Федеральное агентство по образованию
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ
И РАДИОЭЛЕКТРОНИКИ (ТУСУР)

Кафедра радиоэлектроники и защиты информации (РЗИ)

УТВЕРЖДАЮ
Заведующий кафедрой РЗИ
доктор технических наук, профессор
_____ А.С. Задорин
____ _____2007 г.

БАЦУЛА А.П., НЕЛЮБИН А.Б.

ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Методическое пособие по курсовому проектирования

Томск

2007

Содержание

Общие положения по выполнению курсовой работы

Курсовая работа является одной из важнейших форм учебной работы и выполняется студентом в соответствие с учебным планом.

Выполнение курсовой работы способствует углубленному усвоению лекционного материала и приобретению навыков в области оценки информации, создания комплексной системы защиты информации.

Курсовая работа базируется на изучении законов, подзаконных актов и нормативных документов в области защиты информации, методических материалах по данной тематике, а так же лекционном материале.

Выполнение работы требует от студента не только знаний общей и специальной литературы по теме, но и умение анализировать имеющуюся информацию, принимать решения по различным вопросам, увязывать вопросы теории с практикой, делать выводы и предложения по созданию комплексной системы защиты информации.

Все шаги, предпринятые студентом, все умозаключения, которые он произвёл в ходе выполнения курсового проекта (работы) должны быть им аргументированы, доказуемы и однозначно интерпретируемы.

Хотя в рамках данного методического пособия делается акцент на разработку КСЗИ для выделенных помещений, студенты не ограничены темами, предложенными в данном методическом пособии, и могут предложить свой объект защиты для исследования и разработки для него проекта комплексной системы защиты информации.

Для охвата всей тематики курса в рамках данного методического пособия принято решение ограничить число студентов по темам курсовых работ (не более одного студента на одну тему). Только если, выбранный студентами самостоятельно реальный объект защиты слишком сложен для анализа и разработки, то допускается работа над этим объектом одного-двух студентов.

Для выполнения курсовой работы студенты могут и должны пользоваться различной литературой: законами, нормативами, руководящими документами, ГОСТами, ОСТми, периодической литературой, лекциями, специальной литературой, методическими пособиями, книгами по тематики курсовой работы и т.п., а так же руководителя курсового проектирования.

На качество курсовой работы существенное влияние оказывает умелое использование практического и теоретического материалов. Подбор данных, их критическое осмысление и обработка составляют важнейший этап в подготовке и написании курсовой работы.

Графики написания, сдачи и защиты курсовых работ составляются и утверждаются кафедрой.

1. Основные этапы выполнения курсовой работы

Условно все мероприятия, связанные с выполнением студентами курсового проекта можно разбить на три этапа, подробное описание которых представлено в соответствующих разделах данного методического пособия:

- Разработка и утверждение Технического задания на курсовое проектирование.
- Разработка курсового проекта (работы).
- Защита курсового проекта (работы).

Каждый из вышеперечисленных этапов одинаково важен для достижения основных целей выполнения курсового проекта (работы) в ходе учебного процесса и должен удостаиваться одинакового внимания, как со стороны студентов, так и со стороны руководителя курсового проектирования.

2. Разработка и утверждение Технического задания

2.1. Основные сведения

Любая работа, которая требует разработки, начинается с Технического задания. Техническое задание (далее – ТЗ) является основным документом, определяющим требования и порядок создания (развития или модернизации - далее создания) какой либо системы, в соответствии с которым проводится разработка системы и ее приемка при вводе в действие.

Создание ТЗ предполагает наличие как минимум двух заинтересованных сторон: Заказчика, Исполнителя. Заказчик является инициатором проведения работ по созданию ТЗ, Исполнитель, в свою очередь реализует эти мероприятия и согласует полученные результаты с Заказчиком. При необходимости к созданию ТЗ могут привлекаться третья сторона в лице Организаций, обязанных согласовывать либо отдельные части ТЗ, либо ТЗ в целом согласно действующему законодательству или пожеланиям Заказчика.

Состав, содержание и правила оформления ТЗ в Российской Федерации определяются документами уровня ГОСТ, либо внутренними документами Заказчика системы. В частности состав, содержание и правила оформления ТЗ на автоматизированные системы вне зависимости от их назначения определяются ГОСТ 34.602-89 «Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы».

Согласно ГОСТ 51583-2000 «Порядок создания автоматизированных систем в защищённом исполнении», ГОСТ 34.601-90 «Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания» и д.р. им подобных нормативных документов, при разработке какой-либо системы стадии разработки ТЗ предшествуют стадии формирования требований к системе и разработки концепции системы. Выполнение данных стадий подразумевает под собой детальное изучение разрабатываемой системы.

Особенности учебного процесса вносят свои коррективы в создание ТЗ. В частности является затруднительным детальное изучение разрабатываемой системы студентом до получения им ТЗ, так как ТЗ в учебном процессе, по сути, является указанием начала выполнения курсового проекта (работы).

В связи с этим, ТЗ, создаваемое в рамках данного методического пособия, не содержит в себе тех разделов, которые подразумеваются ГОСТ. Однако, для развития у студентов навыков реальной работы, разработка разделов, не вошедших в ТЗ, предусмотрена непосредственно в ходе выполнения курсового проекта (работы).

2.2. Содержание работ по разработке и утверждению Технического задания

Техническое задание (ТЗ) разрабатывается на основе задания, выданного студенту. В данном случае студент выступает в роли Исполнителя, руководитель профилирующей кафедры – Заказчиком ТЗ, а руководитель курсового проектирования в роли третьего лица, согласующего ТЗ в целом. Срок разработки студентом ТЗ не должен превышать 15 календарных дней со дня получения им задания.

Разработанный студентом проект ТЗ согласовывается руководителем курсового проектирования и утверждается руководителем профилирующей кафедры.

Срок согласования технического задания не должен превышать 15 дней. За данный период времени студент и руководитель курсового проектирования обязаны выявить, обсудить и устранить все замечания по представленному на согласование проекту ТЗ.

Замечания по проекту ТЗ должны быть представлены с обоснованием. Замечания, выдвигаемые руководителем курсового проектирования, должны быть аргументированы и при необходимости разъяснены студенту. В случае если студент и руководитель курсового проектирования не могут прийти к согласованию по разделам ТЗ, к процессу согласования привлекаются другие

преподаватели профилирующей кафедры.

Согласованию подлежит как само ТЗ, так и все приложения к нему.

После согласования ТЗ руководителем курсового проектирования, ТЗ передаётся им на согласование руководителю профилирующей кафедры. Срок утверждения ТЗ не должен превышать 7 дней со дня подачи.

Регистрация, учёт и хранение технического задания и приложений к нему осуществляется в соответствии с ГОСТ 2.501-88.

2.3. Содержание Технического задания

ТЗ, разрабатываемое студентом в рамках выполнения курсового проектирования, содержит как минимум следующие разделы, которые допускается делить на подразделы:

1. *Описание объекта защиты*. Данный раздел содержит краткое описание объекта защиты. Все необходимые данные об объекте должны быть занесены в приложения к ТЗ.
2. *Цель написания курсовой работы*. Курсовая работа является завершающим этапом изучения дисциплины. Формулируемая студентом цель курсового проектирования должна быть четкой, прозрачной и достижимой. Достижение поставленной цели при выполнении курсового проекта (работы) является одним из критериев её оценки – нечеткая, неточная или заранее недостижимая цели существенно затруднит защиту курсового проекта (работы).
3. *Содержание курсовой работы*. Раздел содержит название основных этапов выполнения курсового проекта (работы). Согласно ГОСТ 34.601-90 с учётом корректировок вносимых учебным процессом, при выполнении курсового проекта (работы) студентом должны быть последовательно выполнены следующие разделы:

– Анализ объекта защиты.
– Формирование требований к создаваемой КСЗИ.
– Разработка концепции создаваемой КСЗИ.

– Разработка проектного решения по КСЗИ.

  Допускается добавлять дополнительные разделы и более подробно расписывать вышеуказанные разделы.

4. *Источники.* В данном разделе перечисляются базовые нормативные и методические материалы, которыми студент будет руководствоваться в своей деятельности.
5. *Приложения.* В данном разделе приводится перечень приложений к ТЗ.

Пример оформленного в соответствии с данными требованиями ТЗ представлен в Приложении Д.

2.4. Приложения к Техническому заданию

Так как ТЗ является основным документом для разработки, создания и ввода в действие какой-либо системы, то в ТЗ должны быть, как минимум, приведены предварительные сведения о создаваемой системе.

ТЗ, создаваемое в рамках данного методического пособия предполагает наличие трёх приложений:

– Территориальный план местности, с расположенным на нём зданием.
– План выделенного помещения.
– Сводная таблица с данными о выделенном помещении.

В рамках данного методического пособия студенту предлагается воспользоваться следующими приложениями для разработки ТЗ и приложений к нему:

– *Приложение А.* Описывает территориальные планы местности, со зданием и помещениями. Всего представлено 2 варианта территориальных планов, с указанием взаимного расположения 10 зданий.
– *Приложение Б.* Описывает взаимное расположение выделенного помещения с другими помещениями, расположенными на одном с ним этаже. Всего представлено 10 этажных планов.

- П*риложение В*. Приводятся необходимые характеристики выделенного помещения. Всего представлено 58 вариантов.
- П*риложение Г*. Приводятся таблицы с описанием инфраструктуры выделенного помещения. Все полученные из этих таблиц данные необходимо будет занести в таблицу *приложения Ж*. Всего таблиц 8. В каждой таблице от 3х до 9ти параметров.
- *Приложение Д*. Содержит варианты заданий на курсовое проектирование. В этом пронумерованном списке под каждым номером находится вариант задания, состоящий из цифр, каждая из которых обозначает номер в таблице из приложения Г. На основе этих данных студент формирует свое ТЗ.
- *Приложение Е*. Представлен пример оформления ТЗ.
- *Приложение Ж*. Представлена форма сводной таблице сведений о выделенном помещении с методикой её заполнения.

