актуальности (обоснования) темы не должно превышать 0,5–1 страницы введения.

Например, *«Актуальность темы заключается в необходимости обеспечения информационной безопасности в локально-вычислительных сетях посредством внедрения аппаратных средств защиты и программного обеспечения*».

Анализ изученности проблемы заключается в перечислении основных точек зрения, подходов и методологических основ исследований различных авторов, изучавших данную проблему.

Объект исследования – явление (процесс), которое создает изучаемую проблемную ситуацию и существует независимо от исследователя. Это то, на что направлено данное исследование.

Например, «*Информационная инфраструктура общества (информационные коммуникации, сети связи, центры анализа и обработки данных, системы и средства защиты информации)*».

Предмет исследования – формулировка конкретного вопроса или анализируемой проблемы. Это наиболее значимая часть (сторона) объекта, на которую направлено основное внимание исследователя. Предмет исследования обычно содержит центральный вопрос проблемы. Им могут быть наиболее значимые с теоретической, методологической, практической точки зрения свойства, стороны, особенности объекта, которые подлежат непосредственному изучению.

Например, объект «*Организация защиты информации в локально-вычислительной сети бюджетного учреждения здравоохранения*», предмет «*Методы и средства организации защиты информации в локально-вычислительной сети бюджетного учреждения здравоохранения*».

Цель исследования – образ желаемого результата исследования, отражающий главный итог выполняемой исследовательской и практической деятельности. Цель ориентирует студента на конечный результат работы и может содержать определенную новизну.

Например, «*На основе теоретического материала, приобретенного из различных литературных источников, разработать рекомендации по защите*

информации в локально-вычислительной сети бюджетного учреждения здравоохранения».

Методы исследования (желательно) – это набор теоретических и практических приемов, с помощью которых получают определенные знания, умения и навыки, а также собирают данные. То есть, это все те способы решения задач курсового проекта и достижения поставленной в исследовании цели.

Способы достижения цели исследования:

– теоретические (моделирование, абстрагирование, анализ и синтез, от простого к сложному);

– эмпирические (наблюдение, сравнение, эксперимент, тестирование, интервьюирование);

– математические (статистические, сетевое моделирование, программирование, визуализация).

Задачи курсового проекта формулируют вопросы, на которые должен быть получен ответ для реализации цели исследования. Они конкретизируют цель исследования, раскрывая пошаговый алгоритм достижения поставленной цели, в них отражаются не только общие этапы работы, но и значение полученных промежуточных выводов для понимания общей проблемы исследования. Формулировки задач необходимо делать как можно точнее, поскольку они тесным образом связаны с формулировкой глав и параграфов. Рекомендуется для курсового проекта формулировать не более 3–5 задач.

При формулировке цели и задач необходимо использовать следующие слова и выражения: «*проанализировать, разработать, обобщить, систематизировать, выявить, доказать, внедрить, показать, выработать, изыскать, найти, исследовать, определить, описать, установить, выяснить, установить взаимосвязь, сделать прогноз»* и т. п.

Дальнейшее содержание «Введения» определяется основной образовательной программой, частные требования к нему оговариваются непосредственно с научным руководителем.

Объем «Введения» должен быть не более двух страниц печатного текста. Для более четкого уяснения основных методологических характеристик введения рекомендуется запомнить вопросы, на которые они отвечают.

Актуальность – «Почему именно сегодня (в настоящее время) данную тему необходимо изучать?»

Объект исследования – «Какое явление будет исследоваться?»

Предмет исследования – «С какой стороны (какой аспект (срез)) исследуемого явления будет раскрыт?»

Проблема – «Что в выбранной области недостаточно изучено и разобрано, либо вообще не изучалось?»

Цель – «Какой результат необходимо достичь в процессе исследования?»

Задачи – «Что нужно сделать для достижения цели курсового проекта?»

Образец оформления введения в части изложения, касающейся актуальности темы исследования, предмета и объекта исследования, а также постановки целей и задач, приведён в **приложении Е.**

Структура работы – краткое содержание глав и параграфов основной части работы. Последовательность рубрик должна соответствовать приведенному перечню, наименование каждой рубрики выделяется в тексте жирным шрифтом.

Курсовой проект должен быть выдержан в научном стиле, который обладает некоторыми характерными особенностями. Прежде всего, для стиля подобных работ характерно использование конструкций, исключающих употребление местоимений первого лица единственного и множественного числа, местоимений второго лица единственного числа. В данном случае необходимо использовать неопределенно-личные предложения (например, «*Сначала производят отбор факторов для анализа, а затем устанавливают их влияние на показатель»*), формы изложения от третьего лица (например, «*Автор полагает...»*), предложения со страдательным залогом (например, *«Разработан комплексный подход к исследованию...»*) [26].

В тексте нельзя использовать разговорно-просторечную лексику.

Необходимо применять терминологические названия. Если есть сомнения в стилистической окраске слова, лучше обратиться к словарю.

Важнейшим средством выражения смысловой законченности, целостности и связности научного текста является использование специальных слов и словосочетаний.

Подобные слова позволяют отразить следующее:

– последовательность изложения мыслей (*вначале; прежде всего; затем; во-первых, во-вторых; значит; итак,*);

– переход от одной мысли к другой (*прежде чем перейти к; обратимся к; рассмотрим; остановимся на; рассмотрев; перейдем к; необходимо остановиться на; необходимо рассмотреть*);

– противоречивые отношения (*одна; между тем; в то время как; тем не менее*);

– причинно-следственные отношения (*следовательно, поэтому; благодаря этому; сообразно с этим; вследствие этого; отсюда следует, что*);

– различную степень уверенности и источник сообщения (*конечно; разумеется, действительно; видимо; надо полагать; возможно; вероятно; по сообщению; по сведениям; по мнению; по данным*);

– итог, вывод (*итак; таким образом; значит; в заключение отметим; все сказанное позволяет сделать вывод; подведя итог, следует сказать; резюмируя сказанное, отметим*).

Для выражения логической последовательности используют сложные союзы: *благодаря тому, что; между тем как; так как; вместо того чтобы; ввиду того что; оттого что; вследствие того, что; после того как; в то время, как* и др.

Особенно употребительны производные предлоги *в течение; в соответствии с; в результате; в отличие от; наряду с; в связи с; вследствие* и т. п.

В качестве средств связи могут использоваться местоимения, прилагательные и причастия (*данные; этот; такой; названные; указанные; перечисленные*).

В речи очень распространены указательные местоимения *«этот», «тот», «такой»*.

Местоимения *«что-то», «кое-что», «что-нибудь»* в тексте научной работы обычно **не используются**.

Для выражения логических связей между частями научного текста используются следующие устойчивые сочетания: *приведем результаты; как показал анализ; на основании полученных данных*.

Для образования превосходной степени прилагательных чаще всего используются слова *«наиболее», «наименее»*.

Не употребляется сравнительная степень прилагательного с приставкой по- (например, *повыше, побыстрее*).

Особенностью научного стиля является констатация признаков, присущих определяемому слову. Так, прилагательное «следующие», синонимичное местоимению «такие», подчеркивает последовательность перечисления особенностей и признаков (например, «Рассмотрим следующие факторы, влияющие на формирование рынка труда») [26].

Изложение материала в курсовой работе должно быть последовательным и логичным. Все главы должны быть связаны между собой. Особое внимание следует обращать на логические переходы от одной главы к другой, от параграфа к параграфу, а внутри параграфа – от вопроса к вопросу.

Основная часть курсового проекта может содержать следующие части:

- главы;
- разделы (параграфы);
- пункты;
- подпункты.

Каждый элемент основной части должен представлять собой законченный в смысловом отношении фрагмент курсового проекта.

Разделы (параграфы) курсового проекта в рамках соответствующей главы должны быть взаимосвязаны. Рекомендуется, чтобы каждая глава заканчивалась выводами, позволяющими логически перейти к изложению следующего материала.

Задачи, решаемые в рамках конкретной курсового проекта в области безопасности информационных систем, содержат определённую специфику, которая должна быть отражена в главах основной части дипломной проекта.

Как правило, в первой главе содержится понятие раскрываемого вопроса, содержание избранной темы. Дается характеристика, функциональная и организационная структура организации (объекта). Далее описываются общая характеристика процесса управления и его концептуальная модель, общая характеристика автоматизированной системы (АС) или подсистемы, к которой относится разрабатываемая в проекте задача управления. Разрабатываются общая функциональная структура подсистемы и ее характеристика, перечень и краткая характеристика функциональных задач; взаимосвязь задач проектируемой функциональной подсистемы. Должны быть дана характеристика ее информационного обеспечения, математическое, программное и техническое обеспечение, включая описание и краткую характеристику структурной схемы локальной сети компьютеров.

В конце главы студент делает свой вывод о том, как им понимается данный вопрос или почему он разделяет мнение того или иного автора и не согласен с другими.

Вторая глава должна иметь полностью практико-исследовательскую направленность. Ее название может быть близко, но не тождественно формулировке темы, с прибавлением фразы типа *«Результаты анализа…».* Это описание данных анализа с необходимыми итоговыми (обобщающими) таблицами, графиками и диаграммами, а также интерпретация этих данных. Процесс интерпретации – это наполнение смыслами числовых данных, с точки зрения теории, в контексте поставленной цели исследования.

Задачами этой части курсового проекта являются раскрытие и решение практических задач изучаемых явлений или процессов в области защиты информационных систем. Практическая часть должна содержать эксперимент, позволяющей продемонстрировать особенности предложенного решения, характеристики методов экспериментальной проекта, обоснование выбранного метода, основные этапы эксперимента, обработка и анализ результатов. Также излагаются соответствующие предложения, меры, нивелирующие рассматриваемые угрозы с их экспериментальной проверкой (если угрозы невозможно ни-

велировать, должен быть дан прогноз по возможным методам блокирования данных угроз).

Заканчивается глава выводом (собственным мнением студента) по исследуемой проблеме.

В основной части курсового проекта описывается сущность предмета исследования, его современное состояние и тенденции развития. На основе обзора учебной и специальной научной литературы оценивается степень изученности исследуемой проблемы. Сопоставляются различные мнения, высказывается собственная точка зрения по дискуссионным (по-разному освещаемым в научной литературе) и нерешенным вопросам. Содержание этой части должно показать степень ознакомления обучающегося с поставленной проблемой и современным научно-теоретическим уровнем исследований в данной области, а также умение работать с фактическим материалом, сжато и аргументированно формулировать задачи и результаты исследований и давать обоснованные рекомендации по решению выявленных проблем.

Основная часть курсового проекта должна включать графическую часть (чертежи) и расчётно-пояснительную записку. При необходимости, графическая часть (чертежи) могут быть вынесены в приложение.

Основные теоретические положения и выводы следует иллюстрировать цифровыми и статистическими данными из статистических справочников, монографий, журнальных статей и других источников.

При подборе и обработке статистических данных следует помнить, что они являются ценными только в том случае, если подтверждают или опровергают какие-либо выводы и обобщения в курсовом проекте.

Пользоваться рекомендуется официальными государственными статистическими данными и специализированными сборниками и справочниками в сфере информационной безопасности. Наряду с официальными статистическими сообщениями можно также использовать фактические данные из книг, брошюр, газетных и журнальных статей с учетом их сопоставимости.

Хорошо подобранный фактический материал позволяет объяснить многие процессы и выявить закономерности их развития. Поэтому, очень важно правильно проанализировать его, научно обработать, привести к самостоятельным единицам измерения. Особенно внимательно нужно быть к данным из различных источников, обратить внимание на их сопоставимость.

Не следует приводить большого количества цифрового материала. Логичнее всего, если он представлен в виде 2–3 таблиц, графиков или диаграмм с пояснениями, анализом и выводами. Все таблицы, графики, диаграммы должны быть пронумерованы, озаглавлены, и иметь ссылку на источник.

Каждая глава должна содержать не менее двух и не более пяти структурных элементов (разделов или параграфов). При этом необходимо стремиться к

пропорциональному (по объему) распределению материала между главами и внутри них.

Между главами и параграфами должна быть органичная внутренняя связь, логическая последовательность. Каждый параграф завершается обобщающим резюме, глава – выводом по ее содержанию, весь курсовой проект – выводами (теоретическими и практическими по всей работе), которые соотносятся с задачами и целью, символизируя, что задачи решены, цель достигнута.

Таким образом, теоретическая часть работы (глава 1) – это результат тщательного детального «разбора» проблемы, подлежащей исследованию в курсовой работе, что послужило бы основанием не только для разработки и реализации собственного исследования, но и применения полученных научных результатов в практической деятельности (глава 2).

Заключение – краткое изложение основных, наиболее существенных результатов проведенного анализа, сформулированных в виде выводов, соответствующих цели и поставленным во введении задачам исследования.

Написанию этого раздела придается особое значение, так как в нем представляются итоговые результаты проведенной работы. Выводы должны содержать результаты анализа данных по теоретической и практической части курсового проекта. В «Заключении» рекомендуется представить 5–6 выводов общей и конкретной формы, содержащие главные достижения автора курсового проекта.

Слово «ЗАКЛЮЧЕНИЕ» пишется прописными буквами без точки в конце и центрируется. Типовой объем заключения составляет 1–2 страницы.

В **списке использованных источников** должны быть представлены основные источники по теме: нормативно-правовые акты, учебная литература, монографические исследования, статьи и др., в том числе переведенные на русский язык и на языке оригинала, статистические издания, справочники и интернет-источники. Список должен содержать не менее 15 современных источников, изученных студентом.

Подбор литературы целесообразно начинать с изучения тех работ, которые близки к выбранной студентом тематике. Знакомиться с литературой рекомендуется в следующей последовательности:

- руководящие документы – вначале законы, затем законодательные акты;
- научные издания – сначала монографии, затем периодические издания;
- статистические данные.

При этом вначале стоит изучить самые свежие публикации, затем – более ранние. При выполнении курсового проекта студент обязан использовать материалы по исследуемому предмету, опубликованные в печати не позднее пяти лет с момента издания.

При подборе нормативно-правовых актов желательно использовать возможности тематического поиска документов в справочной правовой системе «Гарант» и «Консультант плюс». Данные справочно-информационные системы значительно облегчают тематический поиск необходимых нормативных документов.

Со статистическим и аналитическим материалом, связанным с информационной безопасностью, можно ознакомиться в Интернете с обязательным указанием адреса электронного ресурса. Рекомендуется широко использовать периодические издания в сфере защиты информации, например, журналы: «Защита информации. Инсайд», «Системы безопасности», «Защита персональных данных», «Информационная безопасность», «Вопросы кибербезопасности», «Проблемы информационной безопасности. Компьютерные системы», «Безопасность информационных технологий» и т. п.

На основные приведенные в списке источники должны быть ссылки в тексте курсового проекта. Источники в списке нумеруются в порядке появления ссылок в тексте. При оформлении библиографического описания источников в списке необходимо руководствоваться ГОСТ Р 7.0.100-2018 «Библиографическая запись. Библиографическое описание. Общие требования и правила составления» [26].

При подборе литературы необходимо сразу составлять библиографическое описание отобранных изданий в строгом соответствии с требованиями, предъявляемыми к оформлению списка использованных источников. (**Приложение Ж)**.

Словосочетание «СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ» пишется прописными буквами без точки в конце и центрируется.

Приложения – вспомогательные иллюстративно-графические, табличные, расчетные и текстовые материалы, которые нецелесообразно (объем более 1 страницы) приводить в основном тексте курсового проекта.

Этот раздел необходим для некоторых детальных, иллюстрационных и других дополнительных материалов, полученных, используемых студентом при написании работы. Приложения помещают в конце курсового проекта.

Номера приложений обозначаются арабскими цифрами без знака «№». Нумерация каждого приложения осуществляется в порядке появления ссылок на них в тексте работы. Размеры приложений не регламентируются, так как они не входят в общий объем курсового проекта. Каждое приложение должно начинаться с новой страницы с указанием в правом верхнем углу слова «ПРИЛОЖЕНИЕ» и иметь тематический заголовок. Нумерация страниц, на которых даются приложения, должна быть сквозной и продолжать общую нумерацию страниц основного текста. Связь основного текста с приложениями осуществляется через ссылки. Например, ПРИЛОЖЕНИЕ В.

Каждое приложение обычно имеет самостоятельное значение и может использоваться независимо от основного текста. Отражение приложения в оглавлении работы допускается использовать в виде самостоятельной рубрики с полным названием каждого приложения.

Как правило, в приложении помещается материал, который в основной части курсового проекта загромождает текст, затрудняет его восприятие *(например, таблица, имеющая размер более одной страницы и др.)*

Приложения содержат материал, представляющий конкретные доказательства проделанной работы, являющийся доказательством достоверности и адекватности, полученных результатов, на основе которых сделаны выводы. Вместе с тем, все итоги исследования и практического применения его результатов важные для понимания и доказательства выводов, помещаются в основной текст работы, суть которых должна быть понятна даже без обращения к приложению.

4. ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ КУРСОВОГО ПРОЕКТА

4.1 Оформление текста курсового проекта

Курсовой проект должна быть напечатан на одной стороне листа белой бумаги формата А4. Цвет шрифта должен быть черным.

При компьютерном наборе рекомендуется кегль 14, полуторный междустрочный интервал, гарнитура шрифта – Times New Roman Cyr.

Размеры верхнего и нижнего полей – 20 мм, левого поля – 30 мм, правого – 15 мм. Абзацный отступ равен 1,25 см. Основной текст работы должен быть выровнен по ширине.

Нумерация страниц производится сквозным способом по всему тексту работы, начиная с титульного листа, но цифры печатаются только с третьего листа (в центре или справа нижней части листа, без точки).

Внутри текста работы **не допускается** использование фамилий без инициалов. Инициалы всегда (кроме «СПИСКА ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ») должны стоять перед фамилией автора через пробел. (Например, *И. И. Иванов*).

В тексте разрешено использовать только кавычки «елочки» (не допускается применять кавычки “лапочки”), дефис – «-», среднее тире «−» (ctrl «минус» на боковой клавиатуре с цифрами).

Длинное тире «—» в работе использовать **не допускается**.

В тексте ВКР допустимо использовать общепринятые сокращения, например, и так далее – «и т. д.», тысяч рублей «тыс. руб.», век – «в.», год – «г.», годы – «гг.» и т. п.

