МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

Методические указания

по организации самостоятельной работы обучающихся
по дисциплине «Управление проектами по защите информации и экономика защиты информации»
для студентов направления подготовки /специальности
10.03.01 Информационная безопасность
шифр и наименование направления подготовки/ специальности

(ЭЛЕКТРОННЫЙ ДОКУМЕНТ)

ВВЕДЕНИЕ

Основной целью предприятий на современном этапе развития экономики России является создание, защита и поддержание своей информационной инфраструктуры на современном уровне. В соответствии с этой целью можно сформулировать и его задачи: организация эффективного функционирования предприятия за счет интеграции отдельных функций подразделений с помощью информационных технологий; повышение скорости обработки и предоставления информации, необходимой для принятия решения на всех уровнях управления; повышение качества получаемой информации (избавление от шумов) из микросреды; о положении на рынках, состоянии конкурентов, возможностях сбыта, и макросреды; о международном положении, изменении законодательства и т.д. .

Самостоятельная работа студента заключается в изучении лекционного материала, основной и дополнительной литературы по темам дисциплины «Управление проектами по защите информации и экономика защиты информации». В результате изучения студент должен знать основные положения и особенности экономики защиты информации, в частности: особенности развития рынка информации, правовые аспекты взаимодействия субъектов на рынке информации, состав интеллектуальной собственности предприятия и способы ее оценки, основные методики определения экономической эффективности и целесообразности организации мероприятий по защите информации. Методические указания к самостоятельной работе разработаны в соответствии с программой дисциплины "Управление проектами по защите информации и экономика защиты информации" и предназначены для студентов всех форм обучения по направлению подготовки10.03.01 Информационная безопасность

СОДЕРЖАНИЕ

Раздел 1. Роль информации в экономике

Тема1.Экономические проблемы информационных ресурсов.
Информатизация – объективная закономерность развития общества.
Мировой и внутригосударственный рынок информационных услуг. Новые носители информации.

Информация как товар характеризуется таким показателем как жизненный цикл. Жизненный цикл товара (ЖЦТ) представляет собой времяего существования на рынке. Фазы ЖЦТ обычно делят на внедрение (введение), рост, зрелость, насыщение и спад. Продолжительность жизненногоцикла в целом и его отдельных фаз зависит как от самого товара, так и отконкретного рынка. По общему признаку сырьевые товары имеют более длительный жизненный цикл, готовые изделия имеют более короткий
жизненный, а наиболее технически совершенные товары короткий (2-3 года). Указанные особенности относятся и к информации как товару, жизненный цикл которой может колебаться в широких пределах. Особенно,когда это относится к коммерческой информации, представляющей интерес для конкурирующей организации.

Информация (информационные ресурсы) характеризуются:
неисчерпаемостью - по мере развития общества и роста потребления его запасы не убывают, а растут;
сохраняемостью - при использовании не исчезает и даже может увеличиваться за счет трансформации полученных сообщений;
несамостоятельностью - проявляет свою "движущую силу" только в соединении с другими ресурсами (труд, техника, сырье, энергия).

На сегодня рынок информации в России многообразен и динамичен.Активно используя самые совершенные технологии, он расширяется засчет формирования новых общественных потребностей.

Информация как предмет труда – это первичные исходные данные,сведения в конкретной сфере деятельности и смежных с нею областях.

Информация как средство труда – это совокупность знаний, данныхи приемов, при помощи которых исходная информация (предмет труда)может быть наиболее эффективным образом обработана в целях получениязапланированного результата. Информация как средство труда должнаиметь форму, удобную и понятную специалисту в данной сфере деятельности.
Продукция индустрии информации в укрупненном виде может бытьподразделена на продукты (вычислительная техника, офисное оборудование, коммуникационное оборудование, программное обеспечение, информационный продукт) и услуги (техническое обслуживание, сопровождениепрограммного обеспечения, обучение и консультации, услуги связи, услуги по обработке данных).

Вопросы к теме
1.В чём заключается защита и поддержание информационной инфраструктуры на современном уровне.

2.Системы защиты информации.

3. В чём заключается информационное обслуживание.

4.В чём заключаются специфические особенности производства информации.
5.Жизненный цикл информации.

Тема 2.Информационная безопасность экономической системы предприятия.