3. Разработка курсового проекта

3.1. Этапы разработки курсового проекта

Как уже говорилось ранее, учебный процесс вносит свои коррективы в порядок разработки проектов (работ) по КСЗИ, предусмотренный нормативными документами уровня ГОСТ, в частности ГОСТ 51583-2000.

В связи с этим, процесс разработки проектов по КСЗИ в данном методическом пособии будет заключаться в выполнении следующих этапов:

- Анализ объекта защиты.
- Формирование требований к создаваемой КСЗИ.
- Разработка концепции создаваемой КСЗИ.
- Разработка проектного решения поКСЗИ.

3.2. Анализ объекта защиты

Прежде чем что-то защищать необходимо понять, что и зачем необходимо защищать. Как следует из названия предмета, закрепление основ которого выполняется путем выполнения курсового проекта (работы), объектом защиты является Информация, принадлежащая кому-то, обладающая определенной ценностью и обрабатываемая определённым образом. Следовательно, самый первый и важный вопрос, который должен возникнуть при начале работы над курсовым проектом: Что представляет собой информация?

3.2.1. Понятие информации

Несмотря на то, что существует множество определений термина «Информация», однозначного строго научного однозначного определения не существует. Наблюдается скорее «локальное» применение данного термина в разных сферах деятельности различное смысловое наполнение.

Согласно философскому словарю, *информация* (лат. informatio - разъяснение, изложение, осведомленность) – одно из наиболее общих понятий науки, обозначающее некоторые сведения, совокупность каких-либо данных, знаний,

результат отражения одного объекта в другом, используемый в конечном счете для формирования управляющих воздействий [1].

Согласно Российской энциклопедии, *информация* (от лат. informatio — разъяснение, изложение), первоначально — сведения, передаваемые людьми устным, письменным или другим способом (с помощью условных сигналов, технических средств и т. д.); с середины XX в. общенаучное понятие, включающее обмен сведениями между людьми, человеком и автоматом, автоматом и автоматом; обмен сигналами в животном и растительном мире; передачу признаков от клетки к клетке, от организма к организму; одно из основных понятий кибернетики [2].

Согласно словарю Ожегова, *информация* – сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком или специальным устройством [3].

В области разведки, *информация* — сведения, раскрываемые технической разведкой через демаскирующие признаки объектов защиты или путем несанкционированного доступа к техническим средствам обработки информации [4].

Согласно закону «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ, *информация* - сведения (сообщения, данные) независимо от формы их представления.

Из всего множества определений попробуем сформулировать именно то понятие, которое будет определять слово «информация» в данном методическом пособии. Информация есть нечто, что является:

- объектом собственности;
- объектом защиты и объектом угроз;
- объектом и средством производства;
- объектом анализа, систематизации и структурирования.
- объектом обработки.

Грубо говоря, *информация* – это сведения, которые циркулируют внутри организации и сведения о самом организации, часть из которых нуждается в защите. Часть – потому, что защищать все сведения, которые циркулируют внутри предприятия, не целесообразно. Защищать всё – накладно и не разумно, потому что всегда есть информация, которая не представляет ценности и защита ее лишь осложнит защиту информации, действительно нуждающейся в защите.

Один из важнейших вопросов – выделение информации, требующей защиты, из всего массива информации, обрабатываемой в организации, и реализация необходимых организационно-технических мероприятий по ее защите.

3.2.1.1. Информация как объект собственности

Право собственности – основной институт любой системы права; совокупность правовых норм, закрепляющих состояние присвоенности (принадлежности) вещей – средств производства и результатов труда - за отдельными лицами или коллективами и основанные на этом правомочия владения, пользования и распоряжения ими указанными вещами». (БСЭ)

Федеральный закон РФ от 20.07.2006 № 149 об «Информации, информатизации и защите информации» определяет три категории субъектов, так или иначе реализующих право собственности на информацию:

Собственник – субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения.

Владелец – субъект, осуществляющий владение и пользование указанными объектами (информацией) и реализующий полномочия распоряжения в пределах, установленных законом.

Пользователь – субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

Ряд других нормативных документов РФ так же описывают право собственности Субъекта на Информации, например, происходит деление Информации на открытую и с ограниченным доступом []. Характер реализации права собственности описывается данными нормативными актами и отражает существующий взгляд на Информацию как на объект экономических отношений.

3.2.1.2. Информация как объект защиты и угроз

В соответствии с ФЗ РФ «Об информации, информационных технологиях и о защите информации» от 27.06.2006г. N 149-ФЗ, защите подлежит следующая информация:

- информация, составляющая государственную тайну, в соответствии с законодательством Российской Федерации о государственной тайне;
- коммерческая тайна, служебная тайна и иная тайна, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение;
- информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), Такая информация подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации;
- персональные данные в соответствии с законом «О персональных данных» от 27.07.2006г. №152-ФЗ.

Защита информации – деятельность по предотвращению утраты и утечки конфиденциальной информации и утраты защищаемой открытой информации [5].

При защите информации стоит руководствоваться принципами информационной безопасности:

- *законность* (соблюдение норм международного, права Конституции РФ и законодательства РФ при осуществлении деятельности по обеспечению информационной безопасности);
- *сбалансированность* (соблюдение баланса интересов субъектов правоотношений, их взаимная ответственность);
- *реальность выдвигаемых задач* (с учетом имеющихся ресурсов, сил и средств);
- *сочетание* централизованного управления силами и средствами обеспечения безопасности с передачей в соответствии с федеральным устройством России части полномочий в этой области органам государственной власти субъектов РФ и органам местного самоуправления;
- интеграция с международными системами обеспечения информационной безопасности [6].

Необходимость защиты информации возникает не только и не столько благодаря законам и подзаконным актам. Информация обладает тремя основными свойствами, с помощью которых собственник определяет ценность информации и меры по ее защите:

- конфиденциальность;
- целостность;
- доступность.

Ценность информации для субъекта, так или иначе реализующего права владения, пользования и распоряжения информаций, в контексте свойства конфиденциальности означает, что данный субъект имеет преимущество перед другими субъектами в силу того, что другие субъекты не могут использовать эту информацию в своей деятельности.

Ценность информации для субъекта, так или иначе реализующего права владения, пользования и распоряжения информаций, в контексте свойства целостности означает, что данный субъект имеет возможность воспользоваться дан-

ной информацией в своей деятельности, при этом информация несет в себе то, что от неё ожидает субъект.

Ценность информации для субъекта, так или иначе реализующего права владения, пользования и распоряжения информаций, в контексте свойства доступности означает, что данный субъект имеет возможность воспользоваться данной информацией в своей деятельности в необходимый ему момент времени, при этом промежуток времени между обращением к информации и её использованием является удовлетворительным.

Ценности принято охранять – информация является объектом защиты для субъекта, так или иначе реализующего права владения, пользования и распоряжения информаций, в силу того, что имеет для него некоторую ценность.

Информация является объектом угроз в силу намерений и возможности других субъектов нанести вред субъекту, так или иначе реализующему права владения, пользования и распоряжения информаций, либо самими стать данными субъектами нарушая при этом права первого субъекта.

В целях определения адекватного набора мер защиты проводят категорирование информации по степени важности и возможным негативным последствиям в случае нарушения ее свойств конфиденциальности, целостности и доступности. Категорирование информации заключается в присвоении информации конкретных значений критериев конфиденциальности, целостности, доступности. Категорирование информации, а также средств ее обработки, позволяет определить требуемый уровень защиты и оптимизировать расходы на организационно-технические мероприятия по обеспечению защиты информации. Чем четче категорирована информация, тем меньше потери при ее обработке и анализе. Правильное категорирование позволяет получать для работы и передавать только нужную информацию [7].

Значение критерия конфиденциальности не зависит от способов обработки, хранения и мест хранения информации.

Конфиденциальность информации - субъективно определяемая (присваиваемая государством или собственником) характеристика (свойство) информации, указывающая на необходимость введения ограничений на круг субъектов (лиц), имеющих доступ к данной информации, и обеспечиваемая способностью системы (инфраструктуры) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на доступ к ней [7].

Для информации, отнесенной в соответствии с перечнем «сведений, составляющих государственную тайну» закона «О государственной тайне» у государственной тайны критерий конфиденциальности необходимо соотносить с грифами секретности, определенными законом.

Для государственной тайны критерий конфиденциальности – степень секретности сведений (гриф), отнесенных к ней. В РФ принята следующая система обозначения сведений в соответствии с законом «О государственной тайне», составляющих государственную тайну:

- особой важности;
- совершенно секретно;
- секретно.

К *сведениям особой важности* следует относить сведения, распространение которых может нанести ущерб интересам РФ в одной или нескольких областях деятельности.

К *совершенно секретным сведениям* следует относить сведения, распространение которых может нанести ущерб интересам Министерства (ведомства) или отраслям экономики РФ в одной или нескольких областях деятельности.

К *секретным сведениям* следует относить все иные из числа сведений, составляющих государственную тайну. Ущерб может быть нанесен интересам предприятия, учреждения или организации.

Из этих определений можно видеть сравнительно высокую степень неопределенности признаков, характеризующих ту или иную степень секретности

сведений, составляющих государственную тайну. Поэтому всегда остается место для самостоятельного определения критерия конфиденциальности в процессе засекречивания информации.

Эти грифы проставляются на документах или изделиях (их упаковках или сопроводительных документах) Содержащиеся под этими грифами сведения, являются государственной тайной [5].

Конфиденциальная информация в свою очередь включает в себя то множество тайн, которое предлагается свести к пяти основным видам (один из возможных вариантов классификации конфиденциальных сведений):

- коммерческая тайна;
- банковская тайна;
- профессиональная тайна;
- персональные данные;
- служебная тайна.

