**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**
**«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»**

# МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению практических работ
по дисциплине «Моделирование процессов и систем защиты информации»
для студентов направления подготовки
10.03.01 Информационная безопасность
Направленность (профиль)
«Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)»

Ставрополь
2026

**СОДЕРЖАНИЕ:**

## ВВЕДЕНИЕ

### 1. Цель и задачи освоения дисциплины

Цель освоения дисциплины знакомство с основными принципами моделирования, а также построение статических и динамических моделей с использованием современных программных средств. Изучение основ моделирования позволит сформировать у студентов необходимый объем специальных знаний в области методов моделирования и анализа систем.

### 2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с планируемыми результатами освоения образовательной программы

| Код, формулировка компетенции | Код, формулировка индикатора | Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов |
|---|---|---|
| **УК-1** Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач поставленных задач | ИД-1УК-1 выделяет проблемную ситуацию, осуществляет ее многофакторный анализ и диагностику на основе системного подхода | В совершенстве выделяет проблемную ситуацию, осуществляет ее многофакторный анализ и диагностику на основе системного подхода |
| | ИД-3УК-1 определяет и оценивает риски возможных вариантов решений проблемной ситуации, выбирает оптимальный вариант её решения. | В совершенстве определяет и оценивает риски возможных вариантов решений проблемной ситуации, выбирает оптимальный |

## ПЛАНЫ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

### Тема 1. Основные понятия теории моделирования

Практическое занятие №1

**Название работы:** Основные понятия теории моделирования
**Формируемые компетенции:** УК-1
**Теоретическая часть:**

## ОСНОВНЫЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

При выполнении работ можно использовать следующую модель построения системы информационной безопасности (рис. 1), основанную на адаптации ОК (ISO 15408) и проведении анализа риска (ISO 17799).


Рисунок 1 – Модель построения системы информационной безопасности предприятия

Эта модель соответствует специальным нормативным документам по обеспечению информационной безопасности, принятым в Российской Федерации, международному стандарту ISO/IEC 15408 "Информационная технология - методы защиты - критерии оценки информационной безопасности", стандарту ISO/IEC 17799 "Управление информационной безопасностью", и учитывает тенденции развития отечественной нормативной базы (в частности, Гостехкомиссии РФ) по вопросам информационной безопасности.

Представленная модель информационной безопасности - это совокупность объективных внешних и внутренних факторов и их влияние на состояние информационной безопасности на объекте и на сохранность материальных или информационных ресурсов.

Рассматриваются следующие объективные факторы:

– угрозы информационной безопасности, характеризующиеся вероятностью возникновения и вероятностью реализации;

– уязвимости информационной системы или системы контрмер (системы информационной безопасности), влияющие на вероятность реализации угрозы;

– риск - фактор, отражающий возможный ущерб организации в результате реализации угрозы информационной безопасности: утечки информации и ее неправомерного использования (риск в конечном итоге отражает вероятные финансовые потери - прямые или косвенные).

Для построения сбалансированной системы информационной безопасности предполагается первоначально провести анализ рисков в области информационной безопасности. Затем определить оптимальный уровень риска для организации на основе

заданного критерия. Систему информационной безопасности (контрмеры) предстоит построить таким образом, чтобы достичь заданного уровня риска.

Методика проведения аналитических работ

Предлагаемая методика позволяет:

– полностью проанализировать и документально оформить требования, связанные с обеспечением информационной безопасностью;

– избежать расходов на излишние меры безопасности, возможные при субъективной оценке рисков;

– оказать помощь в планировании и осуществлении защиты на всех стадиях жизненного цикла информационных систем;

– обеспечить проведение работ в сжатые сроки;

– представить обоснование для выбора мер противодействия;

– оценить эффективность контрмер, сравнить различные варианты контрмер.

**Определение границ исследования**

В ходе работ должны быть установлены границы исследования. Для этого необходимо выделить ресурсы информационной системы, для которых в дальнейшем будут получены оценки рисков. При этом предстоит разделить рассматриваемые ресурсы и внешние элементы, с которыми осуществляется взаимодействие. Ресурсами могут быть средства вычислительной техники, программное обеспечение, данные. Примерами внешних элементов являются сети связи, внешние сервисы и т. п.

**Построение модели информационной технологии**

При построении модели будут учитываться взаимосвязи между ресурсами. Например, выход из строя какого-либо оборудования может привести к потере данных или выходу из строя другого критически важного элемента системы. Подобные взаимосвязи определяют основу построения модели организации с точки зрения ИБ.