Цена в условиях рыночной экономики является важнейшей экономической категорией и представляет собой денежную стоимость товара. Ценообразование – это процесс формирования цен, включающий в себя установление цены, способов оплаты, видов скидок и надбавок, политикиизменения цен, определение цен на сопутствующие или дополнительныепродукты и услуги.

Основной особенностью рыночного ценообразования на товаринформацию является то, что реальный процесс формирования цен здесьпроисходит не в среде производства, а в среде реализации продукции, тоесть на рынке под воздействием спроса и предложения.

Вопросы к теме

1.Методы ценообразованияна товар-информацию.
2.В чём заключается ценность, или полезность, информации.
3. Специфические особенностипотребительских свойств информации.

Тема 3.Информация как важнейший ресурс экономики.

В экономике очень важны вопросы юридического характера по информационным правоотношениям. Согласно принятой в Российской Федерации Декларации прав и свобод человека и гражданина «каждый человекимеет право искать, получать и распространять информацию», но, с другойстороны, ограничения этого права устанавливаются законом в целях охраны личной, профессиональной, коммерческой и государственной информации.

Вопросы к теме

1.Элементы информационных правоотношений.

2. Государственная, коммерческая, персональная и профессиональная тайны.

3.Методы защиты информации.

4.Способы получения информации. Источники добывания коммерческой информации.

Раздел 2. Экономическая эффективность защиты информации

Тема 4. Информация как товар, цена информации.
Основные методы определения затрат на информационную безопасность.

На основе сравнительных оценок отдельных факторов с учетом возможности их проявления вычисляется значение интегрального показателявыбранного режима распространения информации

$$Z - V * q - U * p = W \ ,$$

где U – потенциально возможная величина ущерба при распространениисведений;

V – потенциально возможная величина выгоды при свободном распространении сведений;

p – вероятность проявления ущерба в период жизненного цикла сведений;

q – вероятность проявления выгоды в период жизненного цикла присвободномраспространении сведений;

Z – величина затрат на защиту сведений.

В случае если рассчитанное значение интегрального показателя оказывается больше нуля, то включение рассматриваемой информации в перечень сведений, отнесенных к информации ограниченного доступа, целесообразно.

Единовременные затраты включают в себя:

1) Затраты на формирование звена управления системой защиты информации и другие организационные затраты;

2) Затрат на приобретение и установку средств защиты.

Выбор способа минимизации затрат зависит от того, какова исходнаяинформация о различных степенях неприятности.

Вопросы к теме

1. Основные методы определения затрат на информационную безопасность.

2.Интегральный показатель выбранного режима распространения информации.**3.**Систематические затратына информационную безопасность.

4. Методика определения размера целесообразных затрат на обеспечение безопасности информации.

5. Оптимальныйминимум суммы затрат на защиту и вероятностные потери вследствиенеполноты защиты информации.

Тема 5. Основные подходы к определению затрат на защиту информации. Формирование бюджета на защиту информации.

Объектами интеллектуальной собственности (ОИС) принято называть результаты интеллектуальной деятельности и средства индивидуализации участников предпринимательской деятельности. Главный критерий при отнесении таких объектов к ОИС - наличие правовой охраны.На результаты интеллектуальной деятельности и приравненные к нимсредства индивидуализации (результаты интеллектуальной деятельности исредства индивидуализации) признаются интеллектуальные права, которые включают исключительное право, являющееся имущественным правом, а в ряде случаев также личные неимущественные и иные права (правоследования, право доступа и другие). Автором результата интеллектуальной деятельности признается гражданин, творческим трудом которого создан такой результат. Не признаются авторами результата интеллектуальной деятельности граждане, невнесшие личного творческого вклада в создание такого результата, в томчисле оказавшие его автору только техническое, консультационное, организационное или материальное содействие. Исключительное право на результат интеллектуальной деятельности, созданный творческим

трудом,первоначально возникает у его автора. Это право может быть передано автором другому лицу по договору и по иным основаниям, установленнымзаконом.