Для информации, отнесенной к коммерческой тайне, критерий конфиденциальности имеет важное значение, поскольку именно он, в соответствии с законом «О коммерческой тайне», определяет эту информацию. Это видно из самого определения коммерческой тайны: «коммерческая тайна - *конфиденциальность* информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду».

Коммерческая тайна – научно-техническая, технологическая, коммерческая, организационная или иная используемая в экономической деятельности информация, имеющая действительную потенциальную коммерческую ценность в силу ее неизвестности третьим лицам, которые могли бы получить выгоду от ее разглашения или использования, к которой нет свободного доступа на

законном основании, и по отношению к которой принимаются адекватные ее ценности, меры охраны [7].

Коммерческая информация может быть ранжирована по степени ее важности для предприятия с тем, чтобы регулировать ее распространение среди работающих на предприятии, указать пользователей этой информации, уровень ее защиты и т. д.

Одной из возможной классификаций сведений, составляющих коммерческую тайну, может быть деление их на три уровня конфиденциальности:

- коммерческая тайна – строго конфиденциально (КТ – СК);
- коммерческая тайна – конфиденциально (КТ – К);
- коммерческая тайна (КТ) [8].

Для коммерческой тайны, помимо вышеупомянутой системы категорирования, можно использовать свои критерии конфиденциальности. Можно ввести систему градаций, по которым будет определяться конфиденциальность информации. Эту систему категорирования рекомендуется использовать и для других видов конфиденциальной информации, и для не конфиденциальной информации, но по мнению собственника (владельца) важной для предприятия. Число градаций не ограниченно, все зависит от конкретного случая. Студент свободен в выборе системы классификации и числа уровней классификации. Единственное требование – обоснование своего выбора.

Кроме того, можно воспользоваться Методикой «Категорирование и дифференцированный подход к защите информации», которая предполагает 6ти градационную систему категорирования информации по критерию конфиденциальности:

- **К0** (критическая) – разглашение информации приведёт к краху предприятия или к значительным потерям (людским, экономическим, моральным). Ликвидация последствий разглашения либо невозможна,

либо связана со значительными экономическими, временными и моральными затратами.

- **К1** (очень важная) – разглашение приведет к большим потерям (экономическим, моральным). Ликвидация последствий разглашения связана с большими экономическими, временными и моральными затратами.
- **К2** (важная) – разглашение приведет к некоторым материальным (возможно, косвенным) и/или моральным потерям. Ликвидация последствий разглашения связана с некоторыми экономическими, временными и моральными затратами.
- **К3** (значимая) – разглашение приносит незначительный экономический и/или моральный ущерб. Ликвидация последствий разглашения связана с незначительными экономическими, временными и моральными затратами.
- **К4** (малозначимая) – разглашение может принести моральный ущерб в очень редких случаях.
- **К5** (несущественная) – не влияет на работу субъекта.

Значение критерия конфиденциальности не зависит от способа и места её обработки, значение же *остальных* критериев является зависим от способов обработки и хранения информации, а так же места хранения этой информации, т. е. значения критериев целостности и доступности определяются в зависимости от особенностей работы конкретного объекта [6].

Доступность информации (задачи) – свойство системы обработки (инфраструктуры), в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ субъектов (пользователей) к интересующей их информации (при наличии у субъектов соответствующих полномочий на доступ) и готовность соответствующих автоматизированных служб (функциональных задач) к обслуживанию поступающих от субъектов запросов.

При определении значения величины критерия **доступности** информации принимается во внимание максимально возможный ущерб, который может быть нанесён предприятию, его клиентам, корреспондентам, партнерам или сотрудникам в результате блокирования информации, ведущей к нарушению доступности решаемых задач.

Методика «Категорирование и дифференцированный подход к защите информации» предполагает 5 градаций значимости критерия:

Целостность информации – свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

Д0 (критическая) – без доступа к этой информации работа останавливается;

Д1 (очень важная) – без доступа к этой информации можно работать, но очень короткое время;

Д2 (важная) – без доступа к этой информации можно работать, но рано или поздно она понадобится;

Д3 (полезная) – без доступа к этой информации можно работать, но ее использование экономит ресурсы;

Д4 (несущественная) – устаревшая или неиспользуемая информация, не влияющая на работу;

Д5 (вредная) – ее наличие требует обработки, а обработка ведет к расходу ресурсов, не давая результатов, либо принося ущерб.

При определении значения величины критерия целостности информации принимается во внимание максимально возможный ущерб, который может быть нанесён предприятию, его клиентам, корреспондентам, партнерам или сотрудникам в результате нарушения целостности рассматриваемой информации. Введём 5 градаций значимости критерия:

Ц0 (критическая) – несанкционированное изменение информации приведёт к краху предприятия или к значительным потерям (людским, экономическим, моральным);

Ц1 (очень важная) – ее несанкционированное изменение приведет к большим потерям (экономическим, моральным);

Ц2 (важная) – ее несанкционированное изменение приведет к некоторым материальным (возможно, косвенным) и/или моральным потерям;

Ц3 (значимая) – ее несанкционированное изменение приведёт к незначительному экономическому и/или моральному ущербу;

Ц4 (не значимая) – ее несанкционированное изменение не скажется на работе предприятия;

Полная версия методики «Категорирование и дифференцированный подход к защите информации» представлена в Приложении 3.

Как уже говорилось выше, студент не ограничен как в выборе методики классификации ценности информации, так и в модификации представленной выше методики, главное, чтобы все рассуждения были аргументированы и доказуемы.

Защищаемая информация, в отличие от открытой, имеет свои особенности:

- засекречивать информацию, то есть ограничивать к ней доступ, может собственник (владелец) или уполномоченные им на то лица в соответствии с ФЗ РФ «Об информации, информатизации и защите информации», ФЗ РФ «О коммерческой тайне»;
- чем важнее для собственника информация, тем тщательнее он ее защищает. А для того чтобы все, кто сталкивается с этой защищаемой информацией, знали, что одну информацию необходимо оберегать более тщательно, чем другую, собственник определяет ей различную степень секретности (для государственной и коммерческой тайн) или производит категорирование информации по разным критериям;

– защищаемая информация должна приносить определенную пользу ее собственнику и оправдывать затрачиваемые на ее защиту силы и средства [7].
– обращение информации, подлежащей защите, происходит в определенной, ограниченной защитными мерами сфере – научно-производственной, управленческой, коммерческой и др. *Меры по защите информации* – это специальные меры, направленные на предотвращение утечки защищаемых сведений и нарушения основных свойств информации.
– принятие специальных мер, направленных на защиту интеллектуальной собственности, зависит прежде всего от собственника (владельца) информации, складывающейся в их среде деятельности конкурентной обстановки, ценности, которую представляет для них информация, и других факторов [8].

3.2.1.3. Информация как объект и средство производства

Согласно Большой Советской Энциклопедии (БЭС): средства производства - совокупность средств и предметов труда, используемых людьми в процессе производства материальных благ и услуг. С помощью средств труда человек воздействует на предмет труда с целью создания потребительской стоимости.

Например, средствами производства могут быть машины, станки, специальные устройства, позволяющие перерабатывать поступающее на них сырье в готовый продукт.

Ранее уже говорилось, что информация имеет ценность для субъекта в силу того что он её использует в своей деятельности, следовательно информацию можно рассматривать как средство производства.

Действительно, если результатом применения информации стало получение новой информации (продукта или услуги), то такую информацию можно назвать средством производства. А полученная новая информация в свою оче-

редь является объектом производства. Первоначальная информация может не представлять никакой ценности, но собранная воедино и переработанная, она будет нести в себе уже потребительскую стоимость.

Обработка информации называется информационными процессами.

3.2.1.4. Информация как объект анализа, систематизации, структурирования, обработки

Информационные процессы, которым подвержена защищаемая информация, сами нуждаются в постоянном контроле. Информация все время обновляется, модифицируется, удаляется – этот постоянный процесс видоизменения информации.

Информационным называют *процесс*, связанный с определенными операциями над информацией, в ходе которых может измениться содержание информации или ее форма.

Важность информационных процессов состоит в том, что они приводят к различным изменениям в течение событий, к возникновению новых событий. Свойства информационных процессов не зависят от того, где эти процессы происходят, какие объекты в них участвуют.

Информационный процесс – процесс, использующий совокупность средств и методов сбора, обработки и передачи данных.

3.2.2. Понятие факторы, воздействующие на информацию

Как и любой элемент Вселенной, информация подвержена влиянию других элементов. В контексте данной методички будем говорить существовании факторов, способных повлиять на свойства информации (безопасность).

Наиболее опасные факторы, которые могут стать угрозой информационной безопасности, перечислены в ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию».

В ГОСТ Р 51275-99 применён следующий принцип классификации

факторов, воздействующих на защищаемую информацию, следующий:

- подкласс;
- группа;
- подгруппа;
- вид;
- подвид.

В каждом конкретном случае анализа объекта защиты его окружение вносит коррективы в состав факторов по ГОСТ Р 51275-99. Перечень может сокращаться, либо наоборот расширяться (добавляться или конкретизироваться).

3.2.3. Понятие угроза информации

Угроза информации – потенциальная или реальная опасность изменения свойств информации, возникающая или способная возникнуть в результате воздействия на информацию различного рода факторов.

Так, как цель защиты информации – сохранение основных свойств информации, таких как конфиденциальность, целостность, доступность, то все множество угроз можно разделить на три группы:

- Нарушение конфиденциальности информации – потеря ценности информации при ее раскрытии.
- Нарушение целостности информации – это потеря ценности информации при изменении или уничтожении.
- Нарушение доступности информации – это потеря ценности при нарушении возможности доступа к ней в течении определенного промежутка времени.