Эта модель, в соответствие с предлагаемой методикой, строится следующим образом: для выделенных ресурсов определяется их ценность, как с точки зрения ассоциированных с ними возможных финансовых потерь, так и с точки зрения ущерба репутации организации, дезорганизации ее деятельности, нематериального ущерба от разглашения конфиденциальной информации и т. д. Затем описываются взаимосвязи ресурсов, определяются угрозы безопасности и оцениваются вероятности их реализации.

**Выбор контрмер**

На основе построенной модели можно обоснованно выбрать систему контрмер, снижающих риски до допустимых уровней и обладающих наибольшей ценовой эффективностью. Частью системы контрмер будут являться рекомендации по проведению регулярных проверок эффективности системы защиты.

**Управление рисками.**

Обеспечение повышенных требований к ИБ предполагает соответствующие мероприятия на всех этапах жизненного цикла информационных технологий. Планирование этих мероприятий производится по завершении этапа анализа рисков и выбора контрмер. Обязательной составной частью этих планов является периодическая проверка соответствия существующего режима ИБ политике без-опасности, сертификация информационной системы (технологии) на соответствие требованиям определенного стандарта безопасности.

**Оценка достигаемой защищенности**

В завершение работ, можно будет определить меру гарантии безопасности информационной среды Заказчика, основанную на оценке, с которой можно доверять информационной среде объекта.

Данный подход предполагает, что большая гарантия следует из применения больших усилий при проведении оценки безопасности. Адекватность оценки основана на:

– вовлечении в процесс оценки большего числа элементов информационной среды объекта Заказчика;

– глубине, достигаемой за счет использования при проектировании системы

обеспечения безопасности большего числа проектов и описаний деталей выполнения;

– строгости, которая заключается в применении большего числа инструментов поиска и методов, направленных на обнаружение менее очевидных уязвимостей или на уменьшение вероятности их наличия.

**Методология анализа рисков.**

Цель процесса оценивания рисков состоит в определении характеристик рисков в информационной системе и ее ресурсах. На основе таких данных выбираются необходимые средства управления ИБ.

Процесс оценивания рисков содержит несколько этапов:

– описание объекта и мер защиты;

– идентификация ресурса и оценивание его количественных показателей (определение потенциального негативного воздействия на бизнес);

– анализ угроз информационной безопасности;

– оценивание уязвимостей;

– оценивание существующих и предполагаемых средств обеспечения информационной безопасности;

– оценивание рисков.

Риск характеризует опасность, которой может подвергаться система и использующая ее организация, и зависит от:

– показателей ценности ресурсов;

– вероятностей нанесения ущерба ресурсам (выражаемых через вероятности реализации угроз для ресурсов);

– степени легкости, с которой уязвимости могут быть использованы при возникновении угроз (уязвимости системы защиты);

– существующих или планируемых средств обеспечения ИБ.

– Расчет этих показателей выполняется на основе математических методов, имеющих такие характеристики, как обоснование и параметры точности метода.

**Построение профиля защиты**

На этом этапе разрабатывается план проектирования системы защиты информационной среды Заказчика. Производится оценка доступных средств, осуществляется анализ и планирование разработки и интеграции средств защиты (рис. 2). Необходимым элементом работы является утверждение у Заказчика допустимого риска объекта защиты.


Рисунок 2 – Возможный алгоритм оценивания информационных рисков

Обеспечение повышенных требований к информационной безопасности предполагает соответствующие мероприятия на всех этапах жизненного цикла информационных технологий. Планирование этих мероприятий производится по завершении этапа анализа рисков и выбора контрмер. Обязательной составной частью этих планов является периодическая проверка соответствия существующего режима ИБ политике без-опасности, сертификация информационной системы (технологии) на соответствие требованиям определенного стандарта безопасности.

Работа по построению плана защиты объекта начинается с построения профиля защиты данного объекта. При этом часть этой работы уже была проделана при проведении анализа рисков.

**Формирование организационной политики безопасности.**

Прежде чем предлагать какие-либо технические решения по системе информационной безопасности объекта, предстоит разработать для него политику безопасности.

Собственно организационная политика безопасности описывает порядок предоставления и использования прав доступа пользователей, а также требования отчетности пользователей за свои действия в вопросах безопасности.