Вопросы к теме

1.Объекты и структура объектов интеллектуальной собственности предприятия.
2. Лицензионный договор. Авторское право. Объекты смежных прав.
3. Экономическая оценка объектов интеллектуальной собственности предприятия.
4. Основные подходы коценке объектов интеллектуальной собственности: рыночный, затратный, метод восстановительной стоимости, метод исходных затрат, доходный подход: метод расчета роялти; метод исключения ставки роялти; методы DCF; методы прямой капитализации; экспресс оценка; метод избыточной прибыли; метод, основанный на «правиле 25%»; экспертные методы.

Тема 6. Система ресурсообеспечения защиты информации и эффективность её использования.

Руководство хозяйствующего субъекта должно учитывать при защите информации те виды рисков, которыевозникают на том или ином предприятии в зависимости от сферы деятельности. Основной угрозой для экономической безопасности предприятия является риск возникновения потерь ресурсов. Главным источником угроздля экономической безопасности является внешняя среда. Предприятиепостоянно взаимодействует с внешней средой, обеспечивая себе тем самым возможность выживания. Для этого существует разветвленная система связей. В качестве внешних связей понимают каналы поступления факторов производства от поставщиков и сбыта продукции клиентам. Предметом связей могут быть материальные потоки, информация, финансы и т.п.

Под риском принято понимать вероятность (угрозу) потери предприятием части своих ресурсов, недополучения доходов или появления дополнительных расходов в результате осуществления определенной хозяйственной деятельности.

Анализ многочисленных определений риска позволяет выявить основные моменты, которые являются характерными для рисковой ситуации, такие, как:

случайный характер события, который определяет, какой из возможных исходов реализуется на практике;

наличие альтернативных решений;

известны вероятности исходов событий и ожидаемые результаты;

существует вероятность возникновения убытков;

существует вероятность получения дополнительной прибыли.

Вопросы к теме

1.Понятие и классификация предпринимательских рисков.
2. Риск возникновения потерь ресурсов.
3.Анализ многочисленных определений риска и оценка рисков.
4.Потери в хозяйственной деятельности: материальные, трудовые, финансовые, временные, специальные.

5.Модель определения зон защиты предприятия в условиях ограниченности средств.

Тема 7. Управление ресурсами в процессе защиты информации.

Особое значение приобретает анализ и оценка предпринимательскогориска. Цель анализа риска заключается в том, чтобы представить необходимую информацию руководству для принятия решений о целесообразности инвестиций и предусмотреть меры по защите от возможных потерь.

В абсолютном выражении риск может определяться величиной возможных потерь в материально-вещественном (физическом) или стоимостном (денежном) выражении, если только ущерб поддается таком измерению. В относительном выражении риск определяется как величина возможных потерь, отнесенная к некоторой базе, в виде которой наиболееудобно принимать либо имущественное состояние предприятия, либо общие затраты ресурсов на данный вид хозяйственной деятельности, либоожидаемый доход от хозяйственной операции.

Потери, которые могут быть в хозяйственной деятельности, целесообразно разделять на материальные, трудовые, финансовые, временные, специальные. Материальные потери проявляются в непредусмотренных дополнительных затратах или прямых потерях оборудования, имущества, продукции, сырья и т.д. Материальные потери измеряются в тех же единицах, вкоторых измеряется количество данного вида материальных ресурсов (вфизических единицах веса, объема, площади и др.), а также в денежномвыражении.

Трудовые потери представляют потери рабочего времени, вызванныенепредвиденными обстоятельствами. Данный вид потерь выражается в человеко-часах, человеко-днях или чесах рабочего времени. Перевод трудовых потерь в стоимостное выражение осуществляется путем умноженияколичества трудочасов на стоимость одного часа.

Финансовые потери – это прямой денежный ущерб, связанный с непредусмотренными платежами, выплатой штрафов, уплатой дополнительных налогов, потерей денежных средств и ценных бумаг. Кроме того, финансовые потери могут возникать при недополучении денег из предусмотренных источников, при невозврате долгов, неоплате покупателем поставленной ему продукции, уменьшении выручки вследствие снижения цен нареализуемые продукцию и услуги. Особые виды денежного ущерба связаны с инфляцией, изменением валютного курса и т.д.

Потери времени заключаются в том, что процесс хозяйственной деятельности идет медленнее, чем было намечено. Прямая оценка таких потерь осуществляется в часах, днях, неделях, месяцах запаздывания, а дляоценки в денежном выражении необходимо установить, к каким потерямдохода способны приводить случайные потери времени.