Наиболее распространенными последствиями реализации угроз являются:

Для конфиденциальности информации:

Разглашение защищаемой информации – несанкционированное ознакомление с ней лиц, не имеющих законного доступа к этой информации, лицом, которому эти сведения были доверены или стали известны по службе или работе. Разглашение защищаемой информации создает угрозу завладения ею злоумышленником.

Раскрытие защищаемой информации – это опубликование ее в средствах массовой информации, использование в публичных выступлениях собственником или владельцем этой информации или лицами, которым эта информация была доверена по работе. В данном случае секретная или конфиденциальная информация становится достоянием неопределенно широкого круга лиц, утрачивает свою секретность, ценность и потребительскую стоимость.

Распространение защищаемой информации – открытое использование этих сведений.

Утечка защищаемой информации – это несанкционированное, неправомерное завладение соперником этой информацией и получение возможности использования ее в своих целях в ущерб интересам собственника (владельца) информации.

Под утечкой информации может также пониматься ее несанкционированное разглашение, выход ее за пределы круга лиц, которым эта информация была доверена. Однако одного этого признака недостаточно, чтобы считать факт утечки информации состоявшимся. Основным признаком утечки информации должен считаться факт завладения защищаемой информацией злоумышленником.

НСД – получение защищаемой информации злоумышленником с нарушением установленных правовыми документами или собственником (владельцем) информации прав или правил доступа к защищаемой информации;

Копирование информации – изготовление копий защищаемой информации для дальнейшего использования этих копий злоумышленником или лицами, которым он мог ее передать.

Для целостности информации:

Уничтожение информации – это полная физическая ликвидация информации или ликвидация таких ее элементов, которые влияют на изменение существенных идентифицирующих информацию признаков. Для целостности информации – это наиболее опасное явление, так как при этом собственнику наносится максимально реальный вред.

Модификация информации – это внесение в нее любых изменений, обусловливающих ее отличие от той, которую включил в систему и которой владеет собственник.

Для доступности:

Блокирование информации – это ограничение доступа к самой информации, в следствии чего возникает невозможность ее использования в работе предприятия в течение некоторого, а иногда и не определенного, времени.

В рамках данного методического пособия будем различать *потенциальные* и *реальные* угрозы. Под *потенциальными* будем понимать угрозы, которые существуют по причине существования факторов, воздействующих на информацию. Под *реальными* будем понимать те *потенциальные* угрозы, для которых существуют уязвимости, способные составить *канал реализации угрозы* (см. ниже).

Любая угроза для безопасности информации имеет свой *источник*. Невозможно эффективно противодействовать угрозе, если неизвестен ее источник. Устранение угрозы, без устранения ее источника, может привести к тому, что угроза может возникнуть вновь с более серьезными последствиями. Своевременное выявление источника угрозы, может, если не предотвратить воздействие угрозы, то хотя бы уменьшить ее влияние на защищаемую информацию.

Говоря об источнике угрозы, в современной литературе принято применять термин «Злоумышленник».

3.2.4. Понятие модель злоумышленника

Злоумышленник реализует (способен реализовать) угрозу (применяет факторы) в определенном месте и времени, то есть осуществляет атаку на защищаемую информацию. Воздействие атаки на информацию может быть различным и, соответственно, различным будет и ущерб, который понесет собственник (владелец).

Основная цель анализа угроз информационной безопасности заключается в построении модели злоумышленника.

Построение модели злоумышленника - это процесс классификации потенциальных злоумышленников по следующим параметрам:

1. Тип злоумышленника:

По типу злоумышленники делятся на внутренних и внешних.

К внутренним злоумышленникам относятся сотрудники предприятия. Причем должность сотрудника не имеет принципиального значения. Особое внимание следует обращать на вновь принимаемых сотрудников. Известны случаи внедрения сотрудников, работающих на конкурентов.

Группу внешних нарушителей могут составлять (классификация открытая):

- клиенты;
- приглашенные посетители;
- представители конкурирующих организаций;
- сотрудники органов ведомственного надзора и управления;
- нарушители пропускного режима;
- наблюдатели за пределами охраняемой территории;
- и т.д.

Типы злоумышленников могут сильно отличаться, варьироваться по составу, возможностям и преследуемым целям. От одиночного злоумышленника, действующего удаленно и скрытно, до хорошо вооруженной и оснащенной силовой группы, действующей молниеносно и напролом. Нельзя не учитывать возможности сговора между злоумышленниками, относящимися к различным типам, а также подкупа и реализации других методов воздействия.

2. Цели, преследуемые злоумышленником

Вряд ли злоумышленник будет предпринимать действия просто так. Если ему нужна информация, значит она представляет для него интерес, следовательно, получение интересующей ценной информации будет для злоумышленника целью. Среди наиболее распространенных целей, которые может преследовать злоумышленник, можно выделить следующие (классификация открытая):

- любопытство;
- вандализм;
- месть;
- финансовая выгода;
- конкурентная выгода;
- сбор информации;
- военная или политическая выгода;
- и т.д.

3. Мотивы действий злоумышленника

Среди мотивов, побуждающих сотрудников предприятия к неправомерным действиям, можно выделить следующие (классификация открытая):

- Безответственность;
- Ошибки пользователей;
- Демонстрация своего превосходства (самоутверждение);
- "Борьба с системой";

- Корыстные интересы пользователей;
- Недостатки используемых информационных технологий;
- и т.д.

Мотивы действий внешних злоумышленников различны, в зависимости целей и типа злоумышленника. К наиболее распространенными причинами, которые побуждают внешних злоумышленников к действиям, можно отнести (классификация открытая):

- Конкурентная борьба.;
- Личное обогащение;
- Месть кому-то из сотрудников или руководителю;
- Вымогательство;
- Шантаж;
- Демонстрация своего превосходства (самоутверждение);
- и т.д.

У внутреннего злоумышленника, особенно если его действия сознательны, а не являются ошибкой, причин может быть больше, чем у внешнего: от банальной обиды до материальной выгоды, в случае подкупа со стороны конкурентов. Возможностей тоже больше: он может иметь доступ к сведениям на предприятии, в том числе и к конфиденциальной или секретной информации, причем на законных основаниях.

4. Применяемые методы и средства

И внутренним и внешним злоумышленникам приходится применять различные методы и средства, чтобы «добыть» ценную информацию. Основными методами и средствами, применяемыми злоумышленниками являются (классификация открытая):

- сбор информации и данных;
- пассивные средства перехвата;

- использование средств, входящих в информационную систему или систему ее защиты, и их недостатков;
- активное отслеживание модификаций существующих средств обработки информации, подключение новых средств, использование специализированных утилит, внедрение программных закладок и "черных ходов" в систему, подключение к каналам передачи данных;
- и т.д.

5. Время информационного воздействия

Злоумышленник прежде, чем предпринимать действия должен точно знать, где находится защищаемая информация, как обеспечивается ее защита и т.д. Получение этих сведений может занять определенное время. Время воздействия злоумышленника может быть:

- краткосрочным;
- периодическим;
- постоянным.

6. Предполагаемое месторасположение злоумышленника во время реализации атаки

От расположения злоумышленника во время реализации атаки зависят вероятные информационные потери. Если злоумышленнику придется преодолеть достаточно преград для получения доступа к информации, то вероятность, что служба безопасности успеет среагировать на проникновение выше, чем если злоумышленник находится недалеко от нее. Во время реализации атаки злоумышленник может находится (классификация открытая):

- удаленно с использованием перехвата информации, передающейся по каналам передачи данных, или без ее использования;
- на охраняемой территории;
- непосредственно рядом с объектом защиты (угрозы);
- и т.д.

В качестве варианта методики создания модели злоумышленника можно предложить применение методов типа сценарий. Это позволит составить картину как будет действовать злоумышленник (один или их будет группа), какие цели он преследует (мотивы проникновения), какие средства для проникновения будет использовать (сговор с сотрудниками, физическое проникновение и т. д.) и т. д.

Стоит помнить, что создание модели злоумышленника или определения значений параметров в большей мере субъективно. Проект КСЗИ в значительной степени зависит от адекватности модели злоумышленника. Таким образом, правильно разработанная модель злоумышленника является гарантией построения адекватной защиты [10].

3.2.5. Уязвимости

Разрабатывая КСЗИ, следует помнить, что в большинстве случаев реализация угрозы будет осуществлена через самое слабое место на предприятии.

Уязвимость – «окно» в системе безопасности предприятия, через которую возможна реализация угрозы. *Уязвимость защищаемой информации* заключается в возможности ее «заимствования» без нарушения физической целостности носителя [8].

Анализ уязвимостей объекта проводится с целью определения возможных последствий воздействия злоумышленника на элементы объекта, оценки показателей уязвимости объекта, выявления слабых мест и недостатков существующей системы охраны или рассматриваемых проектных вариантов системы, а в итоге - выбора наилучшего варианта системы охраны для конкретного объекта [11].

Уязвимости обуславливают появления канала реализации угроз. Реализация угрозы злоумышленником возможна только при условии существования канала её реализации.

Канал реализации угрозы – последовательность уязвимостей, способных «превратить» фактор, воздействующий на информацию, в действительную угрозу.

Рассмотрим для примера каналы реализации угроз, которые могут существовать для угрозы «утечка защищаемой информации». В зависимости от используемых злоумышленником сил и средств для получения несанкционированного доступа к носителям защищаемой информации различают каналы:

- агентурные;
- технические;
- легальные;
- иные.

Агентурные каналы утечки информации – это использование злоумышленником тайных агентов для получения несанкционированного доступа к носителям защищаемой информации.

Технические каналы утечки информации – совокупность технических средств разведки; демаскирующих признаков объекта защиты; сигналов, несущих информацию об этих признаках.

Легальные каналы утечки информации – это использование злоумышленником открытых источников информации (литературы, периодических изданий и т. п.), выведывание под благовидным предлогом информации у лиц, располагающих интересующей злоумышленника информацией и других возможностей.