Система информационной безопасности (СИБ) объекта окажется эффективной, если она будет надежно поддерживать выполнение правил политики безопасности, и наоборот. Шагами построения организационной политики безопасности являются:

– внесение в описание объекта автоматизации структуры ценности и проведение анализа риска;

– определение правил для любого процесса пользования данным видом доступа к ресурсам объекта автоматизации, имеющим данную степень ценности.

Организационная политика безопасности оформляется в виде отдельного документа, который согласовывается и утверждается Заказчиком.

**Условия безопасного использования ИТ**

Предполагается, что система обеспечения безопасности объекта Заказчика, соответствующая выбранному профилю защиты, обеспечит требуемый уровень безопасности только в том случае, если она установлена, управляется и используется в соответствие с выработанными правилами. Операционная среда должна управляться согласно принятой для данного профиля защиты нормативной документации, а также инструкциям администраторов и пользователей.

Выделяются следующие виды условий безопасного использования ИТ:

– физические условия;
– условия для персонала;
– условия соединений.

Физические условия касаются размещения ресурсов объекта, а также защиты аппаратных средств и программного обеспечения, критичных к нарушению политики безопасности.

Условия для персонала содержат организационные вопросы управления безопасностью и отслеживания полномочий пользователей.

Условия соединений не содержат явных требований для сетей и распределенных систем, но, например, условие равенства положения означает наличие единой области управления всей сетью объекта.

Условия безопасного использования объекта автоматизации оформляются в виде отдельного документа, который согласовывается и утверждается Заказчиком.

**Формулирование целей безопасности объекта**

В этом разделе профиля защиты дается детализованное описание общей цели построения системы безопасности объекта Заказчика, выражаемое через совокупность факторов или критериев, уточняющих цель. Совокупность факторов служит базисом для определения требований к системе (выбор альтернатив).

Факторы безопасности, в свою очередь, могут распределяться на технологические, технические и организационные.

Определение функциональных требований безопасности

Функциональные требования профиля защиты определяются на основе набора хорошо известных, отработанных и согласованных функциональных требований безопасности. Все требования к функциям безопасности можно разделить на два типа: управление доступом к информации и управление потоками информации.

На этом этапе предстоит правильно определить для объекта компоненты функций безопасности. Компонент функции безопасности описывает определенный набор требований безопасности - наименьший выбираемый набор требований безопасности для включения в профиль защиты. Между компонентами могут существовать зависимости.

**Требования гарантии достигаемой защищенности**

Структура требований гарантии аналогична структуре функциональных требований и включает классы, семейства, компоненты и элементы гарантии, а также уровни гарантии. Классы и семейства гарантии отражают такие вопросы, как разработка, управление конфигурацией, рабочая документация, поддержание этапов жизненного цикла, тестирование, оценка уязвимости и другие вопросы.

Требования гарантии достигаемой защиты выражаются через оценки функций безопасности СИБ объекта. Оценка силы функции безопасности выполняется на уровне отдельного механизма защиты, а ее результаты позволяют определить относительную способность соответствующей функции безопасности противостоять идентифицированным угрозам. Исходя из известного потенциала нападения, сила функции защиты определяется,

например, категориями "базовая", "средняя", "высокая".

Потенциал нападения определяется путем экспертизы возможностей, ресурсов и мотивов побуждения нападающего.

Уровни гарантии. Предлагается использовать табличную сводку уровней гарантированности защиты. Уровни гарантии имеют иерархическую структуру, где каждый следующий уровень предоставляет большие гарантии и включает все требования предыдущего.

**Формирование перечня требований**

Перечень требований к системе информационной безопасности, эскизный проект, план защиты (далее - техническая документация, ТД) содержит набор требований безопасности информационной среды объекта Заказчика, которые могут ссылаться на соответствующий профиль защиты, а также содержать требования, сформулированные в явном виде.

В общем виде разработка ТД включает:

−уточнение функций защиты;

−выбор архитектурных принципов построения СИБ;

−разработку логической структуры СИБ (четкое описание интерфейсов);

−уточнение требований функций обеспечения гарантоспособности СИБ;

−разработку методики и программы испытаний на соответствие сформулированным требованиям.

**Оценка достигаемой защищенности**

На этом этапе производится оценка меры гарантии безопасности информационной среды объекта автоматизации. Мера гарантии основывается на оценке, с которой после выполнения рекомендованных мероприятий можно доверять информационной среде объекта.

Базовые положения данной методики предполагают, что степень гарантии следует из эффективности усилий при проведении оценки безопасности.