Нельзя употреблять в тексте знаки (<,>, =, №, %) без цифр, а также использовать в тексте математический знак минус (–) перед отрицательными значениями величин: в этом случае следует писать слово «минус».

В тексте используются только арабские цифры, но при нумерации кварталов, полугодий допускается использование римских цифр. При обозначении веков используются только римские цифры, например, *XX в.*

При записи десятичных дробей целая часть числа от дробной должна отделяться запятой (например, 15,6 тыс. руб., 18,5 м²).

4.2 Оформление ссылок

Важным моментом при написании курсового проекта является оформление ссылок на используемые источники. При использовании в тексте информации из источника, описание которого включено в список литературы, в тексте работы необходимо сделать ссылку.

При цитировании текста цитата приводится в кавычках, а после нее в квадратных скобках указывается ссылка на литературный источник по списку использованной литературы и номер страницы, на которой в этом источнике помещен цитируемый текст. Например, [15, с. 237–239]. При ссылке на источник после упоминания о нем в тексте работы проставляют в квадратных скобках номер, под которым он значится в списке литературы. В необходимых случаях указываются и страницы. При оформлении ссылок на положения нормативных правовых актов в квадратных скобках вместо номера страницы указывается номер соответствующей статьи (пункта) документа с обозначением символа «ст.» («п.»).

При этом следует учесть, что выбранный формат используемых ссылок должен во всей работе быть одинаковым.

При ссылках на таблицы, рисунки, приложения следует писать: «в соответствии с данными таблицы 1», «... по формуле 2».

4.3 Оформление перечислений

В курсовом проекте могут быть приведены перечисления, которые выделяются абзацным отступом. Перед каждой позицией перечисления ставится дефис или строчная буква со скобкой, приводимая в алфавитном порядке. Для дальнейшей детализации перечисления используют арабские цифры, после которых ставят скобку, приводя их со смещением вправо на два знака относительно перечислений, обозначенных буквами.

Например:
Информационная безопасность состоит из трех основных компонентов:
а) конфиденциальность;
б) целостность;
в) доступность.

4.4 Оформление таблиц

Цифровой материал, как правило, оформляют в виде таблиц, что обеспечивает лучшую наглядность и удобство сравнения показателей. Таблицу в зависимости от ее размера обычно помещают под текстом, в котором впервые дана на нее ссылка. Если объем таблицы превышает количество оставшегося места в конце страницы, то ее размещают на следующей странице, а свободное место заполняется текстом, следующим за таблицей. Каждая таблица должна иметь заголовок, точно и кратко отражающий ее содержание.

Все таблицы в курсовой работе имеют сквозную нумерацию арабскими цифрами. Например, «Таблица 1», «Таблица 2». При наличии в тексте единственной таблицы номер ей не присваивается.

Название таблицы следует помещать над таблицей слева, без абзацного отступа в одну строку с ее номером через дефис **(приложение 3).**

Если таблица переносится на следующий лист, следует пронумеровать графы и повторить их нумерацию на следующей странице, при этом над перенесенной частью размещают слова «Продолжение таблицы» с указанием ее номера **(приложение 3)**.

В ячейках таблицы:

− допускается применять меньший размер шрифта, чем в основном тексте (до 11 пт);

− одинарный междустрочный интервал;

− не должно быть абзацного отступа;

− цифровые значения необходимо выравнивать по центру, буквенные – по левому краю;

− центровка производить по горизонтали и вертикали.

Заголовки граф и строк таблицы должны начинаться с прописной буквы, а подзаголовки граф – со строчной буквы, если они составляют одно предложение с заголовком. Подзаголовки, имеющие самостоятельное значение, начинаются с прописной буквы. В конце заголовков и подзаголовков граф и строк точки не ставят. Не допускается выделение курсивом или полужирным шрифтом заголовков граф и строк таблиц, а также самих табличных данных.

К цифровым табличным данным должны быть указаны единицы измерения. Если данные таблицы имеют разные единицы измерения, то они указываются в соответствующих заголовках (подзаголовках) граф или строк таблицы. Цифровые значения в графах таблиц проставляют так, чтобы разряды чисел по всей графе были расположены один под другим. В одной графе следует соблюдать одинаковое количество десятичных знаков для всех значений величин. При отсутствии отдельных данных в таблице следует ставить прочерк. Если данные графы (строки) таблицы не требуют заполнения, то следует ставить знак «х». Для облегчения пользования таблицей допускается проводить горизонтальные линии, разграничивающие строки таблицы.

Ширина таблицы должна соответствовать ширине основного текста. При превышении ширины таблицу следует размещать в альбомном формате по тексту или в приложении.

Не допускается при переносе отделять заголовок таблицы от самой таблицы, оставлять на странице только «шапку» таблицы без записи хотя бы одной строки табличных данных. Итоговая строка также не должна быть отделена от таблицы.

4.5 Оформление иллюстраций

В качестве иллюстраций в курсовом проекте могут быть представлены чертежи, схемы, диаграммы, рисунки, фотографии и т. п. Все иллюстрации обозначают в тексте словом «Рисунок».

Иллюстрации могут быть выполнены как в черно-белом, так и в цветном варианте. Рисунки в зависимости от их размера располагают в тексте непосредственно после того абзаца, в котором данный рисунок был впервые упомянут, или на следующей странице, а при необходимости – в приложении. Рисунок должен располагаться в центре.

Все рисунки должны иметь наименование, которое помещают под иллюстрацией. Перед наименованием вводят слово «Рисунок» (с заглавной буквы), затем пробел, после чего указывают номер рисунка. Слово «Рисунок» начинают печатать с абзацного отступа (**приложение И**).

Рисунки должны иметь сквозную нумерацию по всему тексту. После номера рисунка также должна ставиться точка, затем пробел и наименование рисунка, которое печатают строчными буквами (кроме первой прописной). Точку в конце наименования рисунка не ставят.

Нумерация рисунков проводится отдельно от нумерации таблиц.

Если иллюстрация заимствована из книги или статьи, на нее в конце наименования рисунка должна быть оформлена ссылка.

Например,

Рисунок 1 – Перевозки грузов по видам транспорта общего пользования в Калининградской области, тыс. т [1, с. 15]

Печать основного текста после наименования рисунка начинается через один полуторный междустрочный интервал.

4.6 Оформление формул

При необходимости в тексте курсового проекта могут быть использованы формулы. Формулы следует выделять из текста в отдельную строку. Между текстом и следующей за ним формулой, между формулой и следующим за ним текстом должно быть расстояние, равное одному полуторному междустрочному интервалу. Переносить формулы на следующую строку допускается только на знаках выполняемых математических операций, причем знак в начале следующей строки повторяют.

Формулы имеют сквозную нумерацию по всему тексту. После номера формулы точка не ставится. Номер печатают арабскими цифрами в круглых скобках справа от формулы, на одном уровне с ней. При написании формул следует использовать буквенные символы.

Пояснения символов и числовых коэффициентов, входящих в формулу (если соответствующие пояснения не использованы ранее в тексте), приводят непосредственно под формулой.

Пояснения каждого символа приводят с новой строки в той последовательности, в которой эти символы приведены в формуле. Первую строку пояснения начинают со слова «где» с двоеточием после него. После самой формулы перед пояснениями необходимо ставить запятую.

Например,

Сумма интенсивностей отказов рассчитываться следующим образом:

$$Y = \sum_{i=1}^{n} y_i, \quad (1)$$

где Y – интенсивность отказов комплекса средства защиты;

y_i – интенсивность отказа отдельного средства защиты (средства ИБ можно объединять в группы, избегая излишней детализации при необходимости).

4.7 Оформление списка использованных источников

В конце курсового проекта располагается Список использованных источников, который позволяет автору документально подтвердить достоверность приводимых материалов и показывает степень изученности проблемы **(приложение К).**

В Список использованных источников и литературы включаются только те публикации, которые непосредственно изучались при написании работы. На каждый источник, указанный в списке литературы, в тексте должна быть ссылка. Каждый документ, включенный в список, должен быть описан в соответствии с требованиями ГОСТ Р 7.0.100-2018.

Каждая библиографическая запись в списке получает порядковый номер и начинается с красной строки. Список имеет сквозную единую нумерацию арабскими цифрами.

Расположение источников рекомендуется приводить в следующей последовательности:

– нормативные акты международного уровня (в порядке обратной хронологии опубликования документов):

а. Конституция;

б. кодексы;

в. нормативные акты федерального уровня:

1) Федеральные Законы;

2) Указы Президента;

3) Постановления Правительства;

4) инструкции министерств и ведомств.

г. нормативные акты регионального уровня:

1) законы законодательных органов субъектов Федерации;

2) указы губернаторов краев, областей, президентов республик;

3) постановления администрации краев, областей, правительств республик.

д. нормативные акты местного уровня:

1) решения органов местного самоуправления;

2) корпоративные акты (внутриорганизационные, внутрифирменные).

– документальные материалы, составляющие источниковую базу исследования (архивные документы, летописи, письма, дневники, воспоминания, статистические сборники, ежегодники, материалы социологических исследований и т. п.) – в хронологическом порядке;

– перечень отечественной и зарубежной литературы по теме (книги, статьи, сообщения, тезисы докладов, депонированные рукописи, препринты, нор-

мативно-техническая документация, электронные ресурсы и пр.) – по алфавиту того языка, на котором дается библиографическая запись документа.

В списке использованных источников нормативные правовые акты одинаковой юридической силы располагаются в хронологическом порядке по мере их принятия (от ранее принятых к более поздним документам).

При библиографическом описании нормативных правовых актов сначала указывается статус документа (например, Федеральный закон, Указ Президента РФ и т. п.), затем его название, после чего приводится дата принятия документа, номер и дата его последней редакции.

Специальная литература включает монографии, статьи, диссертации, авторефераты диссертаций, книги, статистические сборники, статьи в периодических изданиях.

Информация, размещенная в Интернете, является электронным ресурсом удаленного доступа и может также использоваться при составлении списка литературы.

4.8 Оформление приложений

Приложение – заключительная часть работы, которая имеет дополнительное, обычно справочное значение, но является необходимой для более полного освещения темы. По содержанию приложения могут быть очень разнообразны: копии подлинных документов, выдержки из отчетных материалов, отдельные положения из инструкций и правил и т. д. По форме они могут представлять собой текст, таблицы, графики, карты.

Приложения размещаются после «Списка использованных источников».

Имеющиеся в тексте приложения иллюстрации, таблицы, формулы и уравнения следует нумеровать в пределах каждого приложения. Объем приложений не ограничивается.

Каждое приложение должно начинаться с нового листа (страницы) с указанием наверху посередине страницы слова «ПРИЛОЖЕНИЕ» и иметь тематический заголовок, который записывается симметрично относительно текста с прописной буквы отдельной строкой.

При наличии в проекте более одного приложения они нумеруются (без знака №), например, «ПРИЛОЖЕНИЕ А», «ПРИЛОЖЕНИЕ Б» и т. д.

В обозначении приложений не используют буквы Ё, З, Й, О, Ч, Ь, Ы, Ъ.

5. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ К СОСТАВЛЕНИЮ ПОЯСНИТЕЛЬНОЙ ЗАПИСКИ

В курсовом проекте рекомендуется построить процессную модель системы информационной безопасности организации, содержащую три уровня процессов:

- процессы стратегического уровня – управление рисками, управление непрерывностью ведения бизнеса, разработка и развитие политики ИБ верхнего уровня;
- тактические процессы – разработка и развитие процедур ИБ, технической архитектуры системы ИБ, классификация ИТ-ресурсов, мониторинг и управление инцидентами и другие;
- процессы операционного уровня – управление доступом, управление сетевой безопасностью, проверка соответствия и др.

Определяются взаимосвязи процессов. В результате должна получиться трехуровневая процессно-сервисная модель системы ИБ, соответствующую требованиям стандарта ИСО/МЭК 27001 [8]. Рекомендуется при выполнении курсового проекта ознакомиться с содержанием данного стандарта. Модель системы ИБ формализуется в едином комплексе нормативных документов.

5.1. Исходные данные к курсовому проекту

В качестве исходных данных студенты выбирают объект защиты в виде организации или предприятия (отдела), информационной системы, используемой на предприятии, локальной сети, выделенного помещения, в котором осуществляется работа с конфиденциальной информацией и т. п. Необходимо дать общую характеристику предприятия.

Затем необходимо провести предпроектное обследование системы защиты информации всей компании (если предприятие небольшое) или информационной безопасности отдельных информационных технологий – систем (сетей передачи данных, вычислительных систем и систем хранения данных, и др.) для крупной компании, рассмотрев:

- все ресурсы, на которых хранится ценная информация;
- все сетевые группы, в которых находятся ресурсы системы (т. е. физические связи ресурсов друг с другом);
- отделы, к которым относятся ресурсы;
- виды ценной информации;
- ущерб для каждого вида ценной информации по трем видам угроз: внешние, внутренние, комбинированные;

– бизнес-процессы, в которых обрабатывается информация;
– группы пользователей, имеющих доступ к ценной информации;
– класс группы пользователей;
– доступ группы пользователей к информации;
– характеристики этого доступа (вид и права);
– средства защиты информации;
– средства защиты рабочего места группы пользователей.

Кроме того, при проведении диагностического обследования/аудита системы ИБ необходимо выполнить – классификацию информационных ресурсов по степени важности/критичности лица и выявление должностных лиц, ответственных за целостность этих ресурсов [7].

Предлагаемый порядок определения требований к защищенности циркулирующей в системе информации представлен ниже:

1. Составляется общий перечень типов информационных пакетов, циркулирующих в системе (документов, таблиц). Для этого с учетом предметной области системы пакеты информации разделяются на типы по ее тематике, функциональному назначению, сходности технологии обработки и т. п. признакам. На последующих этапах первоначальное разбиение информации (данных) на типы пакетов может уточняться с учетом требований к их защищенности.

2. Затем для каждого типа пакетов, выделенного в первом пункте, и каждого критического свойства информации (доступности, целостности, конфиденциальности) определяются (например, методом экспертных оценок):

- перечень и важность (значимость по отдельной шкале) субъектов, интересы которых затрагиваются при нарушении данного свойства информации;
- уровень наносимого им при этом ущерба (незначительный, малый, средний, большой, очень большой и т. п.) и соответствующий уровень требований к защищенности.

При определении уровня наносимого ущерба необходимо учитывать:

- стоимость возможных потерь при получении информации конкурентом;
- стоимость восстановления информации при ее утрате;
- затраты на восстановление нормального процесса функционирования АС и т. д.

Если возникают трудности из-за большого разброса оценок для различных частей информации одного типа пакетов, то следует пересмотреть деление информации на типы пакетов, вернувшись к предыдущему пункту методики.

3. Для каждого типа информационных пакетов с учетом значимости субъектов и уровней наносимого им ущерба устанавливается степень необхо-

димой защищенности по каждому из свойств информации (при равенстве значимости субъектов выбирается максимальное значение уровня).

Также необходимо:

- выявить организацию системы резервного копирования;
- определить требования к системе разделения прав доступа (пароли, разрешения), включая все правила доступа к информационной системе компании;
- провести предварительный анализ уязвимостей активного сетевого оборудования, серверов, рабочих станций, межсетевых экранов;
- выполнить оценку информационных рисков.

Оценка информационных рисков – это процесс комплексной оценки защищенности информационной системы с переходом к количественным или качественным показателям рисков. При этом риск – это вероятный ущерб, который зависит от защищенности системы [34].

Таким образом, из анализа риска можно получить либо количественную оценку рисков (риск измеряется в деньгах), либо – качественную (уровни риска обычно: высокий, средний, низкий).

Пример оценки требований к защищенности некоторого типа информационных пакетов приведен в таблице.

Таблица – Оценка требований к защищенности

Субъекты	Уровень ущерба по свойствам информации			
	Конфиденциальность	Целостность	Доступность	Защита от тиражирования
N	Нет	Средняя	Средняя	Нет
N	Высокая	Средняя	Средняя	Нет
N	Низкая	Низкая	Низкая	Нет
В итоге	Высокая	Средняя	Средняя	Нет

Оценка рисков информационной безопасности осуществляется с помощью построения модели информационной системы организации с точки зрения ИБ, рассматривая средства защиты ресурсов с ценной информацией, взаимосвязь ресурсов между собой, влияние прав доступа групп пользователей, организационные меры, модель исследует защищенность каждого вида информации.

Идентифицировать и оценить активы, разработать модель нарушителя и модель угроз, идентифицировать уязвимости – все это стандартные шаги анализа рисков.

Процесс анализа рисков включает в себя выполнение следующих групп задач:

1. Анализ ресурсов ИТ-инфраструктуры, включая информационные ресурсы, программные и технические средства, людские ресурсы, и построение модели ресурсов, учитывающей их взаимозависимости.

2. Анализ бизнес-процессов и групп задач, решаемых информационной системой, позволяющий оценить критичность ИТ-ресурсов, с учетом их взаимозависимостей.

3. Идентификация угроз безопасности в отношении ресурсов информационной системы и уязвимостей защиты, делающих возможным осуществление этих угроз.

4. Оценка вероятности осуществления угроз, величины уязвимостей и ущерба, наносимого организации.

5. Определение величины рисков для каждой тройки: угроза – группа ресурсов – уязвимость.

6. Ранжирование существующих рисков.

7. Разработка системы первоочередных мероприятий по уменьшению величины рисков до приемлемого уровня на основе проводимого анализа рисков.

8. Определение угроз безопасности (внутренних и внешних) информации и разработку модели вероятного нарушителя применительно к конкретным условиям функционирования.

Первоначальную информацию о модели нарушителя, как и в случае с выбором изначальных направлений деятельности по обеспечению ИБ, целесообразно получить у высшего менеджмента компании или же из специализированных исследований по нарушениям в области компьютерной безопасности в той сфере бизнеса, в которой работает компания [12].

Разработка модели угроз – выявление всех потенциальных угроз:

– внешние источники угроз: лица, распространяющие вирусы и другие вредоносные программы, хакеры и иные лица, осуществляющие несанкционированный доступ (НСД);

– внутренние источники угроз, реализующие угрозы в рамках своих полномочий и за их пределами (персонал, имеющий права доступа к аппаратному оборудованию, в том числе сетевому, администраторы сетевых приложений и т. п.);

– комбинированные источники угроз: внешние и внутренние, действующие совместно и/или согласованно.