Иные каналы утечки информации – выдача злоумышленнику добровольно защищаемой информации лицами, имеющими доступ к такой информации по работе, экспортные поставки секретной продукции за рубеж и т. п.

Технические каналы утечки информации

Самыми распространенными являются технические каналы утечки информации. Технические средства по добыче и съему информации порой использо-

вать злоумышленнику выгоднее, чем искать непорядочного сотрудника или внедрять в организацию своего агента, особенно, если его интересует конкретная информация.

Рассматриваемые каналы утечки информации или каналы несанкционированного доступа к информации (НСД) отличаются физическими явлениями, в силу которых информационные сигналы попадают в среду их распространения. Они из этой среды перехватываются и по этим сигналам восстанавливается информация: обрабатываемая, копируемая, отображаемая, передаваемая и т. п. Другими словами, технический канал утечки информации – это физический путь от источника информации к злоумышленнику, посредством которого может быть осуществлен несанкционированный доступ к защищаемой информации.

Технические каналы утечки информации можно разделить (рис. 3.4.1.1):

- на визуально-оптические;
- на акустические;
- на электромагнитные;
- на материально-вещественные.

Визуально-оптические каналы утечки информации классифицируют по следующим критериям:

- по природе образования (за счет отражения энергии или собственного излучения);
- по диапазону излучения (видимая область, ИК-область, УФ-область);
- по среде распространения (свободное пространство, направляющие линии передачи).

Акустические каналы утечки информации образуются:

– за счет распространения акустических (механических) колебаний в свободном воздушном пространстве (переговоры на открытом пространстве; открытые окна, двери, форточки; вентиляционные каналы);
– за счет воздействия звуковых колебаний на элементы и конструкции зданий, которые вызывают их вибрации (стены, потолки, полы, окна, двери, короба вентиляционных систем, трубы водоснабжения, отопления, кондиционирования и др.);
– за счет воздействия звуковых колебаний на технические средства обработки информации (микрофонный эффект, акустическая модуляция волоконно-оптических линий передачи информации).

Электромагнитные каналы утечки информации классифицируются по следующим критериям:

– по природе образования (акусто-преобразовательные, электромагнитные излучения, паразитные связи и наводки);
– по диапазону излучения (сверхдлинные волны, длинные волны, средние волны, короткие волны, ультра-короткие волны и другие более высокие диапазоны частот);
– по среде распространения (безвоздушное и воздушное пространства, земная и водная среды, направляющие системы).

М*атериально-вещественные* каналы утечки информации классифицируются по следующим критериям:

– физическому состоянию (твердые массы, жидкости, газообразные вещества);
– по физической природе (химические, биологические, радиоактивные);
– по среде распространения (в земле, в воде, в воздухе).

Основные виды технических каналов утечки информации можно классифицировать двумя группами.

Первая группа – это технические каналы НСД на базе методов и средств пассивного перехвата:

- за счет информативных побочных электромагнитных излучений и наводок;
- за счет электроакустических преобразований;
- с использованием узконаправленных специальных микрофонов;
- с использованием аппаратуры фотографирования;
- путем прямой регистрации информационных сигналов.

Вторая группа – это технические каналы НСД на базе методов и средств активного перехвата:

- с использованием технических закладных устройств;
- с использованием лазерных подслушивающих устройств;
- путем прямой регистрации информационных сигналов с последующей передачей по радиоканалу;
- путем передачи низкочастотных и высокочастотных сигналов на технические средства (за счет навязывания).

Обнаружение и распознавание технических каналов утечки информации производится по их демаскирующим признакам. В качестве достаточно общих признаков (уязвимостей) каналов утечки информации можно привести в таблице 3.2.5.1:

Таблица 3.2.5.1 Признаки каналов утечки информации

Вид канала	***Уязвимости***
Оптический	Просматриваемость помещений из окон противоположных домов. Близость к окнам деревьев. Отсутствие на окнах занавесок, штор, жалюзей. Просматриваемость содержания документов на столах со

	сторон окон, шкафов в помещении. Просматриваемость содержания плакатов на стенах помещения для совещания из окон и дверей. Малое расстояние между столами сотрудников в помещении. Просматриваемость экранов мониторов ПЭВМ на столах сотрудников со стороны окон, дверей или других сотрудников. Складирование продукции во дворе без навесов. Малая высота забора и дырки в нем.
Электромагнитный	Наличие в помещении электронных средств, ПЭВМ, ТА городской и внутренней АТС, громкоговорителей трансляционной сети и других предметов. Близость к жилым домам и зданиям иных организаций. Использование в помещении средств связи. Параллельная прокладка кабелей в одном жгуте при разводке их внутри здания на территории предприятия. Отсутствие заземления радио- и электрических приборов. Длительная и частая парковка возле предприятия чужих автомобилей, в особенности с сидящими в машине людьми.
Акустический	Малая толщина дверей и стен помещения. Наличие в помещении открытых вентиляционных отврстий. Отсутствие экранов на отопительных батареях. Близость окон к улице и ее домам. Появление возле предприятия людей с достаточно большими сумками, длинными и толстыми зонтами. Частая и продолжительная парковка возле предприятия чужим автомобилей.
Материально-вещественный	Отсутствие закрытых и опечатанных ящиков для бумаги и твердых отходов с демаскирующими веществами. Применение радиоактивных веществ. Неконтролируемый выброс газов с демаскирующими веществами, слив в водоемы и вывоз на свалку твердых отходов. Запись сотрудниками защищаемой информации на неучтенных листах.

Приведенные индикаторы являются лишь ориентирами при обнаружении потенциальных каналов утечки информации. В конкретных условиях их состав существенно больше.

3.2.6. Информационные риски

Риск – возможное проявление обстоятельств, обуславливающих нанесение ущерба от реализации злоумышленником угрозы защищаемой информации.

Риск важное понятие в процессе управления предприятием, принятии решений или эффективной защиты информации. Зная качественный показатель риска для каждой из угроз, можно при реализации системы защиты, используя различные методы и средства, снизить показатель риска до минимума.

Для управления рисками требуется идентифицировать возможные опасности (угрозы), угрожающие объекту защиты и среде его распространения. Таковыми могут являться, например, наводнение, отключение электропитания или атаки злоумышленников с последствиями разной степени тяжести. При разработке рисков рекомендуется учесть все риски, однако оценивать лишь те, реализация которых возможна исходя из принятой модели злоумышленника. Таким образом, после идентификации реальных угроз, угрозу следует соотнести с моделью злоумышленника с целью определения соответствующей категории злоумышленника и последующей оценки вероятности реализации данной угрозы. Например, если модель злоумышленника не описывает категорию удаленных пользователей (в компании не предусмотрен удаленный доступ), то вероятность утечки информации в результате доступа к ней извне ничтожно мала, и ею можно пренебречь при расчете рисков.

Формула, чаще всего используемая при расчете рисков, представляет собой произведение двух параметров:

- *ценность ресурса*. Указанная величина характеризует ценность ресурса (см. методику «Категорирование и дифференцированный подход к защите информации»);
- *вероятность реализации угрозы*. Этот параметр показывает, в какой степени тот или иной информационный ресурс уязвим по отношению к рассматриваемой угрозе.

Как видно, значение данных параметров определяется эмпирически на основе мнения эксперта (студента). Это связано с тем, что количественная оценка вероятности реализации угрозы затруднена ввиду относительной новизны информационных технологий и, как следствие, отсутствия достаточного количества статистических данных.

3.2.7. Методика выполнения раздела «Анализ объекта защиты»

3.2.7.1. Общие сведения

Согласно вышесказанному, объектом защиты, рассматриваемому в рамках данного методики, является информация, её носители и средства обработки, в том числе и персонал.

Выполнение раздела «Анализ объекта защиты» проводится в два этапа:

- Этап 1 – Описание информационных ресурсов;
- Этап 2 – Расчет информационных рисков.

Для простоты выполнения каждый из этапов разбит на несколько работ.

3.2.7.2. Этап №1.1: Определение сведений, возможно подлежащих защите

Задача данного этапа:	Выявить все информационные ресурсы, которые тем или иным образом обрабатываются (могут быть обработаны) в рассматриваемом выделенном помещении.
Входные данные	Материалы, представленные в ТЗ.
Способ выполнения:	Выявление обрабатываемых информационных ресурсов при выполнении работ по реальным объектам заключается в проведении собеседования с сотрудниками организации, обследовании средств обработки информации с целью выявления, классификации и описания обрабатываемой информации.

В случае если студент выполняет курсовую работу, по варианту, предложенному в данном методическом пособии, то он должен самостоятельно, основываясь на исходных данных, разработать перечень обрабатываемой в выделенном помещении информации.

Критерии выполнения

Результатом выполнения этапа должен явиться перечень обрабатываемой в выделенном помещении информации с необходимыми комментариями и справочными сведениями.

Какие именно сведения и комментарии следует приложить к перечню, какой формы следует сделать перечень – определяется студентом самостоятельно и является частью его исследовательской работы по данному курсовому проекту (работе).

Помощь

Иногда целесообразно объединить выполнение этапа 1.1 с этапами 1.2 – 1.3. Для этого рекомендуется применять методики моделирования бизнес-процессов, таких как IDEF0, IDEF3, IDEF5, ARIS, UML и им подобные. Допускается применять самостоятельно разработанные методики.

При опросе сотрудников реальных предприятий рекомендуется применять методологию, представленную в методике OCTAVE.

3.2.7.3. Этап №1.2: Описание защищаемой информации

Задача данного этапа

На основе перечня сведений, разработанном в ходе выполнения этапа 1.1, а так же сведений, представленных в ТЗ ответить на вопросы:

– Что/Кто является источниками этой информации?

– Что/Кто является носителями этой информации?

– Где в выделенном помещении находится информация?

– Кто имеет доступ к информации?

Входные данные Материалы, представленные в ТЗ, перечень сведений, обрабатываемых в выделенном помещении.