Увеличение усилий оценки предполагает:

– значительное число элементов информационной среды объекта, участвующих в процессе оценивания;

– расширение типов проектов и описаний деталей выполнения при проектировании системы обеспечения безопасности;

– строгость, заключающуюся в применении большего числа инструментов поиска и методов, направленных на обнаружение менее очевидных уязвимостей или на уменьшение вероятности их наличия.

## ПРАКТИЧЕСКАЯ ЧАСТЬ

***Задача:*** «Распределение численности специалистов между подразделениями службы управления персоналом».

***Исходные данные:***

- схема оргструктуры службы управления персоналом организации с указанием состава выполняемых каждым подразделением функций управления показана на рисунке 3;

- варианты соотношения общей численности персонала организации и численности службы управления персоналом, а также общая численность персонала организации приведены в таблице 1;

- варианты соотношения трудоемкости функций управления, выполняемых различными подразделениями в рамках службы управления персоналом даны в таблице 2.

***Постановка задачи.*** По имеющейся для конкретной организации схеме оргструктуры службы управления персоналом и примерному составу выполняемых подразделениями функций управления нужно определить, какой должна быть примерная численность каждого из подразделений оргструктуры службы управления персоналом. При этом, общая численность специалистов по управлению персоналом, необходимая организации, зависит от общей численности всего персонала данной организации. В свою очередь, распределение численности специалистов по управлению персоналом внутри соответствующей службы

зависит от соотношения трудоемкости функций управления, выполняемых каждым из подразделений оргструктуры.

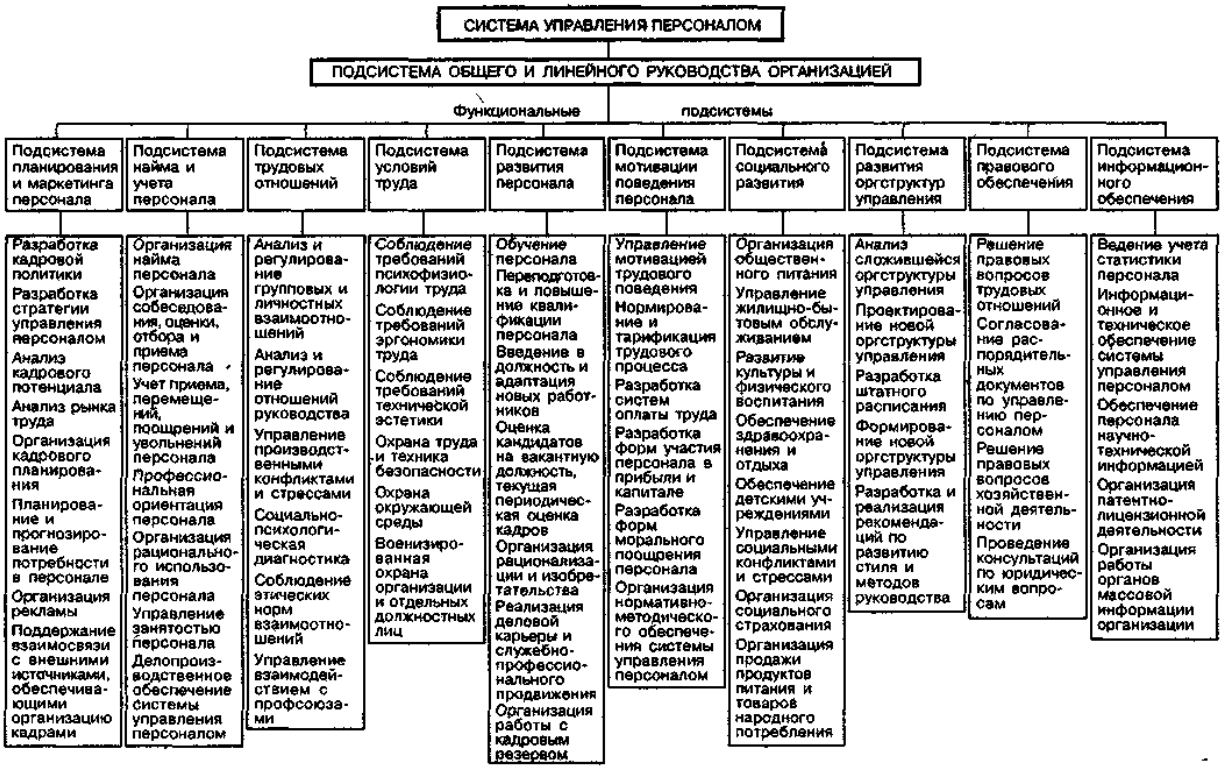



Рисунок 3 - Состав подсистем системы управления персоналом крупной организации и их основные функции.