Вопросы к теме

1. Прямые и косвенные виды ущерба, наносимые информации.
2. Управление ресурсами в процессе защиты информации.

3.В чём проявляются специальные виды потерь в виде нанесения ущерба.

4.Для анализа риска существуют различные способы такие, как статистический, экспертный, расчетно-аналитический, аналогий(дайте краткую характеристику этих способов).

Тема 8. Угрозы информации.

Разновидности угроз информационной безопасности

Угрозой информации называют потенциально возможное влияние или воздействие на автоматизированную систему с последующим нанесением убытка чьим-то потребностям.

На сегодня существует более 100 позиций и разновидностей угроз информационной системе. Важно проанализировать все риски с помощью разных методик диагностики. На основе проанализированных показателей с их детализацией можно грамотно выстроить систему защиты от угроз в информационном пространстве.

Классификация уязвимостей систем безопасности

Угрозы информационной безопасности проявляются не самостоятельно, а через возможное взаимодействие с наиболее слабыми звеньями системы защиты, то есть через факторы уязвимости. Угроза приводит к нарушению деятельности систем на конкретном объекте-носителе.

Основные уязвимости возникают по причине действия следующих факторов:

- несовершенство программного обеспечения, аппаратной платформы;
- разные характеристики строения автоматизированных систем в информационном потоке;
- часть процессов функционирования систем является неполноценной;
- неточность протоколов обмена информацией и интерфейса;
- сложные условия эксплуатации и расположения информации.

Чаще всего источники угрозы запускаются с целью получения незаконной выгоды вследствие нанесения ущерба информации. Но возможно и случайное действие угроз из-за недостаточной степени защиты и массового действия угрожающего фактора.

Существует разделение уязвимостей по классам, они могут быть:

- объективными;
- случайными;
- субъективными.

Если устранить или как минимум ослабить влияние уязвимостей, можно избежать полноценной угрозы, направленной на систему хранения информации.

Объективные уязвимости

Этот вид напрямую зависит от технического построения оборудования на объекте, требующем защиты, и его характеристик. Полноценное избавление от этих факторов

невозможно, но их частичное устранение достигается с помощью инженерно-технических приемов, следующими способами:

1. Связанные с техническими средствами излучения:

- электромагнитные методики (побочные варианты излучения и сигналов от кабельных линий, элементов техсредств);
- звуковые варианты (акустические или с добавлением вибросигналов);
- электрические (проскальзывание сигналов в цепочки электрической сети, по наводкам на линии и проводники, по неравномерному распределению тока).

2. Активизируемые:

- вредоносные ПО, нелегальные программы, технологические выходы из программ, что объединяется термином «программные закладки»;
- закладки аппаратуры – факторы, которые внедряются напрямую в телефонные линии, в электрические сети или просто в помещения.

3. Те, что создаются особенностями объекта, находящегося под защитой:

- расположение объекта (видимость и отсутствие контролируемой зоны вокруг объекта информации, наличие вибро- или звукоотражающих элементов вокруг объекта, наличие удаленных элементов объекта);
- организация каналов обмена информацией (применение радиоканалов, аренда частот или использование всеобщих сетей).

4. Те, что зависят от особенностей элементов-носителей:

- детали, обладающие электроакустическими модификациями (трансформаторы, телефонные устройства, микрофоны и громкоговорители, катушки индуктивности);
- вещи, подпадающие под влияние электромагнитного поля (носители, микросхемы и другие элементы).

Случайные уязвимости

Эти факторы зависят от непредвиденных обстоятельств и особенностей окружения информационной среды. Их практически невозможно предугадать в информационном пространстве, но важно быть готовым к их быстрому устранению. Устранить такие неполадки можно с помощью проведения инженерно-технического разбирательства и ответного удара, нанесенного угрозе информационной безопасности:

1. Сбои и отказы работы систем:

- вследствие неисправности технических средств на разных уровнях обработки и хранения информации (в том числе и тех, что отвечают за работоспособность системы и за контроль доступа к ней);
- неисправности и устаревания отдельных элементов (размагничивание носителей данных, таких как дискеты, кабели, соединительные линии и микросхемы);
- сбои разного программного обеспечения, которое поддерживает все звенья в цепи хранения и обработки информации (антивирусы, прикладные и сервисные программы);

- перебои в работе вспомогательного оборудования информационных систем (неполадки на уровне электропередачи).