Способ выполнения: Ответ на представленные выше вопросы производится, так же как и входе выполнения этапа 1.1 с помощью опроса сотрудников и анализа средств обработки информации.

Критерии выполнения Результатом выполнения этапа должен явиться структурированный массив информации, максимально полно отвечающий на поставленные вопросы.

Полнота представления информации не должна быть использована в ущерб наглядности представления и удобства пользования собранной информацией.

Выбор формы представления и информационная наполненность определяется студентом самостоятельно и является частью его исследовательской работы по данному курсовому проекту (работе).

Помощь Иногда целесообразно объединить выполнение этапа 1.2 с этапами 1.1, 1.3. Для этого рекомендуется применять методики моделирования бизнес-процессов, таких как IDEF0, IDEF3, IDEF5, ARIS, UML и им по-

добные. Допускается применять самостоятельно разработанные методики.

Представление массива информации в виде сводной таблицы целесообразно лишь для перечня с малым количеством пунктов.

При опросе сотрудников реальных предприятий рекомендуется применять методологию, представленную в методике OCTAVE.

3.2.7.4. Этап №1.3: Описание информационных процессов

Задача данного этапа На основе данных, подготовленных в ходе выполнения этапов 1.1 и 1.2, а так же сведений, представленных в ТЗ ответить на вопросы:

- В каких информационных процессах используется информация?
- Какие действия производятся над информацией?
- Какую роль играют рассматриваемые информационные процессы в функционировании организации в целом?

Входные данные Материалы, представленные в ТЗ, данные, подготовленные в ходе выполнения этапов 1.1 и 1.2.

Способ выполнения: Ответ на представленные выше вопросы производится, так же как и входе выполнения этапа 1.1 с помощью опроса сотрудников и анализа средств обработки информации.

Критерии выполнения Результатом выполнения этапа должен явиться структурированный массив информации, максимально полно отвечающий на поставленные вопросы.

Полнота представления информации не должна быть использована в ущерб наглядности представления и удобства пользования собранной информацией.

Выбор формы представления и информационная наполненность определяется студентом самостоятельно и является частью его исследовательской работы по данному курсовому проекту (работе).

Помощь Иногда целесообразно объединить выполнение этапа 1.3 с этапами 1.1, 1.2. Для этого рекомендуется применять методики моделирования бизнес-процессов, таких как IDEF0, IDEF3, IDEF5, ARIS, UML и им подобные. Допускается применять самостоятельно разработанные методики.

При опросе сотрудников реальных предприятий рекомендуется применять методологию, представленную в методике OCTAVE.

3.2.7.5. Этап №1.4: Категорирование информации

Задача данного этапа На основе данных, подготовленных в ходе выполнения этапов 1.1 – 1.3 определить ценность рассматриваемой информации (информационных ресурсов) для организации.

Входные данные Данные, подготовленные в ходе выполнения этапов 1.1 – 1.3.

Способ выполнения: Первое, что должен выполнить студент, это определиться с применяемой им методикой ранжирования информации (информационных ресурсов) по степени важности для их собственника (владельца и т.д.).

Второе, на основе опроса сотрудников организации, анализа средств обработки информации провести оценку ценности рассматриваемой информации (информационных ресурсов) в соответствии с выбранной методикой.

Критерии выполнения Результатом выполнения этапа должен явиться некий перечень информации (информационных ресурсов) с указанием их категории (ценности).

Полнота представления информации не должна быть использована в ущерб наглядности представления и удобства пользования собранной информацией.

Выбор формы представления и информационная наполненность определяется студентом самостоятельно и является частью его исследовательской работы по данному курсовому проекту (работе).

Помощь Применение методик категорирования помогает реализовать дискретный подход к защите информации, предполагающий, что к информации определенной категории (ценности) следует предъявлять определённый набор требований. Студент не ограничен в выборе применяемой методики. Возможно применения собственных методик. Так или иначе, все действия должны быть подробно описаны и обоснованы.

Поэтому, при выборе методики категорирования (определения ценности) следует учитывать выполнения этапа.

3.2.7.6. Этап №2.1: Описание факторов, воздействующих на информацию

Задача данного этапа — На основе данных, подготовленных в ходе выполнения этапов 1, сведений, представленных в ТЗ, и ГОСТ 51583-2000 выявить всё множество факторов, которые могут воздействовать на информацию (информационные ресурсы) в рассматриваемом случае.

Входные данные — Данные, подготовленные в ходе выполнения этапа 1, ГОСТ 51583-2000, сведения, представленные в ТЗ.

Способ выполнения: — Допускается расширение (детализации) перечня факторов, представленных в ГОСТ 51583-2000.

Критерии выполнения — Результатом выполнения этапа должен явиться перечень факторов, воздействующих на информацию, обрабатываемую в рассматриваемом выделенном помещении.

Помощь — В зависимости от конкретной ситуации целесообразно составлять либо общий перечень факторов, либо делать свой перечень для каждого информационного ресурса (группы информационных ресурсов).

3.2.7.7. Этап №2.2: Разработка модели злоумышленника

Задача данного этапа — На основе подготовленных ранее описаний обрабатываемой в выделенном помещении информации, раздела 4.2.4 и РД «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» от от 30

марта 1992 года разработать модель вероятного злоумышленника.

Входные данные — Данные, подготовленные в ходе выполнения этапа 1, раздел 4.2.4, РД.

Способ выполнения: — Разработка модели злоумышленника производится в соответствии с концепцией, представленной в разделе 4.2.4. Студент вправе применять иную концепцию, либо модифицировать имеющуюся. Единственное требование при этом – аргументированность действий и доказуемость результатов.

Критерии выполнения — Результатом выполнения этапа должна явиться максимально адекватная существующей действительности модель вероятного злоумышленника максимально.

Форма представления разработанной модели не регламентируется. Единственное требование, наглядность и достаточная полнота представляемых сведений.

Помощь — Зачастую разработать полную, детализированную модель вероятного злоумышленника не представляется возможным. В таких случаях следует ограничиться сбором данных в объеме, позволяющем выполнять следующие этапы. В ситуациях, когда и такую информацию собрать не удаётся, следует вместо недостающих данных ввести предположения, а дальнейшем ссылаясь на это.

3.2.7.8. Этап №2.3: Описание уязвимостей

Задача данного этапа	На основе анализа данных, представленных в ТЗ и анализа реального состояния дел выявить максимально полный перечень уязвимостей, которыми обладает выделенное помещение и средства обработки информации, находящиеся в нём.
Входные данные	Данные, представленные в ТЗ, анализ выделенного помещения, справочники уязвимостей конкретных информационных систем.
Способ выполнения:	На основе анализа исходных данных, реального состояния дел и справочников возможных уязвимостей, определяются уязвимости, которыми обладает выделенное помещение и средства обработки информации. В случае, когда студент выполняет курсовой проект (работу) по варианту, предложенному данным методическим пособием, и в исходных данных не содержится сведений, необходимых для более точного выявления возможных уязвимостей, он должен в ходе выполнения данного этапа самостоятельно добавить недостающие сведения.
Критерии выполнения	Результатом выполнения этапа должна явиться максимально полный перечень уязвимостей рассматриваемого выделенного помещения и средств обработки информации.
Помощь	При описании уязвимостей типовых систем допускает приводить ссылку на их описания. При описании уязвимостей целесообразно отдельно проводить исследования по направлениям *Организа-*

ционная, *Техническая* и *Программно-техническая* защита информации.

3.2.7.9. Этап №2.4: Описание угроз

Задача данного этапа — На основе сведений, полученных в ходе выполнения этапов 1, 2.1 – 2.3 выявить реальные угрозы информации (информационным ресурсам), обрабатываемым в рассматриваемом выделенном помещении, описать возможные каналы реализации каждой угрозы и предположить последствия их реализации.

Входные данные — Сведения, полученных в ходе выполнения этапов 1, 2.1 – 2.3.

Способ выполнения: — При выполнении данного раздела, студенту следует проработать последовательность *Информационный ресурс – Информационный процесс – Воздействующий фактор – Злоумышленник – Уязвимости*.

Критерии выполнения — Результатом выполнения этапа должен явиться сводный массив данных об угрозах, каналах и последствиях их реализации, оценены вероятности реализации угроз. Вероятности реализации угроз должны быть ранжированы.

Помощь — При проработке цепочки *Информационный ресурс – Информационный процесс – Воздействующий фактор – Злоумышленник* удобно использовать древовидное представление сведений.

3.2.7.10. Этап №2.5: Расчёт информационных рисков

Задача данного этапа — На основе полученных ранее сведений, для каждой из угроз для каждого информационного ресурса опреде-

	лить информационные риски. Проранжровать полученные значения по трехбалльной шкале (Высокие, Средние, Низкие).
Входные данные	Сведения, полученных в ходе выполнения этапов 1, 2.1 – 2.4.
Способ выполнения:	Подсчет величины информационных рисков для каждой из угроз для каждого информационного ресурса приводится в соответствии с методикой, предложенной в разделе 4.2.6. Студент может предложить свой вариант методики оценки. Единственное требование – аргументированность действие и доказуемость результатов.
Критерии выполнения	Результатом выполнения этапа является проранжированная оценка информационных рисков рассматриваемым информационным ресурсам.
Помощь	Для оценки информационных рисков рекомендуется применять механизмы нечеткой логики.

3.3. Формирование требований к создаваемой КСЗИ

3.3.1. Общие сведения

Имея после выполнения этапа «Анализ объекта защиты» максимально полную картину об объекте защиты и информационных рисках, которым он подвигается исследователь (студент) имеет возможность сформулировать то, что он хочет получить от КСЗИ, т.е. сформулировать набор требований к КСЗИ.