Рисунок 4 - Схема оргструктуры службы управления персоналом.

***Таблица 1 – Численность специалистов по управлению персоналом***

| Общая численность персонала | Доля численности, приходящаяся на специалистов по управлению персоналом | | |
|---|---|---|---|
| | 1-й вариант | 2-й вариант | 3-й вариант |
| 100% | 0,3-0,5% | 1,0— 1,5% | 1,9—2,3% |

| | | | |
|---|---|---|---|
| 1500 человек | ? | ? | ? |

***Таблица 2 - Соотношения трудоемкости функций управления, выполняемых различными подразделениями***

| | Подразделения службы управления персоналом (см. рис. 1) | | | | | |
|---|---|---|---|---|---|---|
| | наймам увольнения | планирования | развития персонала | мотивации труда | юридических услуг | социальных льгот и выплат |
| | Доля трудоемкости от общего объема работ | | | | | |
| 1-й вариант | 10% | 40% | 30% | 5% | 10% | 5% |
| 2-й вариант | 15% | 25% | 15% | 20% | 10% | 15% |
| 3-й вариант | 15% | 15% | 50% | 12% | 3% | 5% |

**Методические указания**

Проанализировав организационную структуру службы управления персоналом, а, также используя общие статистические зависимости, известные в системе управления персоналом ведущих отечественных и зарубежных фирм, участники игры при решении задачи должны выбрать по таблице 1 тот вариант соотношения численности, который является наиболее распространенным в практике ведущих организаций. Аналогично по таблице 2 следует выбрать наиболее оптимальный вариант распределения трудоемкости выполняемых функций по подразделениям оргструктуры.

Выбрав определенный вариант по таблице 1, необходимо рассчитать численность специалистов по управлению персоналом исходя из общей численности персонала организации. Затем общую численность службы управления персоналом следует распределить по ее подразделениям согласно варианту, выбранному по таблице 2.

**Список литературы, рекомендуемый к использованию по данной теме.**

*Основная:* 1
*Дополнительная: 1, 2, 3, 4, 5, 6*
*Методическая литература: 1, 2*
*Интернет-ресурсы: 1, 2*

Практическое занятие №2

**Название работы:** Бизнес-моделирование

**Формируемые компетенции:** УК-1

**Теоретическая часть:**

## ОСНОВНЫЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

*Модель системы защиты Герасименко и Малюка.* В обобщенных моделях делается попытка одновременно охватить все возможные факторы, влияющие на систему защиты. В модели Герасименко и Малюка защищенность информации определяется некоторыми показателями, которые в свою очередь определяются параметрами системы и внешней среды. Вся совокупность параметров, определяющих значения показателей защищенности информации, в общем случае разделяется на три вида:

– управляемые параметры, т.е. такие, значения которых полностью формируются системой защиты информации;

– параметры, недоступные для такого однозначного и прямого управления, как параметры первого вида, но на которые система защиты может оказывать некоторое воздействие;

– параметры внешней среды, на которые система защиты информации никаким образом воздействовать не может.

Модель процесса защиты информации в самом общем виде может быть представлена так, как показано на рисунке 1.