2. Ослабляющие информационную безопасность факторы:

- повреждение коммуникаций вроде водоснабжения или электроснабжения, а также вентиляции, канализации;
- неисправности в работе ограждающих устройств (заборы, перекрытия в здании, корпуса оборудования, где хранится информация).

Субъективные уязвимости

Этот подвид в большинстве случаев представляет собой результат неправильных действий сотрудников на уровне разработки систем хранения и защиты информации. Поэтому устранение таких факторов возможно при помощи методик с использованием аппаратуры и ПО:

1. Неточности и грубые ошибки, нарушающие информационную безопасность:

- на этапе загрузки готового программного обеспечения или предварительной разработки алгоритмов, а также в момент его использования (возможно во время ежедневной эксплуатации, во время ввода данных);
- на этапе управления программами и информационными системами (сложности в процессе обучения работе с системой, настройки сервисов в индивидуальном порядке, во время манипуляций с потоками информации);
- во время пользования технической аппаратурой (на этапе включения или выключения, эксплуатации устройств для передачи или получения информации).

2. Нарушения работы систем в информационном пространстве:

- режима защиты личных данных (проблему создают уволенные работники или действующие сотрудники в нерабочее время, они получают несанкционированный доступ к системе);
- режима сохранности и защищенности (во время получения доступа на объект или к техническим устройствам);
- во время работы с техустройствами (возможны нарушения в энергосбережении или обеспечении техники);
- во время работы с данными (преобразование информации, ее сохранение, поиск и уничтожение данных, устранение брака и неточностей).

Ранжирование уязвимостей

Каждая уязвимость должна быть учтена и оценена специалистами. Поэтому важно определить критерии оценки опасности возникновения угрозы и вероятности поломки или обхода защиты информации. Показатели подсчитываются с помощью применения ранжирования. Среди всех критериев выделяют три основных:

- **Доступность** – это критерий, который учитывает, насколько удобно источнику угроз использовать определенный вид уязвимости, чтобы нарушить информационную безопасность. В показатель входят технические данные носителя информации (вроде габаритов аппаратуры, ее сложности и стоимости, а также

возможности использования для взлома информационных систем неспециализированных систем и устройств).

- **Фатальность** – характеристика, которая оценивает глубину влияния уязвимости на возможности программистов справиться с последствиями созданной угрозы для информационных систем. Если оценивать только объективные уязвимости, то определяется их информативность – способность передать в другое место полезный сигнал с конфиденциальными данными без его деформации.
- **Количество** – характеристика подсчета деталей системы хранения и реализации информации, которым присущ любой вид уязвимости в системе.

Каждый показатель можно рассчитать как среднее арифметическое коэффициентов отдельных уязвимостей. Для оценки степени опасности используется формула. Максимальная оценка совокупности уязвимостей – 125, это число и находится в знаменателе. А в числителе фигурирует произведение из КД, КФ и КК.

Чтобы узнать информацию о степени защиты системы точно, нужно привлечь к работе аналитический отдел с экспертами. Они произведут оценку всех уязвимостей и составят информационную карту по пятибалльной системе. Единица соответствует минимальной возможности влияния на защиту информации и ее обход, а пятерка отвечает максимальному уровню влияния и, соответственно, опасности. Результаты всех анализов сводятся в одну таблицу, степень влияния разбивается по классам для удобства подсчета коэффициента уязвимости системы.

Какие источники угрожают информационной безопасности?

Если описывать классификацию угроз, которые обходят защиту информационной безопасности, то можно выделить несколько классов. Понятие классов обязательно, ведь оно упрощает и систематизирует все факторы без исключения. В основу входят такие параметры, как:

1. Ранг преднамеренности совершения вмешательства в информационную систему защиты:

- угроза, которую вызывает небрежность персонала в информационном измерении;
- угроза, инициатором которой являются мошенники, и делают они это с целью личной выгоды.

2. Характеристики появления:

- угроза информационной безопасности, которая провоцируется руками человека и является искусственной;
- природные угрожающие факторы, неподконтрольные информационным системам защиты и вызывающиеся стихийными бедствиями.