Наиболее актуальные источники угроз на уровнях операционных систем (ОС), систем управления базами данных (СУБД), банковских технологических процессов:

– внутренние, реализующие угрозы в рамках своих полномочий и за их пределами (администраторы ОС, администраторы СУБД, пользователи банковских приложений и технологий, администраторы ИБ и т. д.);

– комбинированные источники угроз: внешние и внутренние, действующие в сговоре.

Наиболее актуальные источники угроз на уровне бизнес-процессов:

– внутренние источники, реализующие угрозы в рамках своих полномочий и за их пределами (авторизованные пользователи и операторы АБС, представители менеджмента организации и пр.);

– комбинированные источники угроз: внешние (например, конкуренты) и внутренние, действующие в сговоре.

– определение комплекса мероприятий по ликвидации (локализации) выявленных «брешей» в системе защиты;

– определение функциональных отношений и зоны ответственности при взаимодействии подразделений и лиц по обеспечению информационной безопасности предприятия;

– подготовку итогового отчета, содержащего оценку текущего уровня информационной безопасности, выработку рекомендаций по совершенствованию системы защиты информации с приложением списка конкретных уязвимостей активного сетевого оборудования, серверов, межсетевых экранов и др.

5.2. Формирование требований к проектируемой системе защиты информации

Перед тем как приступить к проектированию автоматизированной системы информационной безопасности необходимо сформулировать требования к разрабатываемой системе.

Это можно сделать на основании результатов предпроектного обследования информационной безопасности компании (в компании должна быть разработана внутренняя нормативная документация: политика информационной безопасности, методика определения ценности или критичности для бизнеса различных данных, правила реагирования на инциденты в области нарушения информационной безопасности и т. п.) и на основе организационно-нормативной документации ФСТЭК РФ.

На основании выполненного отчета определить к какому классу защищенности СВТ или АСОД (в зависимости от того, что используется в фирме: только средства вычислительной техники или же информационные системы)

следует отнести СВТ или АСОД данной компании, чтобы реализовать выработанные рекомендации по совершенствованию системы защиты информации с приложением списка конкретных уязвимостей активного сетевого оборудования, серверов, межсетевых экранов и др.

Формирование требований к защите информации в автоматизированной системе управления осуществляется с учетом ГОСТ Р 51583 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения» (далее – ГОСТ Р 51583) [3], ГОСТ Р 51624 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования» (далее – ГОСТ Р 51624) [4], и стандартов организации.

5.3. Проектирование системы информационной безопасности

Следующим этапом построения системы ИБ является ее проектирование.

Задача проектирования системы ИБ тесно связана с понятием архитектуры системы ИБ. Построение архитектуры системы ИБ, как интегрированного решения обеспечивают ряд преимуществ: интеграция подсистем позволяет снизить совокупную стоимость СИБ, повысить коэффициент возврата инвестиций при внедрении и улучшает управляемость системы ИБ, а, следовательно, возможности отслеживания событий, связанных с ИБ.

Эффективность системы ИБ может быть достигнута, если все ее компоненты представлены качественными решениями, функционируют как единый комплекс и имеют централизованное управление. Система безопасности должна строиться на основе анализа рисков, и стоимость ее внедрения и поддержки должна быть адекватной существующим угрозам, то есть экономически обоснованной.

Интегрированная архитектура систем ИБ включает в себя набор следующих подсистем:

- подсистему защиты периметра сети и межсетевых взаимодействий (межсетевые экраны и т.п.);
- подсистему защиты серверов сети;
- средства защиты рабочих станций;
- подсистему мониторинга и аудита безопасности;
- средства обнаружения атак и автоматического реагирования;
- подсистему комплексной антивирусной защиты;
- средства анализа защищенности и управления политикой безопасности;
- средства контроля целостности данных;
- средства криптографической защиты информации;
- инфраструктуру открытых ключей;
- подсистему резервного копирования и восстановления данных;

- автоматизированную систему установки обновлений ПО;
- подсистему управления ИБ;
- подсистему аутентификации и идентификации;
- подсистему защиты внутренних сетевых ресурсов;
- подсистему защиты Web-ресурсов;
- подсистему контроля содержимого Интернет-трафика;
- подсистему физической защиты.

Проектируемая система информационной безопасности не обязательно будет содержать все подсистемы. Архитектура проектируемой системы ИБ будет определяться в соответствии с требованиями к проектируемой системе ИБ [5].

Остановимся подробнее на задачах, которые решаются с помощью компонентов комплексной системы ИБ.

Подсистема межсетевого экранирования

Система межсетевого экранирования (МЭ) обеспечивает:

- защиту от атак;
- защищенное соединение между офисами;
- защищенный удаленный доступ сотрудников к корпоративным ИТ-ресурсам.

Защита периметра корпоративной сети – первичная задача обеспечения информационной безопасности. Внутри периметра обычно функционируют наиболее критичные для компании системы – серверы с программными приложениями и базами данных, рабочие места пользователей, активное сетевое оборудование и др. Извне сеть компании должна быть абсолютно непрозрачной, иметь регламентированные интерфейсы и протоколы взаимодействия с «внешним миром».

Решая эту задачу, необходимо оградить компанию от сетей с низкой степенью доверия и при этом обеспечить легитимным пользователям удаленный доступ к внутренним ИТ-ресурсам компании.

Территориально распределенные офисы компании должны взаимодействовать через защищенные (доверенные) каналы связи, которые защищены от внешних угроз физически или средствами криптографии. Практикой доказано, что экономически выгодно и эффективно использование технологии виртуальных частных сетей (VPN). VPN позволяют скрывать структуру и передаваемый в защищенном канале трафик, поэтому их можно включать в защищенный периметр сети.

Создание непрозрачной сферы, ограждающей сеть компании, реализуется средствами межсетевого экранирования. Такое решение называется шлюзом безопасности. У шлюзов безопасности есть и другие полезные возможности:

балансировка нагрузки на внутренних серверах сети и использование аппаратных ускорителей криптографических операций.

Выбор конкретного решения для обеспечения безопасности периметра, естественно, зависит от размера компании. Для малого офиса, филиала компании или удаленной группы пользователей, не имеющих выделенных сотрудников для управления МЭ, требуется надежное и недорогое решение, реализующее технологии шлюза безопасности, балансировку трафика, поддержку резервирования провайдера и автоматическую кластеризацию. Для компаний или филиалов среднего масштаба, имеющих более полусотни пользователей и несколько МЭ, необходимы решения другого класса, предоставляющие возможности удобного, оперативного и централизованного управления всеми шлюзами безопасности периметра. Также желательно, чтобы в состав защищаемой сети включались VPN-клиенты мобильных пользователей. Предлагаемые таким компаниям решения должны быть отказоустойчивыми и поддерживать возможность балансировки нагрузки по требованиям к качеству обслуживания. Это решение необходимо и в случае, если компания использует антивирусы разных производителей (например, по рекомендации стандарта ЦБ РФ).

Крупным компаниям нужны решения, обеспечивающие максимальную гибкость и производительность, централизованное управление всеми подсистемами ИБ.

Кроме того, существуют специализированные решения для крупных компаний, имеющих потребность в применении и централизованном администрировании нескольких десятков шлюзов безопасности. Виртуальный шлюз безопасности представляет собой распределенную структуру, которую можно масштабировать и наращивать, обеспечивая требуемую производительность и гибкость.

Необходимо упомянуть еще один класс продуктов – средства обнаружения/предотвращения вторжений (IDS/IPS). Эти инструменты считаются обязательной составляющей любой системы ИБ и получили в последнее время широкое распространение. Лучшие решения этого класса позволяют проводить глубокий анализ активности на всех сетевых уровнях, обновлять в реальном времени базы признаков вторжений, оперативно оповещать администраторов о новых видах вторжений. Кроме того, предоставляются руководства, шаблоны конфигураций и инструменты противодействия вторжениям [25].

Подсистема защиты Web-ресурсов

Сегодня большинство компаний, так или иначе, используют Интернет, и с этим связаны проблемы защиты удаленных и мобильных пользователей информационных систем компании, защиты корпоративных Web-ресурсов (Интернет-сайта и любого приложения компании, работающего по http-протоколу). Интернет – это зона повышенного риска. Соответственно требуются и специ-

альные средства защиты при работе удаленных пользователей с Web-приложениями по SSL-протоколу.

Таким образом, подсистема защиты Web-ресурсов решает следующие задачи:

- обеспечение «диной точки входа» к приложениям;
- интегрированный контроль доступа к корпоративным Web-ресурсам;
- защиту клиентских браузеров;
- защиту Web-ресурсов.

Внутренняя безопасность

Средства обеспечения безопасности внутренних ресурсов сегодня востребованы многими компаниями. Статистика свидетельствует, что около 80% всех инцидентов ИБ возникают по вине или при содействии сотрудников компании. Чтобы снять нагрузку с МЭ и разделить системы защиты периметра и внутренних ресурсов (это также позволяет избежать создания единственной «точки компрометации»), а также снизить стоимость системы защиты, можно использовать решения по защите внутренних ресурсов.

Внутри сети есть множество приложений и сервисов, зачастую написанных собственными силами, в разное время, слабо документированных. Как правило, при их создании разработчики не уделяли должного внимания средствам безопасности, предполагая, что с этими приложениями будут работать только «свои» сотрудники, которым можно доверять.

К сожалению, системные администраторы и администраторы безопасности обычно не имеют исчерпывающих сведений о том, какие приложения функционируют в сети, как они взаимодействуют, кто и как пользуется этими ресурсами. Казалось бы, достаточно просто выделить серверы в отдельный сегмент сети, применить какой-нибудь межсетевой экран и определить права доступа пользователей. Однако на практике создать четкие правила, разрешающие и запрещающие доступ внутри сети, почти невозможно. Обязательно кто-нибудь из пользователей что-то забудет, и реализованная политика разграничения доступа заблокирует что-то лишнее и нарушит предоставление каких-то ИТ-сервисов. А в большинстве организаций предъявляются повышенные требования к постоянной работоспособности систем. В результате непрерывность ИТ-процессов становится первоочередной задачей, гораздо более приоритетной, чем безопасность. И это различие подходов к обеспечению безопасности периметра и внутренних ресурсов приводит к тому, что для периметра используется политика по умолчанию – «запрещено все, что не разрешено», в то время как внутри сети принят диаметрально противоположный подход – «разрешено все, что не запрещено».

Подсистема защиты внутренних ресурсов обеспечивает решение следующих задач:

- сегментацию сети;
- превентивные меры защиты;
- защиту рабочих станций;
- защиту серверов;
- защиту данных.

Внутренние шлюзы безопасности должны блокировать распространение сетевых червей, внутренние атаки, проводить сегментацию сети по уровням доверия, иметь развитые средства мониторинга и отчетности о сетевой активности. На рынке пока немного таких решений, хотя потребность в них очень высока.

Еще один аспект обеспечения внутренней безопасности связан с необходимостью у некоторых компаний предоставлять мобильным пользователям доступ к внутренним ИТ-ресурсам. Основная задача системы ИБ в этом случае – обеспечить безопасность рабочего места пользователя и безопасное его соединение с информационной системой компании. При этом мобильный пользователь находится в зоне с пониженным уровнем доверия.

Аутентификация и авторизация

Чтобы получить доступ к информационным ресурсам, пользователю необходимо пройти процедуру аутентификации и авторизации. На сегодняшний день парольная защита не выдерживает никакой критики. Сложные пароли тяжело запомнить, а слабые легко подобрать. Пароли, как и идентификационные данные, являются мишенью «фишинга». Поэтому для снижения рисков, связанных с аутентификацией, в системе ИБ предлагается использовать средства как минимум двухфакторной аутентификации.

В нашей архитектуре системы ИБ мы предлагаем средства строгой аутентификации с использованием автономных токенов. Эти устройства позволяют генерировать динамически изменяемый пароль, то есть они формируют одноразовый пароль, валидный в течение нескольких секунд. Даже будучи перехваченным, пароль не может быть повторно использован.

Таким образом, ключевое преимущество таких устройств в том, что их работу тяжело подделать. Автономные токены эффективны с точки зрения обеспечиваемого уровня защищенности систем и совокупной стоимости владения: они компактны, просты и надежны в эксплуатации.

Специфика работы пользователей и особенности моделей безопасности различных приложений и прикладных систем требует многочисленных аутентификаций и использования множества идентификаторов и аутентификационных признаков для одного пользователя. Возникающие при этом накладные

расходы и затраты времени снижают решения единого входа («одного окна»): однажды пройдя авторизацию ко всем доступным ему ресурсам, пользователь не нуждается в повторных сеансах входа или подтверждения своих прав.

Вредоносный код

Необходимость защиты от вредоносного кода, проще говоря, антивирусной защиты, сегодня очевидна. Любая информационная система содержит те или иные антивирусные средства (антивирусы). Сравнивать или оценивать эффективность работы решений разных производителей предоставим авторитетным организациям и техническим экспертам. Хотя некоторые вещи учитывать необходимо: эффективность антивируса не определяется максимальным числом вирусных сигнатур в базах, и ни один антивирус не может гарантировать уничтожение 100 % вирусов.

Применение антивирусных средств в малых компаниях, как правило, не создает проблем владельцам или руководству. Использование антивирусных решений в средних и крупных компаниях имеет некоторые особенности, которые могут обернуться серьезными проблемами, если их не принять во внимание.

Во-первых, комплексная антивирусная безопасность невозможна, если не защищена каждая точка сети: шлюзы, рабочие станции и серверы. Сегодня антивирусная защита требуется любым мобильным устройствам, подключаемым в корпоративную ИС.

Во-вторых, антивирусные системы должны, по возможности, защищать ИС от всех видов вредоносного кода, а не только от «вирусов» и «троянов». Если система антивирусной безопасности построена из разных продуктов, то их совместное использование должно быть оправданным, учитывая, что многие решения «не уживаются» вместе, а решения сторонних производителей поддерживаются далеко не всеми поставщиками. В результате интеграция этих средств защиты в единый комплекс часто недостижима.

В-третьих, управление такой системой, обновление сотен и тысяч рабочих станций должно осуществляться централизованно и максимально просто. Решения уровня корпорации позволяют существенно снижать совокупную стоимость владения такой системой. Немногие решения удовлетворяют все требования к корпоративной антивирусной системе.

Контроль и фильтрация трафика

Даже при наличии в составе системы ИБ средств безопасности периметра, Web-ресурсов, средств внутренней безопасности, строгой аутентификации, антивирусной защиты, у компаний остаются нерешенными многие проблемы. Как контролировать доступ из информационной системы компании к внешним Web-ресурсам? Как обеспечивать конфиденциальность информации при массовом использовании электронной почты, систем обмена мгновенными сообще-

ниями? Как избежать нецелевого использования канальных и вычислительных ресурсов ИС, снижения производительности труда сотрудников из-за использования рабочего времени в личных целях? Эти проблемы напрямую влияют на ИБ компании.

По отчетам различных аналитических агентств, до 40 % сотрудников компаний постоянно используют ресурсы Интернет в непроизводственных целях. Сюда же можно добавить неконтролируемое использование сотрудниками непроизводственного ПО, в том числе развлекательного характера. На первый взгляд, это не имеет отношения к безопасности компании.

Но кроме существенного роста информационных и финансовых рисков, существуют реальные угрозы безопасности компании: проникновение злонамеренного ПО, мобильного вредоносного кода (ММС) в ИС из Интернета, фишинг-атаки, дискредитирующие компанию и наносящие вред клиентам. Важна и угроза утечки конфиденциальной информации при использовании Интернета и средств мгновенного обмена сообщениями (IM), применение которых сопровождается бесконтрольной передачей информации практически любого типа за периметр ИС компании. Здесь необходимы решения, которые обеспечивают возможности мониторинга и фильтрации Интернет-трафика и доступа к приложениям, сочетающиеся с высокоэффективными средствами управления и формирования отчетности.

Управление компонентами системы ИБ

Эффективность системы ИБ и труда администраторов средств информационной безопасности будет чрезвычайно низкой при отсутствии средств сбора, анализа, хранения информации о состоянии системы ИБ, централизованного управления всеми ее составляющими. Дело в том, что каждое средство защиты реализует некоторую составляющую политики безопасности, которая на уровне подсистем задается набором параметров и требований. Политике ИБ должны соответствовать не только каждая подсистема или средство защиты, но и система ИБ в целом. Отслеживание работоспособности компонентов системы, примененных правил и других событий в системе ИБ требует наличия средств мониторинга и управления. Для проведения анализа собираемых данных, построения отчетов и принятия управляющих решений необходимы средства мониторинга, аудита и генерации отчетов [25].

Кроме того, отметим, что распределенная атака на ИС в некоторых случаях может быть зафиксирована и предотвращена только при получении данных из многих точек сети, как от средств защиты, так и от серверов, сетевого оборудования, приложений. Зафиксировать такую атаку можно, имея средства консолидации собираемых данных и корреляции регистрируемых событий.

5.4. Этапы работ по проектированию системы ИБ

Разработка концепции системы информационной безопасности

Определяются основные цели, задачи и требования, а также общая стратегия построения системы ИБ. Идентифицируются критичные информационные ресурсы. Вырабатываются требования к системе ИБ и определяются базовые подходы к их реализации.

Концепция информационной безопасности служит методологической основой для:

- формирования и реализации единой политики в области обеспечения информационной безопасности;
- принятия обоснованных управленческих решений по разработки мер защиты информации;
- выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление и ликвидацию последствий реализации различных видов угроз информационной безопасности;
- координации деятельности подразделений при проведении работ по созданию, развитию и эксплуатации информационной системы с соблюдением требований обеспечения безопасности информации.

В концепции системы информационной безопасности для базового предприятия в курсовом проекте необходимо отразить:

- общую характеристику объекта защиты (описание состава, функций и существующей технологии обработки информации);
- формулировку целей создания системы защиты, основных задач обеспечения информационной безопасности и путей достижения целей;
- основные классы угроз информационной безопасности, принимаемые во внимание при разработке подсистемы защиты;
- основные принципы и подходы к построению системы обеспечения информационной безопасности, меры, методы и средства достижения целей защиты.