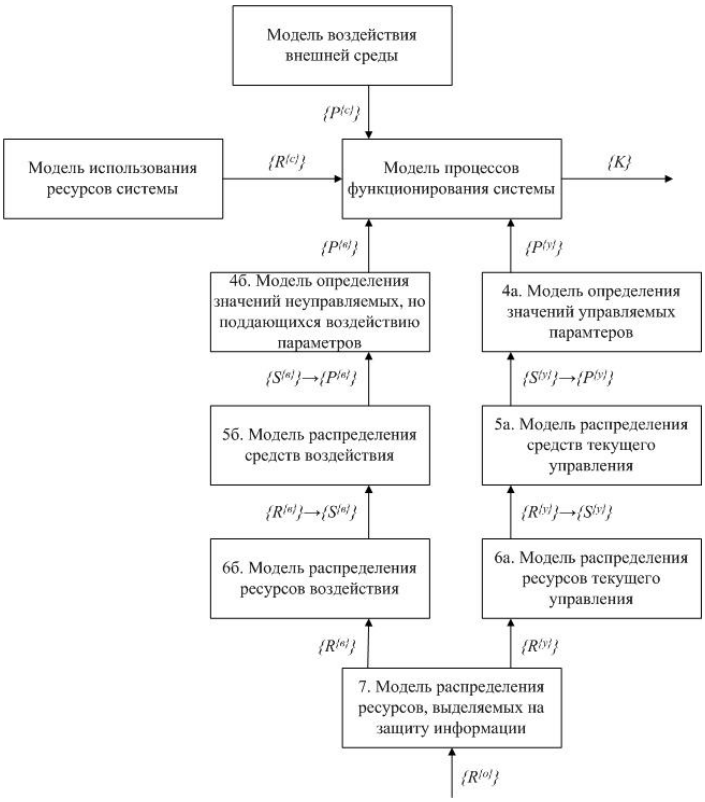



Рисунок 1. Обобщенная модель процессов защиты информации

В модели рассматриваются:

*K* –- множество показателей защищенности (уязвимости) информации;

$P^{(C)}$ – множество параметров внешней среды, оказывающих влияние на функционирование системы;

$R^{(C)}$ – множество ресурсов системы, участвующих в обработке защищаемой информации;

$P^{(y)}$ – множество внутренних параметров системы, которыми можно управлять

непосредственно в процессе обработки защищаемых данных;

$P^{(в)}$ – множество внутренних параметров системы, не поддающихся непосредственному управлению, но поддающихся воздействию (например, в процессе реорганизации или совершенствования компонентов системы);

$S^{(у)}$ и $R^{(у)}$ – множества средств и ресурсов текущего управления;

$S^{(в)}$ и $R^{(в)}$ – множества средств и ресурсов воздействия;

$R^{(о)}$ – множество общих ресурсов управления.

Для приведенной модели возможны следующие модификации:

а) блоки 1, 2 и 3 – модель функционирования системы при отсутствии управления защитой информации (такая модель позволяет лишь определять значения показателей защищенности информации, т.е. решать задачи анализа);

б) блоки 1, 2, 3, 4а и 5а – модель текущего управления защитой информации, основу которого составляет оптимизация использования средств защиты, непосредственно включенных в состав системы (такое управление может быть оперативно-диспетчерским и календарно-плановым);

в) блоки 1, 2, 3, 4а, 5а и 6а – модель управления ресурсами, выделенными на защиту информации, которая дополнительно к предыдущим задачам позволяет оптимизировать процесс формирования средств для текущего управления защитой информации;

г) блоки 1, 2, 3, 4б и 5б - модель управления средствами воздействия на параметры, не допускающие текущего управления, но поддающиеся воздействию;

д) блоки 1, 2, 3, 4б, 5б и 6б – модель управления ресурсами, выделенными на развитие системы;

е) все блоки – полная модель защиты, которая дополнительно ко всем возможностям, рассмотренным выше, позволяет оптимизировать использование всех ресурсов, выделенных на защиту информации.

## ПРАКТИЧЕСКАЯ ЧАСТЬ

Заданы 4 объекта защиты информации: I, II, III, IV. Параметры объектов приведены в таблицах.

Таблица 1 – Влияние параметров внешней среды

| | $P_1^C$ | $P_2^C$ | $P_3^C$ | $P_4^C$ |
|---|---|---|---|---|
| I | 10% | 15% | 5% | 25% |
| II | 30% | 25% | 10% | 15% |
| III | 5% | 26% | 14% | 20% |
| IV | 35% | 10% | 15% | 10% |

Таблица 2 – Влияние множества ресурсов системы, участвующих в обработке защищаемой информации

| | $R_1^C$ | $R_2^C$ | $R_3^C$ | $R_4^C$ |
|---|---|---|---|---|
| I | 55% | 15% | 5% | 25% |
| II | 30% | 25% | 10% | 35% |
| III | 25% | 26% | 14% | 35% |
| IV | 35% | 10% | 15% | 40% |

Таблица 3 – Влияние множества внутренних параметров системы, которыми можно управлять

непосредственно в процессе обработки защищаемых данных

| | $P_1^y$ | $P_2^y$ | $P_3^y$ | $P_4^y$ |
|---|---|---|---|---|
| I | 0,1 | 0,3 | 0,15 | 0,2 |
| II | 0,4 | 0,05 | 0,1 | 0,15 |
| III | 0,2 | 0,15 | 0,05 | 0,3 |
| IV | 0,12 | 0,25 | 0,08 | 0,15 |