3. Классификация непосредственной причины угрозы. Виновником может быть:

- человек, который разглашает конфиденциальную информацию, орудуя с помощью подкупа сотрудников компании;
- природный фактор, приходящий в виде катастрофы или локального бедствия;

- программное обеспечение с применением специализированных аппаратов или внедрение вредоносного кода в техсредства, что нарушает функционирование системы;
- случайное удаление данных, санкционированные программно-аппаратные фонды, отказ в работе операционной системы.

4. Степень активности действия угроз на информационные ресурсы:

- в момент обрабатывания данных в информационном пространстве (действие рассылок от вирусных утилит);
- в момент получения новой информации;
- независимо от активности работы системы хранения информации (в случае вскрытия шифров или криптозащиты информационных данных).

Существует еще одна классификация источников угроз информационной безопасности. Она основана на других параметрах и также учитывается во время анализа неисправности системы или ее взлома. Во внимание берется несколько показателей.

Тема 9. Методы и способы страхования информации. Оценка эффективности защиты и страхования информации

В реальных хозяйственных ситуациях, в условия действия разнообразных факторов риска могут использоваться различные способы снижения финального уровня риска, воздействующие на те или иные сторонывидеятельности предприятия.

К наиболее распространенным методам снижения риска на предприятии относятся следующие.

1. Избежание риска, то есть уклонение от сомнительных проектов,связанных с высоким риском, отказ от работы с ненадежными партнерами.

2. Страхование – представляет собой систему возмещения убытковстраховщиками при наступлении страховых случаев из специальных фондов, формируемых за счет страховых взносов, уплачиваемых страхователями.

Нанесенный предприятию в результате страхового случая материальный ущерб включает в себя два вида убытков: прямые и косвенные.

Самострахование – это создание специального резервного фонда(фонда риска) за счет отчислений на случай возникновения непредвиденной ситуации. Самострахование целесообразно в том случае, когда стоимость страхуемого имущества относительно невелика по сравнению с общим объем капитала предприятия.

Страховой резервный фонд не вовлекается в оборот и является капиталом, не приносящим прибыли. Периодически, в зависимости от статистики убытков в прошлые периоды и размера ожидаемых будущих потерь,а также ситуации на страховом рынке, размер страховых резервов предприятия должен пересматриваться.

Вопросы к теме

1. Методы и способы страхования информации. Страховые случаи материального ущерба.

2. Страховой резервный фонд.

3.Оценка эффективности защиты и страхования информации

Учебно-методическое и информационное обеспечение дисциплины

Рекомендуемая литература

Перечень основной литературы

1. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ Шаньгин В.Ф.— Электрон.текстовые данные.— М.: ДМК Пресс, 2014.— 702 с.— Режим доступа: http://www.iprbookshop.ru/29257.— ЭБС «IPRbooks», по паролю

2. Прохорова О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ Прохорова О.В.— Электрон.текстовые данные.— Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014.— 113 с.— Режим доступа: http://www.iprbookshop.ru/43183.— ЭБС «IPRbooks», по паролю

Перечень дополнительной литературы

1. Кубанков А.Н. Система обеспечения информационной безопасности Российской Федерации: организационно-правовой аспект [Электронный ресурс]: учебное пособие/ Кубанков А.Н., Куняев Н.Н.— Электрон.текстовые данные.— М.: Всероссийский государственный университет юстиции (РПА Минюста России), 2014.— 78 с.— Режим доступа: http://www.iprbookshop.ru/47262.— ЭБС «IPRbooks», по паролю

2. Методы и средства инженерно-технической защиты информации [Электронный ресурс]: учебное пособие/ В.И. Аверченков [и др.].— Электрон.текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 187 с.— Режим доступа: http://www.iprbookshop.ru/7000.— ЭБС «IPRbooks», по паролю

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по выполнению лабораторных работ по дисциплине «Экономика защиты информации»
2. Методические рекомендации для студентов по организации самостоятельной работы по дисциплине «Экономика защиты информации»

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Национальный Открытый Университет. Интуит. http://www.intuit.ru;
2. Федеральный портал «Российское образование. http://www.edu.ru;
3. Российская государственная библиотека. http://www.rsl.ru;
4. Институт Юнеско по информационным технологиям в образовании. http://ru.iite.unesco.org/publications.