Создание политики ИБ

Политика описывает общий подход к ИБ в базовой фирме без специфичных деталей.

Политика безопасности должна пройти через отдел кадров и юридический департамент. Первый, проверив непротиворечивость документа с КЗОТ, сможет использовать его при приеме на работу новых сотрудников (и при аттестации уже работающих). Без юристов не обойтись, потому что документ дол-

жен соответствовать всем действующим в стране нормам и законам. В противном случае отдельные положения политики безопасности в конфликтных ситуациях могут быть оспорены в суде.

Необходимо в курсовом проекте описать все основные моменты, связанные с предметом политики безопасности базового предприятия. При этом надо постоянно помнить, что концепция – это не описание способа реализации. В ней нельзя «привязываться» к конкретным техническим решениям, продуктам и производителям. Иначе изменение ситуации в компании, уход с рынка какого-либо из вендоров и т. п. приведет к необходимости изменения концепции ИБ, а этого происходить не должно.

Подготовка технического задания на создание системы информационной безопасности

Основным документом, на основе которого разрабатывается ТЗ ИСБ, является «Концепция информационной безопасности». Рекомендованный порядок разработки, согласования и утверждения ТЗ ИСБ определен в приложении №1 ГОСТ 34.602-2020 [6].

ТЗ ИСБ является обязательным документом для разработки проектно-сметной документации. ТЗ должна составлять организация-заказчик (далее-заказчик). Учитывая, что далеко не каждая организация имеет в своем штате таких специалистов, то для разработки ТЗ может привлекаться на договорной основе специализированная организация, имеющая опыт работ в данной области и соответствующие лицензии (организация-разработчик, далее – разработчик), а также организации, привлекаемые для реализации различных этапов создания ИСБ (организации-исполнители, далее-исполнитель). ТЗ ИСБ утверждается руководством организации-заказчика и организации-разработчика.

При необходимости, ТЗ ИСБ может согласовываться с органами вневедомственной охраны МВД РФ, государственной противопожарной службы МЧС РФ, ведомственной охраны, организациями-исполнителями и другими структурами. Все подписи должностных лиц согласующих и утверждающих организаций оформляются на первой странице ТЗ ИСБ и заверяются печатями данных организаций. Допускается согласование по письму. Все замечания заказчика по проекту ТЗ ИСБ должны быть представлены с техническим обоснованием.

При возникновении разногласий оформляется протокол разногласий и обе стороны принимают меры к их устранению. Дополнения и изменения к ТЗ ИСБ утверждаются и согласовываются таким же порядком. Не допускается внесение изменений и дополнений после представления системы или ее части на приемо-сдаточные испытания.

Состав и содержание текстовой части ТЗ ИСБ

Состав и содержание ТЗ ИСБ изложены в ГОСТ 34.602-2020 [6], а также будет определяться требованиями конкретного объекта, необходимым составом ИСБ, этапностью развертывания ИСБ и другими факторами.

Здесь необходимо дать точное и полное наименование работы по созданию ИСБ, указать название и адрес или местоположение защищаемого объекта, при необходимости может быть присвоен шифр работы.

1. Основание для создания ИСБ

Основанием для создания ИСБ, как правило, являются решение или документ заказчика, где определена необходимость оборудования объекта ИСБ, а также исходные данные: архитектурно-строительные чертежи, генплан объекта и т. п.

2. Цель и состав работы

Целью работы является создание ИСБ объекта, соответствующей определенным техническим, технологическим, производственно-экономическим показателям. Как правило, здесь же указываются критерии, по которым делается оценка достижения целей создания ИСБ. Так же можно отразить требования по стадийности и этапности создания ИСБ.

3. Сроки создания ИСБ

Минимальные сроки создания ИСБ рассчитываются исходя из трудоемкости работ, нормативных сроков согласования и сдачи работ в надзорных органах. Заказчик или исполнитель может определить большие сроки, учитывая другие факторы.

4. Требования по вариантной разработке

На начальном этапе заказчик может привлечь несколько исполнителей для конкурсной организации работ. На этом этапе могут рассматриваться коммерческие предложения. Для проведения конкурса необходимо указать критерии выбора заказчиком варианта построения ИСБ.

5. Исходные данные для проектирования

В работе по проектированию задействуется много различных специалистов. Не все они имеют возможность принять участие в обследовании, особенно если это удаленный объект. От полноты и точности исходных данных во многом будет зависеть качество проектных работ.

- ***Описание объекта***

Описание объекта должно быть выполнено в такой форме и объеме, чтобы было видно на какую материально-техническую базу должна «наложиться» создаваемая ИСБ. В первую очередь это касается инженерных средств защиты (ограждений, заграждений, освещения, связи и т. п.), состояния и организации физической охраны (караулы, посты, маршруты движения и т. п.), а также других факторов, влияющих на построение ИСБ. Необходимо так же дать краткую

характеристику криминогенной и пожарной обстановки в месте расположения объекта, а также соседних объектов, граничащих с защищаемым объектом.

- ***Перечень основных регламентирующих документов***

Здесь необходимо привести полный перечень тех нормативных документов, которыми должны руководствоваться заказчик, разработчик и исполнитель при выполнении работ по созданию ИСБ. Далее в тексте ТЗ нет необходимости повторять нормативные требования, изложенные в этих документах. Достаточно оговаривать, что элемент должен быть создан в соответствии с тем или иным нормативным документом. При этом надо помнить, что в случае расхождения норм в различных документах, приоритетными являются требования ГОСТ, потом СНиП, ВСН, РД, РТМ, НПБ.

- ***Особые условия***

К особым условиям заказчик вправе отнести то, что не нашло отражения в основном тексте. Например, требования к проектной, монтажной, пусконаладочной организации (наличие определенных лицензий, опыта, квалификации специалистов и т. п.), о необходимости согласования проектно-сметной документации в определенных надзорных или взаимодействующих органах, поэтапному развертыванию ИСБ, о частичном использовании некоторых существующих систем безопасности и прочее.

6. Общие требования к ИСБ

В этом разделе объединены требования, единые для всех подсистем и системы в целом.

- ***Требования по назначению, составу и структуре***

Здесь целесообразно дать определение ИСБ, как совокупности различных элементов и систем, работающих под единым управлением, а также для выявления каких событий и действий она предназначена, какую информацию она должна формировать «на выходе». Необходимо указать из каких подсистем должна состоять ИСБ, алгоритм работы ИСБ, глубину интеграции подсистем, набор функций взаимодействия подсистем, интеллектуальные уровни, решающие задачи интеграции и управления компонентами, а также требования по защите самой ИСБ от преднамеренных и непреднамеренных действий по нарушению штатной работы системы. Кроме того, важно указать, какими другими системами (лифты, освещение, вентиляция и пр.) должна управлять или взаимодействовать ИСБ.

- ***Требования по размещению оборудования***

Требования по размещению основного и промежуточного оборудования, кабельным трассам достаточно полно изложены в нормативных документах [30]:

– ГОСТ Р 50776-95 «Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 4. Руководство по проектированию, монтажу и техническому обслуживанию»;

– ГОСТ 8709-82 «Щитки осветительные для промышленных и общественных зданий»;

– РД 78.145-93 «Системы и комплексы охранной, пожарной и охранно-пожарной сигнализации. Правила производства и приемки работ»;

– НПБ 88-2001 «Установки пожаротушения и сигнализации. Нормы и правила проектирования»;

– ВСН 60-89 «Устройства связи, сигнализации и диспетчеризации инженерного оборудования жилых и общественных зданий. Нормы проектирования»;

– ВСН 59-88 «Электрооборудование жилых и общественных зданий. Нормы проектирования»;

– ОСТН-600-93 «Отраслевые строительно-технологические нормы на монтаж сооружений и устройств связи, радиовещания и телевидения»;

– Правила устройства электроустановок (ПУЭ) и других.

Здесь необходимо конкретно указать место расположения центра управления ИСБ, количество, состав и места размещения автоматизированных рабочих мест (АРМ). Если требуется изготовить специальные стойки, стеллажи, тумбы, столы, то необходимо сделать планы, чертежи в виде приложений или просто изложить требования к ним, оставив решение вопроса по дизайну за исполнителем.

- ***Требования по условиям эксплуатации***

Здесь необходимо выдвинуть требования по климатическому исполнению оборудования, защите от электромагнитных помех, агрессивной среды и т. п. Эти требования изложены в соответствующих ГОСТ.

- ***Требования к безопасности***

Эти требования касаются обеспечения электробезопасности, других мер безопасности при монтаже, наладке, эксплуатации, обслуживании и ремонте ИСБ, соответствии ее санитарным нормам и правилам для лиц, эксплуатирующих ИСБ.

- ***Требования к продолжительности непрерывной работы***

Как правило, при нормальном питающем напряжении система должна функционировать круглосуточно. Так же необходимо указать планируемый срок эксплуатации ИСБ, требуемую наработку на отказ основных блоков и оборудования, предполагаемую схему ремонтов и модернизации.

- ***Требования к электропитанию***

Надо дать характеристику имеющейся электрической сети. Необходимо указать места подключения блоков ИСБ к существующей электрической сети. Если на объекте невозможно обеспечить электропитание ИСБ по первой категории, необходимо сформулировать требования по резервным источникам питания. Минимально необходимые требования по резервному электропитанию для различных подсистем ИСБ изложены в нормативных документах. Так же необходимо изложить требования по заземлению или занулению оборудования, грозозащите наружных устройств, устойчивости к перепаду напряжения в электросети, сопротивлению изоляции электропроводок и т. п.

- ***Требования к обслуживанию и ремонту***

Здесь необходимо изложить требования к персоналу, который будет проводить техническое обслуживание и ремонт ИСБ. Это может быть специально обученный персонал заказчика или специализированная организация, привлекаемая на договорной основе. Так же необходимо указать нормативные документы, которыми необходимо будет руководствоваться при проведении технического обслуживания и ремонта.

- ***Требования к возможности расширения и изменения конфигурации ИСБ***

Если заказчик планирует расширение, изменение конфигурации ИСБ, то необходимо точно указать какие подсистемы, в каких размерах, в какие сроки будут этому подвержены. Проектная организация должна заложить соответствующий резерв возможностей ИСБ.

- ***Требования к надежности и устойчивости***

Здесь можно выдвинуть требования по возможности работы подсистем, отдельных блоков, элементов как в сетевом, так и в автономном режиме, к каким видам разрушающих и неразрушающих воздействий она должна быть устойчива, защита программного продукта и другие.

- ***Требования по метрологическому обеспечению***

Необходимо указать какие параметры системы, с какой точностью и периодичностью должны измеряться, какие и где должны быть встроенные средства контроля параметров системы.

7. Требования к подсистемам ИСБ

В этом разделе формулируются специальные требования к каждой подсистеме:

- **Подсистема сбора и обработки информации**

В ИСБ данная подсистема, как правило, представляет собой программно-аппаратный комплекс. Поэтому надо сформулировать требования как к программной, так и к аппаратной части в виде функциональных и технических требований.

❖ **Подсистема охранно-пожарной сигнализации**

Наиболее важным элементом этой подсистемы являются извещатели. Для того чтобы проектная организация могла выбрать оптимальную модель извещателя, очень важно правильно и полно сформулировать признаки событий, которые должны классифицироваться извещателем, как «тревога», «саботаж» и «неисправность», а также возможные преднамеренные и непреднамеренные помехи работе этих извещателей.

Важным требованием будет тактика постановки и снятия с охраны разделов и зон, которую хотел бы реализовать заказчик. Кроме того, необходимо указать конкретные участки периметра, здания, сооружения, помещения, которые подлежат оборудованию охранной сигнализацией, и указать их особенности (например, кассы, комнаты хранения оружия). Если планируется установка кнопок тревожной сигнализации или ловушек, требуется указать их вид и места установки. Необходимо так же сформулировать требования к приемно-контрольным приборам, извещателям, оповещению о тревожном событии (куда и в каком виде должен приходить сигнал).

Противопожарная автоматика может включать несколько различных установок: пожарную сигнализацию, оповещение людей о пожаре, дымоудаление, пожаротушение. В частном случае, учитывая особенности формирования требований по организации и производству работ по этим установкам, можно разработать ЧТЗ или задание на проектирование противопожарной автоматики. Нормы оборудования помещений, зданий и сооружений противопожарной автоматикой, а также требования к ним, достаточно жестко регламентированы, что в свою очередь значительно облегчает задачу формирования требований.

❖ **Подсистема контроля и управления доступом**

Подсистема контроля и управления доступом может быть предназначена для ограничения и санкционированного перемещения людей, транспорта на территории, в зданиях и помещениях. Требования необходимо формулировать с учетом положений ГОСТ Р 51241-98 «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний». Кроме того, надо указать конкретные требования к подсистеме по организации зон доступа, местам оборудования точек прохода и их пропускной способности, видам идентификационных признаков и устройствам идентификации, видам перекрытия проемов прохода, по штатной процедуре допуска персонала, посетителей и другие.

❖ **Подсистема охранная телевизионная**

Здесь необходимо указать какие элементы объекта подлежат оборудованию данной подсистемой (периметр, контрольно-пропускной пункт, входы, коридоры, помещения и т. п.). В качестве приложения должна быть схема размещения телевизионных камер с обозначенными сценами и их границами осве-

щенности. Для каждой сцены должны быть указаны цели. Отдельно должно быть оговорено применение телевизионных камер на поворотных устройствах и использование трансфокаторов. Остальные требования к телевизионным камерам, устройствам обработки, записи и отображения, соединительным линиям, электропитанию можно сформулировать в соответствии с ГОСТ Р 51558-2000 «Системы охранные телевизионные. Общие технические требования и методы испытаний».

8. Приемка работ и гарантийные обязательства

Здесь необходимо указать виды, состав, объем и методы приемосдаточных испытаний ИСБ и ее составных частей на предмет ее соответствия заданным требованиям. Программы испытаний должны разрабатываться и утверждаться непосредственно перед испытаниями. Необходимо сформулировать требования к гарантийным обязательствам производителей оборудования и привлекаемых к работе монтажных, пусконаладочных организаций. Можно сформулировать требования к индивидуальному и групповому комплекту запасных частей, инструменту, принадлежностям (ЗИП).

9. Требования к проектно-сметной, конструкторской, рабочей и эксплуатационно-технической документации

Требования к проектной, конструкторской, рабочей и эксплуатационно-технической документации достаточно полно изложены в действующих нормативных документах. Необходимо указать требуемое количество экземпляров документации, если необходимо – степень ее конфиденциальности, обязанность подрядных организаций не разглашать эти сведения, использование иностранных терминов и другие. При формировании требований к сметной документации необходимо указать метод составления смет, ценники по которым должен производиться сметный расчет, какие коэффициенты и индексы могут быть применены.

Примечание. *В курсовом проекте должны быть отражены не все приведенные выше требования, а только те, выполнение которых необходимо для проектирования СИБ конкретного предприятия.*

6. ОРГАНИЗАЦИЯ ЗАЩИТЫ КУРСОВОГО ПРОЕКТА

Общее руководство и контроль за ходом выполнения курсового проекта осуществляет руководитель курсового проекта из числа преподавательского состава кафедры информационной безопасности.

На время выполнения курсового проекта составляется расписание консультаций. Консультации проводятся за счет объема времени, отведенного в

рабочем учебном плане на консультации. В ходе консультаций руководителем работы разъясняются назначение и задачи, структура и объем, принципы разработки и оформления, примерное распределение времени на выполнение отдельных частей курсового проекта, даются ответы на вопросы студентов [35].

Выполненный курсовой проект сдается студентом руководителю в установленный срок, который дает письменный отзыв. В отзыве должны содержаться характеристика проделанной работы по всем разделам, положительные стороны и недостатки, степень самостоятельности автора в работе над исследованием, сформированность навыков работы с научной литературой, теоретического и экспериментального исследования, обоснованность и ценность полученных результатов и выводов, возможность их практического применения и заключение о допуске к защите. Курсовые проекты, получившие положительный отзыв, допускаются к защите.

Курсовой проект допускается к защите при следующих условиях:

- итоговая оценка оригинальности текста курсового проекта не ниже 50 % для проектов;
- печатный вариант соответствует требованиям по оформлению;
- курсовой проект выполнен в соответствии с рекомендациями данного пособия и его содержательная часть, в том числе результаты работы, соответствует заявленной теме.

Работа, не соответствующая предъявляемым требованиям, возвращается студенту на доработку.

Дата защиты курсового проекта определяется преподавателем в соответствии с учебным графиком дисциплины. Защита курсового проекта проводится до начала экзаменационной сессии.

Защита состоит из доклада студента по теме курсового проекта в течение 5–7 минут и ответов на вопросы преподавателя (преподавателей). Обучающийся должен: логично построить сообщение о выполненном проекте, обосновать выводы и предложения; показать понимание теоретических положений, на основе которых выполнен проект; показать самостоятельность выполнения проекта; дать правильные ответы на вопросы. Доклад должен быть лаконичен и полностью раскрывать суть проделанной проекта.

Далее в докладе следует последовательно изложить:

- актуальность темы;
- цель, задачи и основные требования проекта;
- предмет исследования;
- объект исследования;
- методы исследования (желательно);

- используемые в проекте методы, подходы и средства, отметив проделанную проект по основным разделам, последовательно на всех ее этапах и полученные при этом результаты;
- описание и анализ экспериментов и их результатов;
- выводы по курсовому проекту в целом.

По итогам защиты выставляется оценка за курсовой проект.

Решение об оценке курсового проекта принимается по результатам анализа предъявленной курсового проекта, доклада, обучающегося на защите и его ответов на вопросы. В случае выполнения группой курсового проекта обязательно присутствие всех обучающихся, участвовавших в ее подготовке, на ее защите.

При этом оценка курсового проекта осуществляется по результатам доклада и ответов на вопросы каждого из участвовавших в написании курсового проекта обучающихся с учетом предварительной оценки, содержащейся в отзыве научного руководителя. В отзыве научного руководителя должен оцениваться вклад каждого из обучающихся в выполнение курсового проекта.