Таблица 4 – Влияние множества внутренних параметров системы, не поддающихся непосредственному управлению, но поддающихся воздействию

| | $P_1^{\hat{a}}$ | $P_2^{\hat{a}}$ | $P_3^{\hat{a}}$ | $P_4^{\hat{a}}$ |
|---|---|---|---|---|
| I | 10% | 15% | 5% | 20% |
| II | 25% | 12% | 8% | 15% |
| III | 30% | 25% | 15% | 15% |
| IV | 20% | 15% | 20% | 15% |

Таблица 5 – Влияние множества средств текущего управления

| | $S_1^y$ | $S_2^y$ | $S_3^y$ | $S_4^y$ |
|---|---|---|---|---|
| I | 0,1 | 0,3 | 0,15 | 0,2 |
| II | 0,4 | 0,05 | 0,1 | 0,15 |
| III | 0,2 | 0,15 | 0,05 | 0,3 |
| IV | 0,12 | 0,25 | 0,08 | 0,15 |

Таблица 6 – Влияние множества ресурсов текущего управления

| | $R_1^y$ | $R_2^y$ | $R_3^y$ | $R_4^y$ |
|---|---|---|---|---|
| I | 40% | 15% | 5% | 20% |
| II | 10% | 25% | 30% | 15% |
| III | 15% | 5% | 15% | 20% |
| IV | 15% | 30% | 15% | 30% |

Таблица 7 – Влияние множества средств воздействия

| | $S_1^{\hat{a}}$ | $S_2^{\hat{a}}$ | $S_3^{\hat{a}}$ | $S_4^{\hat{a}}$ |
|---|---|---|---|---|
| I | 15% | 10% | 15% | 5% |
| II | 10% | 5% | 15% | 25% |
| III | 5% | 10% | 15% | 10% |
| IV | 25% | 5% | 10% | 15% |

Таблица 8 – Влияние множество ресурсов воздействия

| | $R_1^{\hat{a}}$ | $R_2^{\hat{a}}$ | $R_3^{\hat{a}}$ | $R_4^{\hat{a}}$ |
|---|---|---|---|---|
| I | 15% | 10% | 15% | 5% |
| II | 10% | 5% | 15% | 25% |
| III | 5% | 10% | 15% | 10% |
| IV | 25% | 5% | 10% | 15% |

**Задание 1.** Рассчитать показатели для модели функционирования системы при отсутствии управления защитой информации (см.модификацию а).

Показатели защищенности рассчитываются по формуле: $K^{a} = \dfrac{P^{y} + 0.5P^{\hat{a}}}{2\mathrm{R}^{c} + 5P^{c}}$

**Задание 2.** Рассчитать показатели для модели текущего управления защитой информации, основу которого составляет оптимизация использования средств защиты, непосредственно включенных в состав системы (см.модификацию б).

Показатели защищенности рассчитываются по формуле: $K^{\hat{a}} = \left| \dfrac{2 \cdot P^{C} - R^{C}}{0{,}5 \cdot P^{y}} \right|$.

**Задание 3.** Рассчитать показатели для модели управления ресурсами, выделенными на защиту информации, которая дополнительно к предыдущим задачам позволяет оптимизировать процесс формирования средств для текущего управления защитой информации (см.модификацию в).

Показатели защищенности рассчитываются по формуле: $K^{\hat{a}} = \dfrac{P^{C} + R^{C}}{2\left|P^{y} - 3S^{y}\right| \cdot}$.

**Задание 4.** Рассчитать показатели для модели управления средствами воздействия на параметры, не допускающие текущего управления, но поддающиеся воздействию (см.модификацию г).

Показатели защищенности рассчитываются по формуле: $K^{\tilde{a}} = \dfrac{1}{P^{c}} + \dfrac{\left|R^{c} - P^{\hat{a}}\right|}{S^{\hat{a}} + 0{,}3 \cdot}$.

**Задание 5.** Рассчитать показатели для модели управления ресурсами, выделенными на развитие системы (см.модификацию д).

Показатели защищенности рассчитываются по формуле: $K^{\ddot{a}} = \dfrac{1}{P^{c}} - \dfrac{\left|R^{c} - P^{\hat{a}} R^{\hat{a}}\right|}{S^{\hat{a}} + 0{,}3 \cdot}$.