Согласно ГОСТ 34.602-89 и с учетом особенностей учебного процесса при подготовке ТЗ на любую КСЗИ должны быть сформулированы следующие наборы требований:

- требования к структуре и функционированию КСЗИ;
- требования к численности и квалификации обслуживающего персонала и пользователей КСЗИ;
- показатели надежности функционирования КСЗИ;
- показатели эффективности функционирования КСЗИ;
- требования к безопасности КСЗИ;
- требования к информационной безопасности КСЗИ (НСД, сохранность при чрезвычайных ситуациях);
- требования к защите от внешних воздействий компонент и КСЗИ в целом;
- дополнительные требования.

Как видно из представленного списка студент не ограничен в расширении, дополнении и уточнении набора требований, предъявляемых КСЗИ. В случае, когда сформулировать требование в явном виде не представляется возможным, допускается пропустить описание такого требования, однако необходимо обосновать принятие данного решения.

3.3.2. Этап 3: Формулирование требований к КСЗИ

Задача данного этапа	На основе полученных ранее сведений, сформулировать набор требований к КСЗИ, представленных в разделе 4.3.1.
Входные данные	Сведения, полученные в ходе выполнения раздела «Анализ объекта защиты»
Способ выполнения:	Формулирование требований к КСЗИ в рамках выполнения данного курсового проекта (работы) требует от студента поставить себя на место сотрудников организации, работающей в рассматриваемом выделенном помещении. Студент должен иметь представ-

ления о реальной работе организация для грамотного и полного формулирования требований.

Критерии выполнения Результатом выполнения этапа является максимально полное описание каждого из требований и, в некоторых случаях, доказательства почему то или иное требование не представляется возможным сформулировать.

Помощь При выполнении данного раздела студенту рекомендуется обращаться за консультациями к людям, уже имеющих опыт работ в сфере близкой к сфере работы организации.

3.4. Разработка концепции КСЗИ

3.4.1. Общие сведения

Концепция КСЗИ – система взглядов, выражающая определенный способ видения ("точку зрения"), понимания, трактовки КСЗИ.

Концепция КСЗИ – предложение использование некоторого набора мер по защите информации, предложения по составу этих мероприятий.

Разработка комплексной системы защиты информации процесс творческий и в большей степени зависит от опыта и взглядов разработчика системы информационной безопасности, т. е. студента выполняющего работу. Как результат – множество взглядов на решение одной и той же проблемы.

Основная задача данного радела – рассмотреть несколько наиболее удачных концепций КСЗИ и выбрать наиболее соответствующую разработанным в ходе выполнения предыдущего раздела требованиям к КСЗИ.

3.4.2. Основные принципы защиты информации

Построение системы защиты полезно проводить с принципами, на которые необходимо опираться, чтобы система защиты была отлаженной и эффективной.

Под принципами защиты информации понимаются основополагающие идеи, важнейшие рекомендации по организации и осуществлению этой деятельности на различных этапах решения задач сохранения ценных сведений.

Наиболее распространенными принципами являются:

- *Адекватность* (разумная достаточность). Совокупная стоимость защиты (временные, людские и денежные ресурсы) должна быть ниже стоимости защищаемой информации. Если, например, оборот компании составляет 10 тыс. рублей в месяц, вряд есть смысл развертывать систему защиты на миллион. То же самое и наоборот, если доходы компании достаточно большие, то экономия на защите информации не даст необходимого эффекта, не все каналы утечки будут перекрыты, а следовательно, злоумышленник сможет ими воспользоваться для реализации атаки;
- *Системность*. Важность этого принципа состоит в том, что система защиты информации должна строиться не абстрактно (защита от всего), а на основе анализа угроз, средств защиты от этих угроз, поиска оптимального набора этих средств и построения системы;
- *Прозрачность* для сотрудников. Введение механизмов безопасности по ограничению доступа к защищаемой информации может приводить к усложнению действий сотрудников при выполнении ими своей работы. При создании системы защиты стоит учитывать, что никакой механизм не должен требовать невыполнимых действий от сотрудников предприятия или на слишком долгое время затягивать процедуру доступа к информации;
- *Равностойкость* звеньев системы защиты. Звенья - это элементы защиты, преодоление любого из которых означает преодоление всей за-

щиты. Нельзя слабость одних звеньев компенсировать усилением других. В любом случае, прочность защиты определяется прочностью самого слабого звена. И если нелояльный сотрудник готов за определенные услуги сотрудничать со злоумышленником, то вряд злоумышленник ли будет выстраивать сложную атаку для достижения цели.

– *Непрерывность*. Почти тоже самое, что и равностойкость, только во временной области. Защищаемую информацию и ее носителей необходимо защищать в любой момент времени. Нельзя, например, решить по пятницам делать резервное копирование информации, а в последнюю пятницу месяца устроить «санитарный день». Может случиться, что именно в тот момент, когда меры по защите информации будут ослаблены, злоумышленник может реализовать угрозу. Временный провал в защите информации, делает ее бессмысленной и неэффективной;
– *Многоуровневость*. Защита должна строиться в несколько уровней, которые должен преодолевать как злоумышленник, так и сотрудники предприятия? Потому что всегда существует вероятность того, что какой-то уровень может быть преодолен либо в силу непредвиденных случайностей, либо с ненулевой вероятностью. И, если один уровень гарантирует защиту в 90%, то три уровня (ни в коем случае не повторяющих друг друга) – 99,9% [13].

Принципы реализации КСЗИ можно разделить на три группы:

– правовые;
– организационные;
– принципы, используемые при защите информации от технических средств разведки и в средствах вычислительной техники.

Основными правовыми принципами защиты информации являются следующие:

- *принцип законности* – выражается прежде всего в том, что необходимо нормативно-правовое регулирование этой области общественных отношений. Законодательно должны быть обозначены права различных субъектов в области защиты информации; определено, что является секретными и конфиденциальными сведениями; установлена уголовная, административная, материальная, моральная ответственность за незаконное покушение на защищаемую информацию и последствия для собственника;
- *принцип приоритета международного права над внутригосударственным*.
- *принцип собственности и экономической целесообразности*. Этот принцип дает право принимать меры к защите информации, а также оценивать ее потребительские свойства [4].

Организационные принципы защиты информации заключаются в следующем:

- научный подход к организации защиты информации, в основе которого лежит системный подход. Системный подход к организации защиты информации позволяет создать органически взаимосвязанную совокупность сил, средств и специальных методов по оптимальному ограничению сферы обращения засекреченной информации, предупреждение ее утечки;
- максимальное ограничение числа лиц, допускаемых к защищаемой информации, т. к. сохранность засекреченной информации находиться в зависимости от количества лиц, допущенных к обращению с нею;
- дробление технологической цепочки производства на отдельные операции, знание одной из которых не дает возможность восстановить всю технологию;
- персональная ответственность за сохранность доверенных секретов;

- единство в решении производственных, коммерческих, финансовых, кадровых и режимных вопросов;
- непрерывность защиты информации предполагает, что защита конфиденциальной информации должна начинаться с момента ее появления на всех этапах ее обработки, передачи, использования и хранения, вплоть до этапа ее уничтожения.

Принципы защиты информации, используемые при организации противодействия техническим средствам разведки (ТСР):

- *активность защиты информации* - выражается в целенаправленном навязывании технической разведке ложного представления об объекте его разведывательных устремлений, в соответствии с замыслом защиты;
- *убедительность защиты информации* - состоит в оправданности замысла защиты условиям обстановки в соответствии с характером защищаемого объекта или свойствам окружающей среды, в применении технических решений защиты, соответствующих климатическим, сезонным и другим условиям;
- *непрерывность защиты информации* предполагает организацию защиты объекта на всех стадиях организации его жизненного цикла;
- *разнообразие защиты информации* – предусматривает исключение шаблона, повторяемости в выборе объекта прикрытия и путей реализации смысла защиты, в том числе с применением типовых решений.

Из-за повсеместного использования компьютеров на предприятиях стоит привести принципы защиты информации, используемые в системах вычислительной техники:

- введение избыточности элементов системы;
- резервирование элементов;
- защитные преобразования данных;

– контроль состояния элементов системы, их работоспособности и правильности функционирования [13].

3.4.3. Методы управления рисками

При проработке раздела «Анализ объекта защиты» упоминалась необходимость ранжирования степени важности риска. В зависимости от важности, риск может быть:

– *Принят* – руководство предприятия согласно на риск и связанные с ним потери, поэтому работа продолжается в обычном режиме;
– *Снижен* – с целью уменьшения величины риска будут приняты определенные меры;
– *Передан* – компенсацию потенциального ущерба возложат на страховую компанию, либо риск трансформируют в другой риск с более низким значением путем внедрения специальных механизмов.

В литературе так же встречается описание еще одного способа управления – "*Упразднение*". Он подразумевает принятие мер по ликвидации источника риска. Например, удаление из системы функций, порождающих риск, либо выведение части системы из эксплуатации. При низких значениях риска данный метод трансформируется в метод снижения риска.

После ранжирования рисков определяются требующие первоочередного внимания; основным методом управления такими рисками является снижение, реже — передача. Риски среднего ранга могут передаваться или снижаться наравне с высокими рисками. Риски низшего ранга, как правило, принимаются и исключаются из дальнейшего анализа.

Таким образом, управление рисками, в данном контексте, сводится к снижению величин высоких и средних рисков до характерных для низких рисков значений, при которых возможно их принятие. Снижение величины риска достигается за счет уменьшения вероятности реализации угрозы [14].

3.4.4. Методы защиты информации

При реализации системы защиты необходимо опираться не только на принципы и методы управления рисками, но и определиться с методами защиты. Невозможно найти один способ (метод) защиты информации от всех угроз. В зависимости от ситуации (угрозы) действия по защите будут разными, следовательно, и методы должны быть тоже разными.

Метод – в самом общем значении это способ достижения цели, определенным образом упорядоченная деятельность.