Курсовой проект оценивается дифференцированной отметкой: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно»:

- оценка **«отлично»** получают проекты, в которых содержатся элементы научного исследования, приводятся и обуславливаются математические модели и формальные доказательства, делаются самостоятельные выводы, дается аргументированная критика и самостоятельный анализ фактического материала на основе глубоких знаний литературы по данной теме, в процессе выполнения проекта приобретены навыки самостоятельного проектирования и выполнения научно-исследовательской проекта; получен опыт сбора и обработки исходного материала, анализа научно-технической литературы, материал излагается грамотно, оформление проекта соответствует правилам (указаны в пособии). Результат работы представлен и апробирован экспериментальным способом.
- оценка **«хорошо»** ставится тогда, когда в проекте, выполненном на достаточном теоретическом уровне, полно и всесторонне освещаются вопросы темы, но нет должной степени творчества, углублены теоретические и практические знания, материал излагается грамотно и по существу, не допущены существенные неточности в ответе на вопрос, оформление проекта соответствует правилам. Результат работы представлен и апробирован экспериментальным способом.
- оценка **«удовлетворительно»** имеют проекты, в которых правильно освещены основные вопросы темы, но не проявилось умение логически стройного их изложения, самостоятельного анализа источников, содержатся отдель-

ные ошибочные положения, проект носит реферативный характер, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении при защите, оформление проекта имеет незначительные отклонения от правил.

– оценку **«неудовлетворительно»** получают студенты в случае, когда в процессе защиты не могут ответить на вопросы и замечания, не владеют материалом проекта, не в состоянии дать объяснения выводам и теоретическим положениям данной проблемы. Курсовой проект носит реферативный характер, студент допускает существенные ошибки при защите, с большими затруднениями отвечает на вопросы, оформление проекта не соответствует правилам.

Критерии оценки курсового проекта:

- степень усвоения студентом понятий и категорий по теме исследования;
- умение работать с документальными и литературными источниками;
- четкость в определении основного содержания курсового проекта, убедительность доказательств, обоснований, выводов и рекомендаций по результатам анализа конкретного материала;
- грамотность и стиль изложения;
- самостоятельность работы, оригинальность в осмыслении материала;
- правильность и аккуратность оформления;
- соответствие оформления курсового проекта установленным требованиям.

Положительные оценки по курсовому проекту заносятся в ведомость и зачетную книжку, неудовлетворительные оценки проставляются только в ведомость.

Обучающийся, не предъявивший в установленный срок курсовую проект при соблюдении всех требований, предъявляемых к оформлению и содержанию курсового проекта, или не защитивший его по неуважительной причине, считается имеющим академическую задолженность.

Курсовые проекты после их защиты должны сдаваться на кафедры в распечатанном бумажном виде и в электронном (файл, расширение *.docx, *.odt).

Электронный вариант защищённой студентом курсового проекта размещается в формате PDF в электронной информационной образовательной среде Университета (по необходимости, в разделе электронное портфолио).

При рейтинговой системе курсовой проект оценивается дифференцированно по 100-балльной системе в соответствии с Положением о рейтинговой системе оценки успеваемости и качества знаний обучающихся.

ЛИТЕРАТУРА

1. Федеральный закон РФ «Об информации, информатизации и защите информации». Собрание законодательства Российской Федерации. 20 февраля 1995 г. Официальное издание. – Москва: Юридическая литература.

2. ФСТЭК РФ. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. [Электронный ресурс]. – URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-25-iyulya-1997-g.

3. ГОСТ Р 51583-2014. Порядок создания автоматизированных систем в защищенном исполнении [Электронный ресурс]. – URL: http://docs.cntd.ru/ document/ 1200108858.

4. ГОСТ Р 51624 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования» [Электронный ресурс]. – URL: http://docs.cntd.ru/ document/ 1200108858.

5. ГОСТ 34.601-90. Автоматизированные системы. Стадии создания [Электронный ресурс]. – URL: http://www.insapov.ru/gost-34-601-90.html.

6. ГОСТ 34.602-2020. Информационные технологии. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы [Электронный ресурс]. – URL: https://www.edsd.ru/files/pdf/GOST-34.602-2020.

7. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Методы и средства обеспечения безопасности. Практические правила управления информационной безопасностью. – Москва: Стандартинформ, 2006.

8. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – Москва: Стандартинформ, 2008.

9. ГОСТ Р 53113.1-2008. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Ч. 1. Общие положения. – Москва: Стандартинформ, 2009.

10. ФСТЭК РФ. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. – Москва: Воениздат, 1992.

11. ФСТЭК РФ. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционирован-

ного доступа к информации [Электронный ресурс]. – URL: http://fstec.ru/component/ attachments/ download/299.

12. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. – Москва: Военное издательство, 1992.

13. Гостехкомиссия России. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. – Москва: Военное издательство, 1992.

14. Гостехкомиссия России. Руководящий документ. Средства защиты информации. Специальные общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам. – Москва: Военное издательство, 2000.

15. ГОСТ 7.32-2001. Межгосударственный стандарт. Система стандартов по информации, библиотечному и издательскому делу. Отчет о научно-исследовательской работе. Структура и правила оформления (введен Постановлением Госстандарта России от 04.09.2001 N 367-ст) (ред. от 07.09.2005) Введен. Постановлением Госстандарта России от 4 сентября 2001 г. N 367-ст. Дата введения – 1 июля 2002 года.

16. ГОСТ Р 7.0.5-2008 «Библиографическая ссылка. Общие требования и правила составления».

17. ГОСТ Р 1.5-2004 Стандартизация в Российской Федерации. Стандарты национальные Российской Федерации. Правила построения, изложения, оформления и обозначения.

18. ГОСТ 7.1-2003 Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Библиографическое описание. Общие требования и правила составления.

19. ГОСТ 8.417-2002 Государственная система обеспечения единства измерений. Единицы величин.

20. ГОСТ 7.32-2001 Система стандартов по информации, библиотечному и издательскому делу. Отчет о научно-исследовательской работе. Структура и правила оформления.

21. ГОСТ 7.82-2001 Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Библиографическое описание электронных ресурсов. Общие требования и правила составления.

22. ГОСТ 7.80-2000 «Библиографическая запись. Заголовок. Общие требования и правила составления».

23. ГОСТ 7.9-95 Система стандартов по информации, библиотечному и издательскому делу. Реферат и аннотация.

24. ГОСТ 2.105-95. Общие требования к текстовым документам.

25. Солодянников, А. В. С60 Информационная безопасность автоматизированных систем / А. В. Солодянников. – Санкт-Петербург: Изд-во СПбГЭУ, 2020. – 108 с.

26. Библиографическое описание в примерах: ГОСТ Р 7.0.100–2018 «Библиографическая запись. Библиографическое описание. Общие требования и правила составления»: методические рекомендации / ГБУК «СКУНБ им. Лермонтова»; сост.: Л. А. Бедарева, В. В.Фурманова. – Ставрополь, 2020. – 20 с.

27. Васильков, А. В. Безопасность и управление доступом в информационных системах / А. В. Васильков, И. А. Васильков. – Москва: ФОРУМ: ИНФРА-М, 2013. – 368 с.

28. Мельников, В. П. Информационная безопасность и защита информации: учеб. пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков. – 6-е изд. – Москва: Академия, 2012.

29. Астахова, А. В. Информационные системы в экономике и защита информации на предприятиях — участниках ВЭД: учеб. пособие / А. В. Астахова. – Санкт-Петербург: Троицкий мост, 2014.

30. Синилов, В. Г. Системы охранной, пожарной и охранно-пожарной сигнализации: учебник для нач. проф. образования / В. Г. Синилов. 6-е изд. – Москва; Издательский центр «Академия», 2011. – 512 с.

31. Чеботарева, А. А. Информационное право: учеб. пособие / А. А. Чеботарева. – Москва: Юридический институт МИИТа, 2014.

32. Груздева, Л. М. Информационные технологии в профессиональной деятельности: метод. указания по выполнению практических работ / Л. М. Груздева, С. Л. Лобачев, А. А. Чеботарева. – Москва: Юридический институт МИИТа, 2015.

33. Шаньгин, В. Ф. Информационная безопасность и защита информации [Электронный ресурс] / В. Ф. Шаньгин. – Электрон. текстовые данные. – Саратов: Профобразование, 2017. – 702 с. – Режим доступа: http://www.iprbookshop.ru/63594.html. – ЭБС «IPRbooks».

34. Шаньгин. В. Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / В. Ф. Шаньгин. – Электрон. текстовые данные. – Саратов: Профобразование, 2017. – 544 с. – Режим доступа: http://www.iprbookshop.ru/63592.html. – ЭБС «IPRbooks».

35. Жестовский, А. Г. Методические указания по выполнению курсовой работы «Программно-аппаратные средства обеспечения информационной безопасности». – Калининград. 2019. – 32 с.

ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ»

1. http://www.inside-zi.ru – сайт журнала «Защита информации».
2. http://www.inside-zi.ru – сайт журнала «Инсайд».
3. http://garant.ru – Гарант: законодательство РФ.
4. http://www.consultant.ru – Консультант +: законодательство РФ.
5. http://fstec.ru/ – официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России).
6. http://wm-help.net/books-online/book/98618/98618-7.html – принципы защиты операционных систем.
7. http://rudocs.exdat.com/docs/index-56877.html – принципы построения операционных систем.
8. http://emanual.ru/download/6661.html – средства безопасности для защиты сервисов.
9. http://www.ab-solutions.ru/articles/information_security/ – методы обеспечения информационной безопасности предприятия.
10. http://asher.ru/security/book/its/08 – приемы обеспечения безопасности информационных систем.
11. http://www.garlic.com/~lynn/secure.htm – глоссарий по информационной безопасности.
12. http://blacksun.box.sk/tutorials.html – статьи по различным аспектам сетевой безопасности и работы сетевых сервисов.

ПРИЛОЖЕНИЯ

ПРИЛОЖЕНИЕ А

ПРИМЕРНЫЕ ТЕМЫ КУРСОВЫХ ПРОЕКТОВ

1. Разработка и эксплуатация автоматизированных систем в защищенном исполнении в медицинской организации города.
2. Разработка и эксплуатация автоматизированных систем в защищенном исполнении автопредприятия города.
3. Разработка и эксплуатация автоматизированных систем в защищенном исполнении в проектной организации.
4. Разработка и эксплуатация автоматизированных систем в защищенном исполнении в строительной организации.
5. Разработка и эксплуатация автоматизированных систем в защищенном исполнении в торговой организации.
6. Разработка и эксплуатация автоматизированных систем в защищенном исполнении в спортивных организациях города.
7. Разработка и эксплуатация автоматизированных систем в защищенном исполнении библиотечного фонда города.
8. Разработка и эксплуатация автоматизированных систем в защищенном исполнении в организации гостиничного комплекса.
9. Разработка и эксплуатация автоматизированных систем в защищенном исполнении в организации социального обеспечения и помощи.

ПРИЛОЖЕНИЕ Б

Предметная область при разработке автоматизированных систем в различных организациях

Автоматизированная система медицинских организаций города

Каждая больница города состоит из одного или нескольких корпусов, в каждом из которых размещается одно или несколько отделений, специализирующихся на лечении определенной группы болезней; каждое отделение имеет некоторое количество палат на определенное число коек. Поликлиники могут административно быть прикрепленными к больницам, а могут и не быть. Как больницы, так и поликлиники обслуживаются врачебным (хирурги, терапевты, невропатологи, окулисты, стоматологи, рентгенологи, гинекологи и пр.) и обслуживающим персоналом (мед. сестры, санитары, уборщицы и пр.).

Каждая категория врачебного персонала обладает характеристиками, присущими только специалистам этого профиля и по-разному участвует в связях: хирурги, стоматологии гинекологи могут проводить операции, они же имеют такие характеристики, как число проведенных операций, число операций с летальным исходом; рентгенологи и стоматологи имеют коэффициент к зарплате за вредные условия труда, у рентгенологов и невропатологов более длительный отпуск. Врачи любого профиля могут иметь степень кандидата или доктора медицинских наук. Степень доктора медицинских наук дает право на присвоение звания профессора, а степень кандидата медицинских наук на присвоение звания доцента. Разрешено совместительство, так что каждый врач может работать либо в больнице, либо в поликлинике, либо и в одной больнице, и в одной поликлинике. Врачи со званием доцента или профессора могут консультировать в нескольких больницах или поликлиниках.

Лаборатории, выполняющие те или иные медицинские анализы, могут обслуживать различные больницы и поликлиники, при условии наличия договора на обслуживание с соответствующим лечебным заведением. При этом каждая лаборатория имеет один или несколько профилей: биохимические, физиологические, химические исследования.

Пациенты амбулаторно лечатся в одной из поликлиник, и по направлению из них могут стационарно лечиться либо в больнице, к которой относится поликлиника, либо в любой другой, если специализация больницы, к которой приписана поликлиника не позволяет провести требуемое лечение. Как в больнице, так и в поликлинике ведется персонифицированный учет пациентов, полная история их болезней, все назначения, операции и т. д. В больнице пациент имеет в каждый данный момент одного лечащего врача, в поликлинике – несколько.

Автоматизированная система автопредприятия города

Автопредприятие города занимается организацией пассажирских и грузовых перевозок внутри города. В ведении предприятия находится автотранспорт различного назначения: автобусы, такси, маршрутные такси, прочий легковой транспорт, грузовой транспорт, транспорт вспомогательного характера, представленный различными марками. Каждая из перечисленных категорий транспорта имеет характеристики, свойственные только этой категории: например, к характеристикам только грузового транспорта относится грузоподъемность, пассажирский транспорт характеризуется вместимостью и т. д. С течением времени, с одной стороны, транспорт стареет и списывается (возможно, продается), а с другой, – предприятие пополняется новым автотранспортом.

Предприятие имеет штат водителей, закрепленных за автомобилями (за одним автомобилем может быть закреплено более одного водителя). Обслуживающий персонал (техники, сварщики, слесари, сборщики и др.) занимается техническим обслуживанием автомобильной техники, при этом различные вышеперечисленные категории также могут иметь уникальные для данной категории атрибуты. Обслуживающий персонал и водители объединяются в бригады, которыми руководят бригадиры, далее следуют мастера, затем начальники участков и цехов. Введении предприятия находятся объекты гаражного хозяйства (цеха, гаражи, боксы и пр.), где содержится и ремонтируется автомобильная техника.

Пассажирский автотранспорт (автобусы, маршрутные такси) перевозит пассажиров по определенным маршрутам, за каждым из них закреплены отдельные единицы автотранспорта. Ведется учет числа перевозимых пассажиров, на основании чего производится перераспределением транспорта с одного маршрута на другой. Учитывается также пробег, число ремонтов и затраты на ремонт по всему автотранспорту, объем грузоперевозок для грузового транспорта, интенсивность использования транспорта вспомогательного назначения. Учитывается интенсивность работы бригад по ремонту (число ремонтов, объем выполненных работ), число замененных и отремонтированных узлов и агрегатов (двигателей, КП, мосты, шасси и т. д.) по каждой автомашине, и суммарно по участку, цеху, предприятию.

Автоматизированная система проектной организации

Проектная организация представлена следующими категориями сотрудников: конструкторы, инженеры, техники, лаборанты, прочий обслуживающий персонал, каждая из которых может иметь свойственные только ей атрибуты. Например, конструктор характеризуется числом авторских свидетельств, техники – оборудованием, которое они могут обслуживать, инженер или конструктор может руководить договором или проектом и т. д. Сотрудники разделены

на отделы, руководимые начальником так, что каждый сотрудник числится только в одном отделе.

В рамках заключаемых проектной организацией договоров с заказчиками выполняются различного рода проекты, причем по одному договору может выполняться более одного проекта, и один проект может выполняться для нескольких договоров. Суммарная стоимость договора определяется стоимостью всех проектных работ, выполняемых для этого договора. Каждый договор и проект имеет руководителя и группу сотрудников, выполняющих этот договор или проект, причем это могут быть сотрудники не только одного отдела. Проекты выполняются с использованием различного оборудования, часть которого приписано отдельным отделам, а часть является коллективной собственностью проектной организации, при этом в процессе работы оборудование может передаваться из отдела в отдел. Для выполнения проекта оборудование придается группе, работающей над проектом, если это оборудование не используется в другом проекте.

Для выполнения ряда проектов подрядная организация может привлекать субподрядные организации, передавая им объемы работ.

Ведется учет кадров, учет выполнения договоров и проектов, стоимостной учет всех выполненных работ.

Автоматизированная система строительной организации

Строительная организация занимается строительством различного рода объектов: жилых домов, больниц, школ, мостов, дорог и т. д. по договорам с заказчиками (городская администрация, ведомства, частные фирмы и т. д.). Каждая из перечисленных категорий объектов имеет характеристики, свойственные только этой или нескольким категориям: например, к характеристикам жилых домов относится этажность, тип строительного материала, число квартир, для мостов уникальными характеристиками являются тип пролетного строения, ширина, количество полос для движения.

Структурно строительная организация состоит из строительных управлений, каждое строительное управление ведет работы на одном или нескольких участках, возглавляемых начальниками участков, которым подчиняется группа прорабов, мастеров и техников. Каждой категории инженерно-технического персонала (инженеры, технологи, техники) и рабочих (каменщики, бетонщики, отделочники, сварщики, электрики, шофера, слесари, и пр.) также свойственны характерные только для этой группы атрибуты. Рабочие объединяется в бригады, которыми руководят бригадиры. Бригадиры выбираются из числа рабочих, мастера, прорабы, начальники участков и управлений назначаются из числа инженерно-технического персонала.

На каждом участке возводится один или несколько объектов, на каждом объекте работу ведут одна или несколько бригад. Закончив работу, бригада пе-

реходит к другому объекту на этом или другом участке. Строительному управлению придается строительная техника (подъемные краны, экскаваторы, бульдозеры и т. д.), которая распределяется по объектам.

Технология строительства того или иного объекта предполагает выполнение определенного набора видов работ, необходимых для сооружения данного типа объекта. Например, для жилого дома – это возведение фундамента, кирпичные работы, прокладка водоснабжения и т. д. Каждый вид работ на объекте выполняется одной бригадой. Для организации работ на объекте составляется графики работ, указывающие в каком порядке и в какие сроки, выполняются те или иные работы, а также смета, определяющая какие строительные материалы и в каких количествах необходимы для сооружения объекта. По результатам выполнения работ составляется отчет с указанием сроков выполнения работ и фактических расходов материалов.

Автоматизированная система торговой организации

Торговая организация ведет торговлю в торговых точках разных типов: универмаги, магазины, киоски, лотки и т. д.), в штате которых работают продавцы. Универмаги разделены на отдельные секции, руководимые управляющими секций и расположенные, возможно, на разных этажах здания. Как универмаги, так и магазины могут иметь несколько залов, в которых работает определенное число продавцов, универмаги, магазины, киоски могут иметь такие характеристики, как размер торговой точки, платежи за аренду, коммунальные услуги, количество прилавков и т. д. Кроме того, в универмагах и магазинах учет проданных товаров ведется персонифицировано с фиксацией имен и характеристик покупателя, чего в киосках и на лотках сделать не представляется возможным.

Заказы поставщику составляются на основе заявок, поступающих из торговых точек. На основе заявок менеджеры торговой организации выбирают поставщика, формируют заказы, в которых перечисляются наименования товаров и количество, которое может отличаться от запроса из торговой точки. Если указанное наименование товара ранее не поставлялось, оно пополняет справочник номенклатуры товаров. На основе маркетинговых работ постоянно изучается рынок поставщиков, в результате чего могут появляться новые поставщики и исчезать старые. При этом одни и те же товары торговая организация может получать от разных поставщиков и, естественно, по различным ценам.

Поступившие товары распределяются по торговым точкам и в любой момент можно получить такое распределение.

Продавцы торговых точек ведут продажу товаров, учитывая все сделанные продажи, фиксируя номенклатуру и количество проданного товара, а продавцы универмагов и магазинов дополнительно фиксируют имена и характеристики покупателей, что позволяет вести учет покупателей и сделанных ими по-

купок. В процессе торговли торговые точки вправе менять цены на товары в зависимости от спроса и предложения товаров, а также по согласованию передавать товары в другую торговую точку.

На основании анализа описания предметной области и запросов к будущей информационной системе сформулировать основные требования к ее функциям.

Выполнить поиск прототипа проектируемой информационной системы с применением Интернет.

Используя сформулированные требования к информационной системе, а также документацию пользователя на прототип найденного программного средства, разработать техническое задание на проектирование информационной системы в соответствии с ГОСТ 19.20178.

Автоматизированная система спортивных организаций города

Спортивная инфраструктура города представлена спортивными сооружениями различного типа: спортивные залы, манежи, стадионы, корты и т. д. Каждая из категорий спортивных сооружений обладает атрибутами, специфичными только для нее: стадион характеризуется вместимостью, корт – типом покрытия.

Спортсмены под руководством тренеров занимаются отдельными видами спорта, при этом один и тот же спортсмен может заниматься несколькими видами спорта, и в рамках одного и того же вида спорта может тренироваться у нескольких тренеров. Все спортсмены объединяются в спортивные клубы, при этом каждый из них может выступать только за один клуб.

Организаторы соревнований проводят состязания по отдельным видам спорта на спортивных сооружениях города. По результатам участия спортсменов в соревнованиях производится награждение.

Автоматизированная система библиотечного фонда города

Библиотечный фонд города составляют библиотеки, расположенные на территории города. Каждая библиотека включает в себя абонементы и читальные залы. Пользователями библиотек являются различные категории читателей: студенты, научные работники, преподаватели, школьники, рабочие, пенсионеры и другие жители города. Каждая категория читателей может обладать непересекающимися характеристиками-атрибутами: для студентов это название учебного заведения, факультет, курс, номер группы, для научного работника - название организации, научная тема и т. д. Каждый читатель, будучи зарегистрированным в одной из библиотек, имеет доступ ко всему библиотечному фонду города.

Библиотечный фонд (книги, журналы, газеты, сборники статей, сборники стихов, диссертации, рефераты, сборники докладов и тезисов докладов и пр.) размещен в залах хранилищах различных библиотек на определенных местах

хранения (номер зала, стеллажа, полки) и идентифицируется номенклатурными номерами. При этом существуют различные правила относительно тех или иных изданий: какие-то подлежат только чтению в читальных залах библиотек, для тех, что выдаются, может быть установлен различный срок выдачи и т. д. С одной стороны, библиотечный фонд может пополняться, с другой – с течением времени происходит его списание.

Произведения авторов, составляющие библиотечный фонд, также можно разделить на различные категории, характеризующиеся собственным набором атрибутов: учебники, повести, романы, статьи, стихи, диссертации, рефераты, тезисы докладов и т. д.

Сотрудники библиотеки, работающие в различных залах различных библиотек, ведут учет читателей, а также учет размещения и выдачи литературы.

Автоматизированная я система гостиничного комплекса

Гостиничный комплекс состоит из нескольких зданий-гостиниц (корпусов). Каждый корпус имеет ряд характеристик, таких, как класс отеля (двух-, пятизвездочные), количество этажей в здании, общее количество комнат, комнат на этаже, местность номеров (одно-, двух-, трехместные и т. д.), наличие служб быта: ежедневная уборка номера, прачечная, химчистка, питание (рестораны, бары) и развлечения (бассейн, сауна, бильярд и пр.). От типа корпуса и местности номера зависит сумма оплаты за него. Химчистка, стирка, дополнительное питание, все развлечения производятся за отдельную плату.

С крупными организациями (туристические фирмы, организации, занимающиеся проведением международных симпозиумов, конгрессов, семинаров, карнавалов и т. д.) заключаются договора, позволяющие организациям бронировать номера с большими скидками на определенное время вперед не для одного человека, а для группы людей. Каждая из перечисленных групп организаций обладает характеристиками, свойственными только этой группе. Желательно группы людей от одной организации не расселять по разным этажам. В брони указывается класс отеля, этаж, количество комнат и общее количество людей. Броня может быть отменена за неделю до заселения. На основе маркетинговых работ расширяется рынок гостиничных услуг, в результате чего заключаются договора с новыми фирмами. Также исследуется мнение жильцов о ценах и сервисе. Жалобы фиксируются и исследуются. Изучается статистика популярности номеров. Ведется учет долгов постояльца гостинице за все дополнительные услуги.

Новые жильцы пополняют перечень клиентов гостиницы. Ведется учет свободных номеров, дополнительных затрат постояльцев гостиницы и учет расходов и доходов гостиничного комплекса [29].

Автоматизированная система аэропорта

Работников аэропорта можно подразделить на пилотов, диспетчеров, техников, кассиров, работников службы безопасности, сплавочной службы и других, которые административно относятся каждый к своему отделу. Каждая из перечисленных категорий работников имеет уникальные атрибуты-характеристики, определяемые профессиональной направленностью. В отделах существует разбиение работников на бригады. Отделы возглавляются начальниками, которые представляют собой администрацию аэропорта. В функции администрации входит планирование рейсов, составление расписаний, формирование кадрового состава аэропорта. За каждым самолетом закрепляется бригада пилотов, техников и обслуживающего персонала. Пилоты обязаны проходить каждый год медосмотр, не прошедших медосмотр необходимо перевести на другую работу. Самолет должен своевременно осматриваться техниками и при необходимости ремонтироваться. Подготовка к рейсу включает в себя техническую часть (техосмотр, заправка необходимого количества топлива) и обслуживающую часть (уборка салона, запас продуктов питания и т. п.).

В расписании указывается тип самолета, рейс, дни вылета, время вылета и прилета, маршрут (начальный и конечный пункты назначения, пункт пересадки), стоимость билета. Билеты на авиарейсы можно приобрести заранее или забронировать в авиакассах. Цена билета зависит не только от маршрута, но и от времени вылета (в неудобное время – ночь, раннее утро – цена билета ниже). До отправления рейса, если в этом есть необходимость, билет можно вернуть. Авиарейсы могут быть задержаны из-за погодных условий, технических неполадок, а также могут быть отменены, если не продано меньше установленного минимума билетов.

Авиарейсы можно разделить на следующие категории: внутренние, международные, чартерные, грузоперевозки, специальные рейсы. Пассажир при посадке в самолет должен предъявить билет, паспорт, а для международного рейса обязан также предъявить заграничный паспорт и пройти таможенный досмотр. Пассажиры могут сдавать свои вещи в багажное отделение. На рейсы грузоперевозок и специальные рейсы билеты не продаются. Для спец. рейсов не существует расписания. Билеты на чартерные рейсы распространяет то агентство, которое его организовало.

Автоматизированная система ГИБДД

У ГИБДД есть три наиболее важные функциональные задачи: регистрация автотранспортных средств при совершении сделки купли-продажи; разработка мер, повышающих безопасность дорожного движения и выполнение всех мер при совершении ДТП (дорожно-транспортное происшествие) на улицах города (регистрация, разбор, выявление виновных, автоэкспертиза и т. п.); борьба

с угоном автотранспортных средств, оперативный поиск угнанных машин и задержание преступников.

ГИБДД занимается выделением и учетом номерных знаков на автотранспорт. К автотранспортным средствам относятся легковые, грузовые автомобили, прицепы, полуприцепы, мотоциклы, тракторы, автобусы, микроавтобусы. На разные виды транспорта выдаются разные виды номеров и в базу данных заносятся разные характеристики. Номера могут выделяться как частным владельцам, так и организациям. В справочнике номеров, выданных частным владельцам, фиксируется: номер, ФИО владельца, его адрес, марка автомобиля, дата выпуска, объем двигателя, номера двигателя, шасси и кузова, цвет и т. п. В справочнике номеров, выданных организации, дополнительно фиксируется: название организации, район, адрес, руководитель. Существует справочник свободных номеров (серия, диапазон номеров). ГИБДД периодически проводит технический осмотр (ТО) машин. Для прохождения техосмотра необходима квитанция об оплате налогов, сумма оплаты зависит от объема двигателя. Периодичность прохождения зависит от года выпуска и вида транспортного средства. Технические характеристики, проверяемые на ТО и допуски, также зависят от вида транспортного средства.

ГИБДД занимается учетом и анализом ДТП (дорожно-транспортное происшествие). При регистрации ДТП фиксируется: дата, тип происшествия (наезда пешехода, наезд на ограждение либо столб, лобовое столкновение, наезд на впереди стоящий транспорт, боковое столкновение на перекрестке и т. п.), место происшествия, марки пострадавших автомобилей, государственный номер, тип машины (легковая, грузовая, специальная), краткое содержание, число пострадавших, сумма ущерба, причина, дорожные условия и т. п. Анализ накопленной по ДТП статистике поможет правильно расставить запрещающие и предупреждающие знаки на улицах города, а так же спланировать местонахождение постов патрульных.

Угон либо исчезновение виновника ДТП с места происшествия требует оперативного вмешательства всех постов ГИБДД и патрульных машин. Для информирования о разыскиваемой машине ее данные (включая номера двигателя и кузова) извлекаются из базы зарегистрированных номеров и передаются по рации всем постам. Ведение статистики угонов, ее анализ и опубликование результатов в СМИ поможет снизить количество угонов, а хозяевам машин принять необходимые меры (самые угоняемые марки, самый популярный способ вскрытия, самые надежные сигнализации и т. п.).

Автоматизированная система в организации социального обеспечения и помощи

Актуализация проблем социальной защиты населения со всей остротой поставила проблему совершенствования ее правовой базы, отработки инстру-

ментария и новых технологий по ее реализации, подготовки соответствующего кадрового потенциала. Огромную роль в правильности и адекватности принимаемых мер по социальной защите населения имеет своевременная и достоверная информация. В настоящее время существует целый ряд объективных факторов, настоятельно требующих изменения технологии обработки информации по социальной защите населения, удовлетворяющего новым требованиям.

Основные из этих факторов таковы:

– постоянное увеличение объемов обрабатываемой информации и необходимость сокращения сроков ее обработки вследствие частого изменения законодательства по пенсионному обеспечению и социальной защите малоимущих слоев населения, отражающего нестабильность экономической и политической обстановки в стране;

– высокая интенсивность актуализации нормативно – правовой информации, как в части содержания отдельных норм, так и некоторых разделов и даже нормативных актов: объем и сложность нормативно – правовой системы растут быстрее возможностей персонала органов социальной защиты населения изучить правила ее практического применения;

– потребность в налаживании должного учета реальной нуждаемости всех социально незащищенных слоев населения (адресная защита);

– потребность в мощной информационно – аналитической базе, позволяющей осуществлять контроль расходуемых средств, проводить анализ текущего состояния, разрабатывать Программы-минимум и Целевые программы;

– постоянное изменение характера задач, стоящих перед органами социальной защиты населения, оперативное выполнение ими новых сложных функций;

– постоянно возрастающие требования к сотрудникам органов соцзащиты по повышению производительности и качества труда и вытекающая отсюда необходимость сокращения текучести и повышения престижности их профессии;

– интенсивная компьютеризация различных сфер управленческой деятельности, базирующаяся на широком распространении относительно дешевых ПЭВМ с быстро прогрессирующими техническими характеристиками и средств телекоммуникации, позволяющих создавать интегрированные системы, обеспечивающие всем их пользователям оперативный доступ к распределенным базам данных и знаний, оперативную обработку больших массивов информации и выдачу результатов в удобном пользователю виде.

Указанные факторы обусловливают необходимость введения новых информационных технологий в процессы социальной защиты населения.

Информационная система в первую очередь является автоматизированной системой управления, а, чтобы управлять системой социальной защиты

населения как объектом управления необходимо четко представлять его структуру и функции.

Вся система социальной защиты состоит из четырех составных частей:

– субъекты – физические лица, нуждающиеся в социальной защите и помощи;

– объекты – учреждения и организации социальной защиты населения;

– финансы – денежные и материальные потоки;

– законодательство – нормативно-правовое обеспечение.

Каждая из составных частей имеет собственные характеристики и является функциональной подсистемой АИС «Адресная социальная помощь», включающая в себя отдельные достаточно автономно функционирующие фрагменты конкретных социальных процессов.

Функциональная подсистема «субъекты социальной защиты» представляет собой регистр физических лиц, имеющих право на получение социальной помощи или льготы. В свою очередь данный регистр состоит из отдельных категорий, характеризующихся своими признаками: Ветераны Великой Отечественной войны, дети и несовершеннолетние, инвалиды, ликвидаторы ЧАЭС и других аварий, малообеспеченные и т. д. Информационная система мониторинга контингента социально незащищенных групп населения предназначена для создания и ведения картотеки нуждающихся в адресной социальной защите слоев населения.

Только с помощью системы мониторинга социально незащищенных слоев населения можно решить задачу налаживания должного учета реальной нуждаемости всех социально незащищенных слоев населения, создать мощную информационно – аналитическую базу, позволяющую осуществлять контроль расходуемых средств, проводить анализ текущего состояния, разрабатывать Программы-минимум и Целевые программы.

На основе данной системы создаются регистры социально – незащищенного населения, позволяющие наладить полный учет всех видов льгот и выплат конкретному физическому лицу и перейти к системе адресной социальной помощи не на словах, а на деле. На основе данного регистра можно внедрять новые технологии безналичной оплаты льгот и выплат (например, социальная карточка москвича), что позволяет резко повысить производительность всей системы социального обслуживания населения.

Карточка учета содержит следующие сведения: учетные данные для главы семьи, учетные данные для каждого члена семьи, индивидуальные признаки учета каждого члена семьи, виды заболеваний, социально-реабилитационные мероприятия, доход каждого члена семьи, характеристика семьи (жилищные условия, дополнительные источники дохода, список доходов семьи, список по-

требностей семьи, список предоставленных семье льгот, список оказанной семье помощи, количественные характеристики семьи).

Функциональная подсистема «объекты системы социального защиты населения» – представлена регистром учреждений социальной защиты населения (органы социальной защиты, дома престарелых, протезно-ортопедические мастерские, пансионаты, детские лагеря отдыха, медицинские учреждения для инвалидов и престарелых, хосписы и др.). Каждый из таких объектов характеризуется своими характеристиками и особенностями в зависимости от назначения и профиля. Задача информационной системы обеспечить оказание наибольшего количества услуг социально-незащищенному населению, используя имеющиеся социальные объекты.

Все характеристики социального объекта разделены на отдельные обособленные фрагменты, позволяющие описывать данный объект по определенным параметрам: материально-техническое обеспечение (здания, помещение, оборудование учреждения), кадры – персонал учреждения (специальность, образование), финансовый блок (система бухгалтерского учета и экономического анализа), система учета оказанных услуг, позволяющая контролировать объем и качество оказанных услуг населению.

В каждом социальном учреждении стоит своя информационная система, позволяющая управлять им как объектом управления, а собранная информация со всех учреждений дает уникальную возможность определения эффективности деятельности практически всей системы социальной защиты населения.

Функциональная подсистема «Управление финансами» – позволяет осуществлять контроль расходуемых средств, проводить анализ текущего состояния, разрабатывать Программы-минимум и Целевые программы. Фактически – это планово-экономическая система, позволяющая как формировать бюджет территории в разделе социальная защита и социальное обеспечение, так и обеспечивать контроль за расходованием средств как на уровне территории, так и на уровне конкретного учреждения.

Функциональная подсистема «Законодательство» – создает нормативно-правовое обеспечение социальной защиты населения. Система управления социальной защитой населения задается системой правовых норм федерального и регионального законодательства; системой подзаконных нормативных актов организации процессов оказания социальной помощи и прекращения правоотношений физических лиц – получателей льгот и пособий с органами социальной защиты населения. Высокая интенсивность актуализации нормативно-правовой информации, как в части содержания отдельных норм, так и некоторых разделов, требует создания справочно-правовой системы, позволяющей, с одной стороны, максимально удовлетворить потребность граждан в правовой информации по данной тематике, тем самым решать проблему обеспечения

права гражданина на получение той или иной льготы и, с другой стороны, облегчить работу сотрудников органов социального обслуживания населения по законному назначению и определению льгот и пособий нуждающимся физическим лицам.

Система «Адресная социальная помощь» работает на четырех уровнях: территориальном, муниципальном, региональном и федеральном.

Автоматизированная система обработки информации «Адресная социальная помощь» состоит из шести основных программных комплексов:

– адресная социальная помощь;

– предоставление социальных услуг;

– прогнозирование ресурсов для социального обслуживания населения;

– анализ результатов социального обслуживания населения;

– формирование социально-демографического портрета района и региона;

– начисление и выплата социальных пособий.