В области защиты информации разработано достаточное количество методов, среди которых можно выбрать наиболее подходящий для конкретной ситуации при разработке системы защиты. Основные методы, используемые в защите информации:

- скрытие;
- ранжирование;
- дезинформация;
- дробление;
- страхование;
- морально-нравственные;
- учет;
- кодирование;
- шифрование [13].

Скрытие – как метод защиты информации является в основе своей реализации на практике одного из основных организационных принципов защиты информации - максимального ограничения числа лиц, допускаемых к сведениям. Реализация этого метода достигается обычно путем:

- засекречивание информации, то есть отнесение ее к секретной или конфиденциальной информации различной степени секретности и ог-

раничение в связи с этим доступа к этой информации в зависимости от ее важности для собственника, что проявляется в поставляемом на носителе грифе секретности;

– устранения или ослабления технических демаскирующих признаков объектов защиты и технических каналов утечки сведений о них.

Скрытие – один из наиболее общих и широко применяемых методов защиты информации.

Ранжирование как метод защиты включает, во-первых, деление засекречиваемой информации по степени секретности, и, во-вторых, регламентацию допуска и разграничение доступа к защищаемой информации: предоставление индивидуальных прав отдельным пользователям на доступ к необходимой им конкретной информации и на выполнение отдельных операций. Разграничение доступа к информации может осуществляться по тематическому признаку или по признаку секретности информации.

Ранжирование как метод защиты информации является частным случаем метода скрытия: пользователь не допускается к информации, которая ему не нужна для выполнения его служебных функций, и тем самым эта информация скрывается от него и всех остальных (посторонних) лиц.

Дезинформация – один из методов защиты информации, заключающийся в распространении заведомо ложных сведений относительно истинного назначения каких-либо объектов и изделий, действительного состояния положения дел на предприятии и т.д.

Дезинформация обычно проводится путем распространения ложной информации по различным каналам, имитацией или искажением признаков и свойств отдельных элементов объектов защиты, создания ложных объектов, по внешнему виду или проявлениям похожих на интересующие соперника объекты, и др.

Дробление (расчленение) информации на части с таким условием, что знание какой-то одной части информации не позволяет восстановить всю картину, всю технологию в целом.

Страхование – сущность данного метода сводится к тому, чтобы защитить права и интересы собственника информации или средства информации как от случайных угроз (кражи, стихийные бедствия), так и от преднамеренных угроз безопасности информации, а именно: защита информации о утечки, хищения, модификации (подделки), разрушения и др.

При страховании информации должно быть проведено аудиторское обследование и дано заключение о сведениях, которые предприятие будет защищать как коммерческую тайну и надежности средств защиты.

Морально-нравственные методы защиты информации можно отнести к группе тех методов, которые, играют очень важную роль в защите информации. Поскольку именно человек, сотрудник предприятия, допущенный к защищаемым сведениям и накапливающий в своей памяти колоссальные объемы информации, в том числе секретной или конфиденциальной, нередко становится источником утечки этой информации или по его вине злоумышленник получает возможность несанкционированного доступа к носителям защищаемой информации.

Данные методы защиты информации предполагают, прежде всего, воспитание сотрудника, допущенного к защищаемым сведениям, то есть проведение специальной работы, направленной на формирование у него системы определенных качеств, взглядов и убеждений (патриотизма, понимания важности и полезности защиты информации и для него лично), и обучение сотрудника, осведомленного в сведениях, составляющих тайну, правилам методам защиты информации, привитие ему навыков работы с носителями секретной или конфиденциальной информации.

Учет также один из важнейших методов защиты информации, обеспечивающий возможность получения в любое время данных о любом носителе защищаемой информации, о количестве и местонахождении всех носителей засекреченной информации, а также о всех пользователях этой информации. Без учета решать проблемы было бы невозможно, особенно когда количество носителей превысит какой-то минимальный объем.

3.4.5. Меры защиты информации

При разработке концепции КСЗИ в условиях выбранной политики управления информационными рисками и применяемыми методами защиты информации предполагается формирование нескольких наборов мер по защите информации с примерной оценкой их состава. Разработанные варианты концепции затем оцениваются экспертами по критериям эффективности и стоимости. На основании оценки принимается решение выбрать ту или иную концепцию.

Существует множество классификаций применяемых мер защиты. Так, стандарт ГОСТ 17799-2005 определяет 11 групп мер по защите информации, классификация по признаку «целевой канал утечки информации» приводит к появлению двух групп методов: «меры, направленные на противодействие агентурному каналу утечки информации» и «меры, направленные на противодействие техническим каналам утечки информации» (Приложение И).

3.4.6. Этап №4.1: Разработка нескольких вариантов концепции КСЗИ

Задача данного этапа	На основе анализа данных, подготовленных на предыдущих этапах разработать несколько (2-3) варианта концепции КСЗИ.
Входные данные	Данные, подготовленные на предыдущих этапах.
Способ выполнения:	На основе сведений об информационных рисках для каждого из информационных ресурсов, обрабатывае-

мых в выделенном помещении, выбирают конкретный метод управления рисками для каждого из ресурса.

Для каждого информационного ресурса выбирается предпочтительный метод защиты и делается предположение о возможном наборе мер для поддержки реализации метода.

Совокупность выбранных методов управления рисками, методов защиты информации и предполагаемых мер защиты составляет концепцию КСЗИ.

Студентом разрабатываются 2-3 варианта концепции КСЗИ.

Критерии выполнения Результатом выполнения этапа должен явиться набор концепция КСЗИ.

Помощь Выбор определённого метода управления рисками и метода защиты может быть упрощен, если поставить в соответствие конкретному значению набора критериев КЦД конкретный набор методов управления рисками и защиты.

3.4.7. Этап №4. 2: Выбор оптимальной концепции КСЗИ

Задача данного этапа Из подготовленного в результате выполнения предыдущего этапа набора концепций КСЗИ выбрать оптимальную концепцию.

Входные данные Набор концепций КСЗИ.

Способ выполнения: Оптимальная концепция КСЗИ выбирается из числа ранее разработанных концепций на основе оценки сочетания эффективность-стоимость.

Критерии выполнения	Результатом выполнения этапа должна явиться оптимальная концепция КСЗИ, выбор которой обоснован.
Помощь	Выбор оптимальной концепции КСЗИ может быть упрощен, если оценивать каждую концепцию КСЗИ с позиций нескольких критериев, важность каждого критерия при этом должен быть оценен отдельно.

3.5. Разработка проектного решение по КСЗИ

3.5.1. Общие сведения

Проектное решение КСЗИ является непосредственной реализацией выбранной концепции КСЗИ.

Разработка проекта КСЗИ ведется студентом на основании знаний, полученных в результате изучения данного и остальных учебных курсов. При необходимости студент может привлекать отечественные и зарубежные нормативные документы и методики, каталоги средств защиты информации и т.п. сведения.

3.5.2. Этап №5. 1: Разработка проектного решения

Задача данного этапа	На основе всех ранее собранных данных разрабатывается проектное решение по КСЗИ.
Входные данные	Данные, подготовленные на предыдущих этапах, отечественные и зарубежные нормативные документы, методики, каталоги средств защиты и т.п. сведения.
Способ выполнения:	На основе разработанной концепции КСЗИ производится разработка общих решений по КСЗИ в целом и ее частям, функционально структуре КСЗИ, по функциям персонала и организационной структуре, по

структуре технических средств и по программному обеспечению.

Критерии выполнения Разработанный проект КСЗИ должен максимально полно отвечать требованиям, сформулированным в ходе выполнения этапа №3, а так же целям выполнения данного курсовой работы (проекта).

Помощь Разработке проекта КСЗИ может значительно помочь анализ уже выполненных проектов КСЗИ по схожим проектам.

3.5.3. Этап №5. 2: Вывод по курсовому проекту (работе)

Задача данного этапа Подвести итог выполненной работе. Оценить достижение целей и задач, поставленных в ТЗ. Оценить текущую защищенность объектов защиты.

Входные данные Данные, подготовленные на предыдущих этапах.

Способ выполнения: Выводы являются кратким изложением работы, проделанной студентом в ходе выполнения курсового проекта (работы), отражением основных полученных результатов, описанием того, что было выполнения для достижения цели курсовой работы, а что не удалось.

Критерии выполнения В заключительной части курсового проекта (работы) должны присутствовать выводы как по отдельным частям работы, так и по всей работе в целом.

Помощь Подведение выводов по выполненному курсовому проекту (работе) значительно упростится, если в кон-

це выполнения каждого из этапов работы студент будет формулировать частные выводы, наиболее важные из которых зачем вынесет в заключительную часть работы.

4. Защита курсового проекта

Защита курсовой работы производится индивидуально до сдачи экзаменационной сессии. Защита курсового проекта (работы) производится перед научным руководителем и группой приглашенных преподавателей.

Условием получения оценки по курсовой работе является не только подготовка текста, но и устная защита. К защите допускается готовые работы - окончательный вариант, исправленный на основании замечаний руководителя

На защите курсовой работы обучаемый должен быть готов к краткому изложению основного содержания работы и ее результатов, к собеседованию по отдельным моментам работы, к ответу на любые вопросы как по данной теме, так и по всему курсу.

Для защиты студент готовит презентацию на 10-15 минут, в ходе которой должны быть представлены цель, гипотеза, основные рабочие интересные моменты, примеры, заключительные выводы. В целях повышения эффективности и степени усвоения возможно использование наглядного материала. Непосредственно во время защиты следует вести себя уверенно.

На защите обязательно присутствуют все студенты группы, в которой проходит защита, другие студенты – по желанию. Все участники имеют право задавать вопросы по содержанию работы. Ответы на вопросы должны быть четкими и уверенными.

По результатам презентации и защиты курсовой работы выставляется оценка. При неудовлетворительной оценке студент обязан повторно выполнить работу по новой теме или переработать прежнюю. Повторная защита работ должна завершиться до начала сессии. Студенты, не сдавшие и не защитившие в срок курсовую работу, к сессии не допускаются.