Информационной основой системы является наличие единого банка данных, содержащий информацию социально-экономического и социально-демографического характера о той части общества, которую ставят на учет в органах и учреждениях социальной защиты населения.

При этом разработаны общесистемные справочники, которые позволяют классифицировать: категории семей (социально-демографические типы семей); индивидуальные признаки учета в органах социальной защиты граждан или семьи в целом; потребности и заявки граждан в различных видах социальной помощи, услуг и льгот; виды социальной помощи и услуг, оказываемых гражданам; виды льгот, предоставленных гражданам по законодательству; источники финансирования; причины отказа в социальной помощи.

В системе автоматизированы все основные виды работ, связанные с учетом граждан и членов их семей, обращающихся в органы или учреждения социальной защиты населения, а также связанные с оказанием им различных видов социальной помощи и услуг, предоставлением льгот и с составлением различных аналитических и отчетных документов.

ПРИЛОЖЕНИЕ В

Пример титульного листа

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО РЫБОЛОВСТВУ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Калининградский государственный технический университет»

Институт цифровых технологий

Кафедра _____
наименование кафедры

Курсовой проект допущен к защите

Руководитель: _____
(уч. степень, звание, должность*)

_____ И.О. Фамилия
«___» _____ 202__ г.

Курсовой проект защищен с оценкой
_____

Руководитель: _____
(уч. степень, звание, должность)

_____ И.О. Фамилия
«___» _____ 202_ г.

ТЕМА КУРСОВОГО ПРОЕКТА

Курсовой проект по дисциплине
«Наименование дисциплины»
КР.ХХ1.ХХ.ХХ.ХХ2.Х3.Х4

Проект выполнил:
студент гр._____
___ _____ И.О. Фамилия
«___» _____ 20__ г.

Калининград
202__

ПОЯСНЕНИЯ

Обозначения в шифре

КП.ХХ1.ХХ.ХХ.ХХ2.Х3.ХХ4.ПЗ

КР – курсовой работа.
КП – курсового проект.
ХХ1 – номер кафедры.
ХХ.ХХ.ХХ2– шифр направления подготовки
Х3 – последняя цифра года, когда выполнена проект (например, 2022 год, будет цифра 2).
ХХ4 – номер варианта курсового проекта.
ПЗ – пояснительная записка

*Ученую степень и звание следует сокращать в соответствии с рекомендациями Министерства науки РФ, например:

Сокращение	**Полное написание**
Учёные степени	
д-р биол. наук	доктор биологических наук
д-р с.-х. наук	доктор сельскохозяйственных наук
д-р техн. наук	доктор технических наук
канд. с.-х. наук	кандидат сельскохозяйственных наук
канд. техн. наук	кандидат технических наук
канд. хим. наук	кандидат химических наук
Учёные звания	
доц.	доцент
проф.	профессор

ПРИЛОЖЕНИЕ Г

Пример оформления структурного элемента курсового проекта «Содержание»

СОДЕРЖАНИЕ

ПРИЛОЖЕНИЕ Д

Пример оформления заголовков и подзаголовков

1. СОВРЕМЕННЫЕ МЕТОДЫ И СИСТЕМЫ РЕЗЕРВИРОВАНИЯ
(по центру)

1.1 Требования к современным системам резервирования
(с абзацного отступа)

«Процедура разработки и проектирование систем резервирования проводится с учетом определенных правил и характеристик. Например, в процессе выбора систем резервного копирования надо соблюдать определенные требования к характеристикам процесса резервирования и процесса хранения, которые учитываются при разработке этой системы и называются, как принято, Service Level Agreement (соглашение об уровне предоставления услуги). При рассматривании общих технических требований обычно используют такие понятиями как «RPO», «RTO», «RTA», «Data Security» и т. д. И так, что же означает каждая характеристика» [4.16].

Данные разной важности требуют разного обращения с собой, это очевидно. Востребованные и важные документы необходимо хранить более бережно. Разделив данные по частоте обновления можно, к примеру, сэкономить время, занимаемое резервным копированием.

Пример двух различных типов резервного копирования данных, которые необходимо выполнять раздельно друг от друга:

— Резервное копирование данных. Это различного рода невостребованные документы (документы Word, фотоснимки, аудио и видеозаписи). Аналогично к этому могут относиться закладки браузера, письма в почтовом ящике, адресная книга, календарь со встречами, конфигурационный файл различных банковских приложений и т. д.

— Резервное копирование системы. Речь идет о копировании операционной системе со всеми ее настройками и характеристиками. Такой backup обязателен и избавляет от необходимости устанавливать операционную систему заново, делать все настройки, устанавливать программы.

Помимо предъявляемых требований к системам резервирования, а также их принципов, существуют некоторые ограничивающие факторы, определяющие рамки функциональности системы резервирования.

ПРИЛОЖЕНИЕ Е

Пример оформления структурного элемента «Введение»

ВВЕДЕНИЕ

Поскольку в цифровую эпоху объем данных растет очень быстро, а утечки данных происходят чаще, чем когда-либо прежде, предотвращение утечки конфиденциальной информации неавторизованным сторонам становится одной из самых серьезных проблем безопасности для предприятий.

Утечка данных представляет собой серьезную угрозу для работы предприятий, таких как корпорации и правительственные учреждения. Потеря конфиденциальной информации может привести к значительному ущербу для репутации и финансовым потерям и даже может нанести ущерб долгосрочной стабильности организации.

Актуальность работы заключается в том, что в современных условиях в деятельности предприятий и организаций все большую роль играет защита коммерческих сведений.

Системы состоят из фото- или видеокамеры и специализированного программного обеспечения, которое идентифицирует и классифицирует объекты. Они способны анализировать образы (фотографии, картинки, видео, штрихкоды), а также лица и эмоции. [5]

Таким образом, целью курсового проекта является разработка приложения для анализа изображения документа, считывания с него печатных символов и классификация документа по содержанию персональных данных.

Объект исследования – OCR-системы.

Предметом исследования является разработка и тестирование приложения.

Задачи курсового проекта:

– Рассмотреть основные проблемы безопасности на предприятии.

– Классифицировать угрозы.

– Проанализировать возможность утечки документов, представляющих коммерческую тайну.

– Разобрать тему компьютерного зрения, в особенности технологии оптического распознавания символов.

ПРИЛОЖЕНИЕ Ж

Пример оформления структурного элемента «Список использованных источников»

КНИГА ПОД ФАМИЛИЕЙ АВТОРА

Книга с ОДНИМ АВТОРОМ

ПРАВИЛО: библиографическое описание документа начинается с фамилии автора, если авторов НЕ БОЛЕЕ ТРЕХ.

Учебник, учебное пособие

Дорман, В. Н. Экономика организации. Ресурсы коммерческой организации: учебное пособие / В. Н. Дорман; под редакцией Н. Р. Кельчевской. – Москва: Юрайт; Екатеринбург : Изд-во Урал. ун-та, 2019. – 134 с. – (Профессиональное образование). – ISBN 978-5-534-10585-8. – Текст: непосредственный.

Игнатьев, С. В. Принципы экономико-финансовой деятельности нефтегазовых компаний: учебное пособие / С. В. Игнатьев; Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации. – Москва: МГИМО (университет), 2017. – 144 с. – ISBN 978-5-9228-1632-8. – Текст: непосредственный.

Котляров, М. А. Экономика недвижимости: учебник и практикум для бакалавриата и магистратуры / М. А. Котляров. – 2-е изд., перераб. и доп. – Москва: Юрайт, 2019. – 238 с. – (Бакалавр и магистр. Академический курс). – ISBN 978-5-9916-9081-2. – Текст: непосредственный.

Монография

Белкина, Т. Д. Экономические и социальные функции городов. Методология анализа: монография / Т. Д. Белкина. – Москва: ИНФРА-М, 2018. – 206 с. – (Научная мысль). – ISBN 978-5-16-013340-9. – Текст: непосредственный.

Морозов, С. Л. Единый универсальный календарь и его применение в мировой экономике, астронавигации и религии в эпоху четвертой цифровой промышленной революции = The uniform universal calendar and its application in to economic, astronavigations and religions during an epoch of the fourth digital industrial revolution: [монография] / С. Л. Морозов. – 7-е изд., испр. и доп. – Москва: Ваш формат, 2017. – 190 с. – ISBN 978-5-906982-02-5. – Текст: непосредственный.

Книга с ДВУМЯ АВТОРАМИ

Учебник, учебное пособие

Шапцев, В. А. Теория информации. Теоретические основы создания информационного общества: учебное пособие / В. А. Шапцов, Ю. В. Бидуля. – Москва: Юрайт, 2019. – 177 с. – (Университеты России). – ISBN 978-5-534-02989-5. – Текст: непосредственный. Шубаева, В. Г. Маркетинговые технологии в туризме: учебник и практикум / В. Г. Шубаева, И. О. Сердобольская. – 2-е изд. исправ. и доп. – Москва: Юрайт, 2019. – 120 с. – (Профессиональное образование). – ISBN 978– 5-534-10550-6. – Текст: непосредственный.

Монография

Абдрахимов, В. З. Экологический менеджмент: учеб. пособие / В. З. Абдрахимов, А. К. Кайракбаев. – Актобе: РИО Учреждения Актюбинский университет им. академика С. Баишева, 2019. – 240 с. – ISBN 978-601-7566-55-5. – Текст: непосредственный.

Кожевников, С. А. Эффективность государственного управления: проблемы и методы повышения: монография / С. А. Кожевников, Е. Д. Копытова; под ред. В. А. Ильина, Т. В. Усковой; ФГБУН «Вологодский научный центр РАН». – Вологда: ФГБУН ВолНЦ РАН, 2018. – 208 с. – ISBN 978-5-93299-402-3. – Текст: непосредственный.

Книга с ТРЕМЯ АВТОРАМИ

Учебник, учебное пособие

Джонсон, Д. Корпоративная стратегия: теория и практика: учебник / Д. Джонсон, К. Шоулз, Р. Уиттингтон. – 7-е изд.; пер. с англ. А. Ю. Заякина. – Москва: Вильямс, 2017. – 800 с. – ISBN 978-5-8459-1159-9. – Текст: непосредственный.

Поляков, Н. А. Управление инновационными проектами: учебник и практикум / Н. А. Поляков, О. В. Мотовилов, Н. В. Лукашов. – Москва: Юрайт, 2019. – 330 с. – (Бакалавр. Академический курс). – ISBN 978-5-534-00952-1. – Текст: непосредственный. Словари Варламова, Л. Н. Управление документацией: англо-русский аннотированный словарь / Л. Н. Варламова, Л. С. Баюн, К. А. Бастрикова. – Москва: Спутник+, 2017. – 398 с. – ISBN 978-5-9973-4489-4. – Текст: непосредственный.

Монография

Абдрахимов, В. З. Экологические и практические аспекты использования отходов цветной металлургии в производстве кислотоупоров и плиток для полов: монография / В. З. Абдрахимов, А. К. Кайракбаев, Е. С. Абдрахимова. –

Актобе: РИО Учреждения Актюбинский университет им. академика С. Баишева, 2018. – 200 с. – ISBN 978-601-7566-37-1. – Текст: непосредственный.

Лукин, Е. В. Организация и факторы новой индустриализации: монография / Е. В. Лукин, А. Е. Кожевников, А. Е. Мельников; под ред. Т. В. Усковой; ФГБУН «Вологодский научный центр РАН». – Вологда: ФГБУН ВолНЦ РАН, 2018. – 144 с. – ISBN 978-5-93299-408-5. – Текст: непосредственный.

КНИГА ПОД ЗАГЛАВИЕМ

ПРАВИЛО: библиографическое описание документа начинается с заглавия (названия), если книга написана ЧЕТЫРЬМЯ АВТОРАМИ. В области ответственности за косой чертой (/) приводятся ВСЕ авторы. Под заглавием, как правило, описываются коллективные монографии, сборники статей и т. п.

Книга с ЧЕТЫРЬМЯ АВТОРАМ

Учебник, учебное пособие

История сервиса: учебное пособие / В. Э. Багдасарян, И. Б. Орлов, М. В. Катагошина, С. А. Коротков. – 2-е изд. перераб. и доп. – Москва: ИНФРА-М, 2018. – 337 с. – (Высшее образование. Бакалавриат). – ISBN 978-5-16-012845-0. – Текст: непосредственный.

Международная торговля товарами и услугами: учебник для бакалавриата и магистратуры / Г. В. Кузнецова, Г. В. Подбиралина, И. М. Субботина, И. В. Головкин; Российская академия им. Г. В. Плеханова. – Москва: Юрайт, 2017. – 433 с. – (Бакалавр и магистр. Академический курс). – ISBN 978-5-534-02462-3. – Текст: непосредственный.

Экономический анализ в схемах и таблицах: учебник / М. В. Мельник, С. И. Соцкова, Г. А. Шатунова, О. Н. Поташова. – 2-е изд. перераб. и доп. – Самара: Изд-во Самар. гос. экон. ун-та, 2018. – 432 с. – (Учет и анализ – наглядно и просто). – ISBN 978-5-94622-817-6. – Текст: непосредственный.

Монография

Управление рисками приоритетных инвестиционных проектов. Концепция и методология: монография / В. Г. Антонов, В. В. Масленников, Л. Г. Скамай, А. М. Вачегин. – Москва: Русайнс, 2018. – 188 с. – ISBN 978-5– 4365-0147-5. – Текст: непосредственный.

Управленческий учет и контроль строительных материалов и конструкций: монография / В. В. Говдя, Ж. В. Дегальцева, С. В. Чужинов, С. А. Шулепина; под общ. ред. В. В. Говдя; Министерство сельского хозяйства Российской Федерации, Кубанский государственный аграрный университет им. И. Т. Тру-

билина. – Краснодар: КубГАУ, 2017. – 149 с. – ISBN 978-5-9500276-6-6. – Текст: непосредственный.

Материалы конференции

«Институциональная экономика: развитие, преподавание, приложения», международная научная конференция: сборник научных статей V Международной научной конференции «Институциональная экономика: развитие, преподавание, приложения», Москва, 15 ноября 2017 г. – Москва: ГУУ, 2017. – 382 с. – ISBN 978-5-215-03012-7. – Текст: непосредственный.

Проблемы развития предприятий: теория и практика: материалы 16-й Международной научно-практической конференции, Самара, 16–17 ноября 2017 г.: в 3 ч. Ч. 2. Региональное развитие в условиях глобализации. Развитие теории и практики менеджмента предприятий в условиях перехода к инновационной экономике / отв. ред. С. И. Ашмарина. – Самара: Изд-во Самар. гос. экон. ун-та, 2017. – 276 с. – ISBN 978-5-94622-775-9. – Текст: непосредственный.

КНИГА С ПЯТЬЮ И БОЛЕЕ АВТОРАМИ

ПРАВИЛО: при наличии информации О ПЯТИ И БОЛЕЕ АВТОРАХ приводят имена ПЕРВЫХ ТРЁХ АВТОРОВ и в квадратных скобках указывают «[и др.]»

Учебник, учебное пособие

Теория и практика немецкой грамматики = Theorie und Praktikum in der deutschen Grammatik: учебное пособие / Г. В. Глухов, Ю. И. Ефимова, О. В. Петрянина [и др.]. – Самара: Изд-во Самар. гос. экон. ун-та, 2019. – 188 с. – (Учебная литература для вузов). – ISBN 978-5-94622-897-8. – Текст: непосредственный.

Французский язык в сфере юриспруденции: учебно-методическое пособие / И. С. Голованова, Ю. Д. Ермакова, Л. В. Капустина [и др.]. – Самара: Изд-во Самар. гос. экон. ун-та, 2019. – 54 с. – ISBN 978-5-906432-21-6. – Текст: непосредственный.

Монография

Распределенные интеллектуальные информационные системы и среды: монография / А. Н. Швецов, А. А. Суконщиков, Д. В. Кочкин [и др.]. – Курск: Университетская книга, 2017. – 196 с.: ил. – ISBN 978-5-9909988-3-4. – Текст: непосредственный.

Формирование информационно-технологической компетентности будущих педагогов в электронной информационно-образовательной среде вуза: монография / В. В. Болгова, Н. П. Бурцев, С. В. Горбатов [и др.]. – Самара: Изд-во

Самар. гос. экон. ун-та, 2019. – ISBN 978-5-94622-870-1. – Текст: непосредственный.

ГОСТЫ, СТАНДАРТЫ

ГОСТ Р 57564-2017. Организация и проведение работ по международной стандартизации в Российской Федерации = Organization and implementation of activity on international standardization in Russian Federation: национальный стандарт Российской Федерации: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 28 июля 2017 г. № 767-ст: введен впервые: дата введения 2017-12-01 / разработан Всероссийским научно-исследовательским институтом стандартизации и сертификации в машиностроении (ВНИИНМАШ). – Москва: Стандартинформ, 2017. – 43 с. – Текст непосредственный.

ГОСТ Р 57618.1–2017. Инфраструктура маломерного флота. Общие положения = Small craft infrastructure. General provisions: национальный стандарт Российской Федерации: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 17 августа 2017 г. № 914-ст: введен впервые: дата введения 2018-01-01 / разработан ООО «Техречсервис». – Москва: Стандартинформ, 2017. – 7 с. – Текст: непосредственный.

ГОСТ Р 51303-2013. Торговля. Термины и определения: национальный стандарт Российской Федерации: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 28 августа 2013 г. № 582-ст: дата введения 2014-04-01. – Москва: Стандартинформ, 2014. – 22 с. – Текст: непосредственный.

ЗАКОНОДАТЕЛЬНЫЕ МАТЕРИАЛЫ

Российская Федерация. Законы. Уголовный кодекс Российской Федерации: УК: текст с изменениями и дополнениями на 1 августа 2017 года: [принят Государственной думой 24 мая 1996 года: одобрен Советом Федерации 5 июня 1996 года]. – Москва: Эксмо, 2017. – 350 с. – (Актуальное законодательство). – ISBN 978-5-04-004029-2. – Текст: непосредственный.

Российская Федерация. Законы. Об общих принципах организации местного самоуправления в Российской Федерации: Федеральный закон № 131-ФЗ: [принят Государственной думой 16 сентября 2003 года: одобрен Советом Федерации 24 сентября 2003 года]. – Москва: Проспект; Санкт-Петербург: Кодекс, 2017. – 158 с. – ISBN 978-5-392-26365-3. – Текст: непосредственный.

АВТОРЕФЕРАТ ДИССЕРТАЦИИ, ДИССЕРТАЦИЯ

Величковский, Б. Б. Функциональная организация рабочей памяти: специальность 19.00.01 «Общая психология, психология личности, история психологии»: автореферат диссертации на соискание ученой степени доктора психологических наук / Величковский Борис Борисович; Московский государственный университет им. М. В. Ломоносова. – Москва, 2017. – 44 с. – Библиогр.: с. 37-44. – Место защиты: Ин-т психологии РАН. – Текст: непосредственный.

Аврамова, Е. В. Публичная библиотека в системе непрерывного библиотечно-информационного образования: специальность 05.25.03 «Библиотековедение, библиографоведение и книговедение»: диссертация на соискание ученой степени кандидата педагогических наук / Аврамова Елена Викторовна; Санкт-Петербургский государственный институт культуры. – Санкт-Петербург, 2017. – 361 с. – Библиогр.: с. 296–335. – Текст: непосредственный.

САЙТЫ В СЕТИ ИНТЕРНЕТ

Официальный сайт Правительство Российской Федерации: официальный сайт. – Москва. – Обновляется в течение суток. – URL: http://government.ru (дата обращения: 19.02.2018). – Текст: электронный.

Министерство труда и социальной защиты Российской Федерации: официальный сайт. – 2017. – URL: https://rosmintrud.ru/docs/1281 (дата обращения: 08.04.2017). – Текст: электронный.

Научная электронная библиотека (НЭБ) eLIBRARY.RU: научная электронная библиотека: сайт. – Москва, 2000. – URL: https://elibrary.ru (дата обращения: 09.07.2019). – Режим доступа: для зарегистрир. пользователей. – Текст: электронный.

ЭБС Юрайт: электронная библиотечная система: сайт. – Москва, 2013. – URL: https://biblio-online.ru (дата обращения: 09.08.2019). – Режим доступа: для зарегистрир. пользователей. – Текст: электронный.

Электронная библиотека: библиотека диссертаций: сайт / Российская государственная библиотека. – Москва: РГБ, 2003. – URL: http://diss.rsl.ru/?lang=ru (дата обращения: 20.07.2018). – Режим доступа: для зарегистрир. читателей РГБ. – Текст: электронный.

Электронный журнал Вопросы государственного и муниципального управления: Public administration issues: электронный журнал. – URL: https://vgmu.hse.ru/about (дата обращения: 28.06.2017). – Текст: электронный.

Теория и практика каталогизации и поиска библиотечных ресурсов: электронный журнал. – URL: http://www.nilc.ru/journal/. – Дата публикации: 21 апреля 2017. – Текст: электронный. Сайт, портал Газета.Ру: [сайт] / учредитель

АО «Газета.Ру». – Москва, 1999. – Обновляется в течение суток. – URL: https://www.gazeta.ru (дата обращения: 15.04.2018). – Текст: электронный.

Российская книжная палата: [сайт]. – 2018. – URL: http://bookchamber.ru/isbn.html (дата обращения: 22.05.2018). – Текст: электронный. ТАСС: информационное агентство России: [сайт]. – Москва, 1999 – Обновляется в течение суток. – URL: http://tass.ru (дата обращения: 26.06.2018). – Текст: электронный.

СОСТАВНЫЕ ЧАСТИ (СТАТЬИ, ГЛАВЫ) РЕСУРСОВ

ПРАВИЛО: библиографическое описание составной части документа начинается с фамилии автора, если авторов НЕ БОЛЕЕ ТРЕХ или начинается с заглавия, если авторов ЧЕТЫРЕ ИЛИ БОЛЕЕ.

Статья, раздел...
...из монографического издания
…из учебника, учебного пособия

Аннушкина, В. В. Исторические предпосылки формирования первоначального накопления капитала / В. В. Аннушкина. – Текст: непосредственный // История экономических учений: учебное пособие / В. В. Аннушкина. – Саратов: Орион, 2018. – С. 18–29.

Лимитовский, М. А. Оценка корпоративных ценных бумаг / М. А. Лимитовский. – Текст: непосредственный // Корпоративный финансовый менеджмент. Финансовый менеджмент как сфера прикладного использования корпоративных финансов: учебно-практическое пособие / М. А. Лимитовский. – Москва: Юрайт, 2014. – С. 63-91.

…из материалов конференции

Калинина, Г. П. Развитие научно-методической работы в Книжной палате / Г. П. Калинина, В. П. Смирнова. – Текст: непосредственный // Российская книжная палата: славное прошлое и надежное будущее: материалы научно-методической конференции к 100-летию РКП / Информационное телеграфное агентство России (ИТАР-ТАСС), филиал «Российская книжная палата»; под общ. ред. К. М. Сухорукова. – Москва: РКП, 2017. – С. 61–78.

Фирулина, И. И. Некоторые аспекты состояния Волжского бассейна / И. И. Фирулина, А. А. Сидоров, Н. В. Лазарева. – Текст: непосредственный // Проблемы развития предприятий: теория и практика. В 3-х частях: материалы 17-й Международной научно-практической конференции, Самара, 20–21 декабря 2018 г. Ч. 3: Корпоративные информационные системы, электронные и когнитивные технологии [и др.] / Г. Р. Хасаев, Н. В. Никитина, А. А. Чудаева ; под

ред. С. И. Ашмариной. – Самара: Изд-во Самар. гос. экон. ун-та, 2018. – С. 295–301.

…из монографии

Карпунина, Т. И. Системная диагностика социально-экономических проблем современного города / Т. И. Карпунина. – Текст: непосредственный // Белкина, Т. Д. Экономические и социальные функции городов. Методология анализа: монография / Т. Д. Белкина, Т. И. Карпунина. – Москва: ИНФРА-М, 2018. – С. 26–80.

Лабынцев, Н. Т. Теоретические вопросы в области подготовки кадров / Н. Т. Лабынцев. – Текст: непосредственный // Лабынцев, Н. Т. Профессионально-общественная аккредитация и независимая оценка квалификаций в области подготовки кадров и осуществления бухгалтерской деятельности: монография / Н. Т. Лабынцев, Е. А. Шароватова; Ростовский государственный экономический университет (РИНХ). – Ростов-на-Дону: РИНХ, 2017. – С. 3–12.

Статья

...из сериального издания

...статья из журнала

Влияние психологических свойств личности на графическое воспроизведение зрительной информации / С. К. Быструшкин, О. Я. Созонова, Н. Г. Петрова [и др.]. – Текст: непосредственный // Сибирский педагогический журнал. – 2017. – № 4. – С. 136–144. Московская, А. А. Между социальным и экономическим благом: конфликт проектов легитимации социального предпринимательства в России / А. А. Московская, А. А. Берендяев, А. Ю. Москвина. – DOI 10.14515/monitoring.2017.6.02. – Текст: электронный // Мониторинг общественного мнения. – 2017. – № 6. – С. 31-35. – URL: https://wciom.ru/fileadmin/file/monitoring/2017/142/2017_142_02_Moskovskaya.pdf (дата обращения: 11.03.2017).

Скрипник, К. Д. Лингвистический поворот и философия языка Дж. Локка: интерпретации, комментарии, теоретические источники / К. Д. Скрипник. – Текст: непосредственный // Вестник Удмуртского университета. Серия: Философия. Психология. Педагогика. – 2017. – Т. 27, вып. 2. – С. 139-146. ...статья из газеты Ясин, Е. Г. Евгений Ясин: «Революция, если вы не заметили, уже состоялась»: [об экономической ситуации: беседа с научным руководителем Национального исследовательского университета «Высшая школа экономики», Москва / [записал П. Каныгин]. – Текст: непосредственный // Новая газета. – 2017. – 22 дек. (№ 143). – С. 6–7.

Статья, раздел...
…с сайта в сети Интернет

Бахтурина, Т. А. От MARC 21 к модели BIBFRAME: эволюция машиночитаемых форматов Библиотеки конгресса США: [презентация]: материалы Международной научно-практической конференции «Румянцевские чтения 2017», Москва, 18-19 апреля 2017 г.] / Т. А. Бахтурина. – Текст: электронный // Теория и практика каталогизации и поиска библиотечных ресурсов: электронный журнал. – URL: http://www.nilc.ru/journal/. – Дата публикации: 21 апреля 2017.

Грязев, А. «Пустое занятие»: кто лишает Россию права вето в СБ ООН: в ГА ООН возобновлены переговоры по реформе Совета Безопасности / А. Грязев. – Текст: электронный // Газета.ru: [сайт]. – 2018. – 2 февр. – URL: https://www.gazeta.ru/politics/2018/02/02_a_11634385.shtml (дата обращения: 09.08.2019). План мероприятий по повышению эффективности госпрограммы «Доступная среда». – Текст: электронный // Министерство труда и социальной защиты Российской Федерации: официальный сайт. – 2017. – URL: https://rosmintrud.ru/docs/1281 (дата обращения: 08.04.2017).

ПРИЛОЖЕНИЕ И

Пример оформления таблиц и формул

Таблица 1.3.1 – Применяемые и неприменяемые технологии в АИС учета имущества

№ п/п	Технологии	Применяемость
1.	Съемные носители информации	Применяются
2.	Технологии виртуализации	Применяются
3.	Технология беспроводного доступа	Не применяются
4.	Веб-технологии	Применяются
5.	Smart-карты	Не применяются
6.	Технологии грид-систем	Не применяются
7.	Технологии суперкомпьютерных систем	Не применяются
8.	Большие данные	Не применяются
9.	Числовое программное оборудование	Не применяются
10.	Одноразовые пароли	Не применяются
11.	Облачные технологии	Не применяются
12.	Электронная почта	Применяются
13.	Технология искусственного интеллекта	Не применяются

Таблица 2.5.1 – Способы реализации угроз безопасности в АИС учета имущества

Идентификатор	Способы реализации
СР.1	Использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей)
СР.2	Внедрение вредоносного программного обеспечения
СР.3	Использование не декларированных возможностей программного обеспечения и (или) программно-аппаратных средств
СР.4	Установка программных и (или) программно-аппаратных закладок в программное обеспечение и (или) программно-аппаратные средства
СР.5	Формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных

Продолжение таблицы 2.5.1

Идентификатор	Способы реализации
СР.6	Перехват (измерение) побочных электромагнитных излучений и наводок (других физических полей) для доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации
СР.7	Инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации
СР.8	Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам (в том числе администрированию, обслуживанию)
СР.9	Ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств
СР.10	Перехват трафика сети передачи данных
СР.11	Несанкционированный физический доступ и (или) воздействие на линии, (каналы) связи, технические средства, машинные носители информации
СР.12	Реализация атак типа "отказ в обслуживании" в отношении технических средств, программного обеспечения и каналов передачи данных

Пример 1:

Коэффициент эффективности, который считается по формуле:

$$К = 1 - \frac{И}{И_{max}} \qquad (3)$$

где: 1 – заведомо полная эффективность;

И – количество инцидентов за 3 месяца (20);

$И_{max}$ – максимальное количество инцидентов за 3 месяца (100).

Итого К будет равно 0,8 %.

ПРИЛОЖЕНИЕ К

Примеры оформления иллюстраций

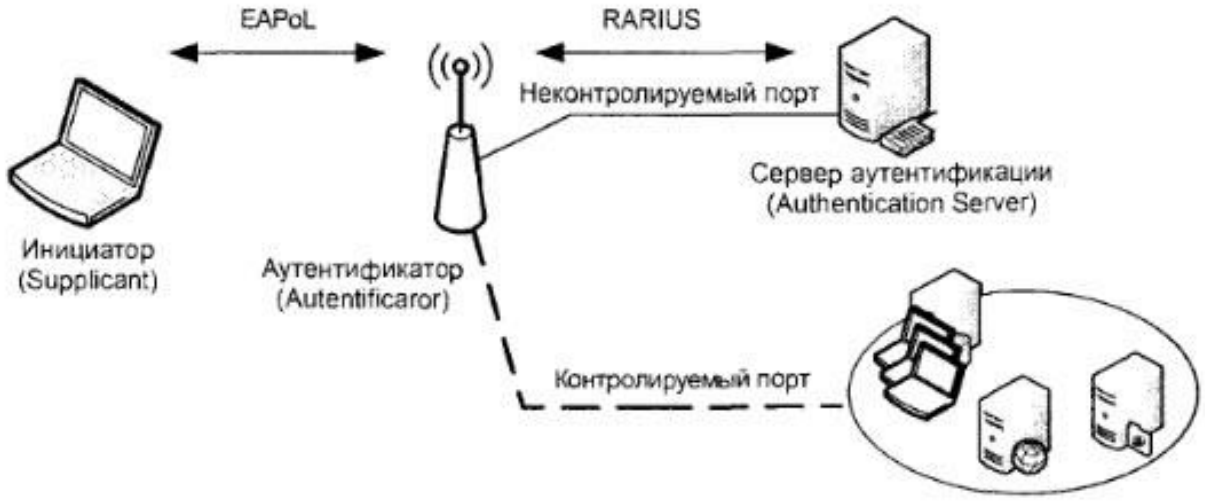

Рисунок 2.3 – Компоненты 802.11

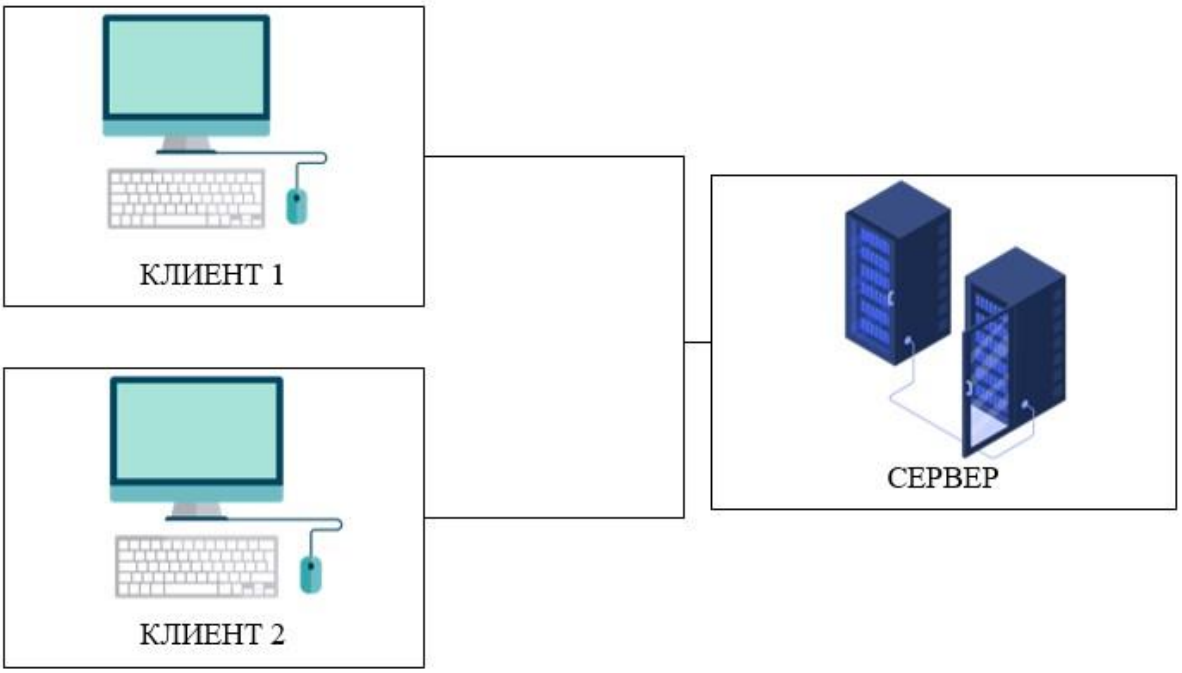

Рисунок 1.3.1 – Архитектура «клиент-сервер»

ПРИЛОЖЕНИЕ Л

Пример оформления списка использованных источников

1. Актуальные киберугрозы. – Текст: электронный // https://www.ptsecurity.com: [сайт]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/ (дата обращения: 06.04.2022).
2. Затраты федерального проекта. – Текст: электронный // https://www.cnews.ru: [сайт]. – URL: https://www.cnews.ru/articles/2021-12-20_gosudarstvo_potratit_na_kiberbezopasnost (дата обращения: 25.04.2022).
3. Кибербезопасность 2022. – Текст: электронный // https://vc.ru: [сайт]. – URL: https://vc.ru/future/362452-kiberbezopasnost-2022-statistika-trendy-ugrozy-metody-zashchity (дата обращения: 22.05.2022).
4. Возможности REDCHECK. – Текст: электронный // https://www.redcheck.ru: [сайт]. – URL: https://www.redcheck.ru/ (дата обращения: 11.05.2022).
5. ISO/IEC 27002 «Информационные технологии – Технологии безопасности – Практические правила менеджмента информационной безопасности».
6. ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий».
7. Чефранов, А. О. Администрирование системы защиты информации ViPNet (Windows & Linux / А. О. Чефранов, В. В. Гусев, В. Е. Чаплыгин. – Учебное издание. –: Горячая Линия – Телеком, 2018. – 366 с.
8. Звягинцева, П. А. Оценка эффективности средств защиты информации / П. А. Звягинцева, О. А. Крыжановксая. – Текст: непосредственный // «Интерэкспо Гео-Сибирь». – 2017. – № 3 (1). – С. 199–201.
9. Баранова С.Ю. Методики анализа и оценки рисков информационной безопасности, Вестник Московского университета им. С.Ю. Витте. Серия 3. Образовательные ресурсы и технологии, 2015. – № 1 (9). – С. 73–79.

Локальный электронный методический материал

Александр Георгиевич Жестовский

РАЗРАБОТКА И ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ

Редактор С. Кондрашова

Уч.-изд. л. 6,3. Печ. л. 5,5.

Издательство федерального государственного бюджетного образовательного учреждения высшего образования «Калининградский государственный технический университет».
236022, Калининград, Советский проспект, 1