**Задание 6.** Рассчитать показатели для полной модели защиты, которая дополнительно ко всем возможностям, рассмотренным выше, позволяет оптимизировать использование всех ресурсов, выделенных на защиту информации. (см.модификацию е).

Показатели защищенности рассчитываются по формуле: $K^{\mathring{a}} = \dfrac{\left|K^{a} - K^{\hat{a}}\right|}{10\hat{E}^{\acute{a}}} - \hat{E}^{\tilde{a}} \hat{E}^{\ddot{a}}$.

**Задание 6.** Вычислить критерии $F_1$, $F_2$, $1 - F_3$ для каждого из четырех объектов защиты и внести их в таблицу 9.

Критерии:

$F_1 = \dfrac{1}{6} \sum_{i=a}^{e} K^{i}$ – средний уровень защищенности;

$F_2 = \min\limits_{1 \le i \le 6} K^{i}$ – оценка по наихудшему;

$F_3 = \sqrt{\sum_{i=1}^{6} \left(K^{i} - \overline{K}\right)^{2}}$ – расстояние до идеальной точки, $\overline{K} = 0{,}7$ – идеальная точка (заданный уровень защищенности).

$\widetilde{F} = \lambda_1 \cdot F_1 + \lambda_2 \cdot F_2 + \lambda_3 \cdot \left(1 - F_3\right)$ – обобщенный критерий ($\lambda_1 = 0{,}1, \lambda_2 = 0{,}3, \lambda_5 = 0{,}6$ – коэффициенты важности критериев).

Таблица 9 – Значения критериев оценки объектов защиты информации

| Объекты | Критерии | | | |
|---|---|---|---|---|
| | $F_1$ | $F_2$ | $1 - F_3$ | $\widetilde{F}$ |

| | | | | |
|---|---|---|---|---|
| I | $F_1(I)$ | $F_2(I)$ | $1-F_3(I)$ | $\widetilde{F}(I)$ |
| II | $F_1(II)$ | $F_2(II)$ | $1-F_3(II)$ | $\widetilde{F}(II)$ |
| III | $F_1(III)$ | $F_2(III)$ | $1-F_3(III)$ | $\widetilde{F}(III)$ |
| IV | $F_1(IV)$ | $F_2(IV)$ | $1-F_3(IV)$ | $\widetilde{F}(IV)$ |

**Задание 8.** Выделить множество доминирующих объектов защиты (объект является доминирующим, если $F_1 \to max$, $F_2 \to max$, $F_3 \to max$) и указать оптимальный по обобщенному критерию объект защиты.

**Контрольные вопросы**

1. Понятие системы и процессов защиты информации.
2. Управляемые параметры обобщенной модели системы защиты информации.
3. Параметры, на которые система защиты информации может оказывать воздействие.
4. Параметры внешней среды для системы защиты информации.
5. Модификации обобщенной модели системы защиты информации.
6. Критерии защищенности объекта информатизации.

**Список литературы, рекомендуемый к использованию по данной теме.**

*Основная:* 1

*Дополнительная: 1, 2, 3, 4, 5, 6*

*Методическая литература: 1, 2*

*Интернет-ресурсы: 1, 2*

**Тема 2. Бизнес-моделирование**

Практическое занятие № 3

**Название работы:** Математическое моделирование

**Формируемые компетенции:** УК-1

**Теоретическая часть:**

## ОСНОВНЫЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Решение проблемы защиты информации с точки зрения системного подхода можно сформулировать как трансформацию существующей системы в требуемую.

Целями системы защиты являются обеспечение требуемых уровней безопасности информации на фирме, в организации, на предприятии (в общем случае – на объекте защиты). Задачи конкретизируют цели применительно к видам и категориям защищаемой информации. А также элементам объекта защиты и отвечают на вопрос, что надо делать для достижения целей. Кроме того, уровень защиты нельзя рассматривать в качестве абсолютной меры, безотносительно от ущерба, который может возникнуть от потери информации и использовании ее злоумышленником во вред владельцу информации.

В качестве ориентира для оценки требуемого уровня защиты информации необходимо определить соотношение между ценой защищаемой информации и затратами на ее защиту. Уровень защиты рационален, когда обеспечивается требуемый уровень безопасности информации ($С_{уи} \le С_{уд}$) и минимизируются расходы на защиту информацию ($С_{зи} \le С_{зд}$). Эти расходы $С_{ри}$ складываются из:

- затрат на защиту информации $С_{зи}$;
- ущерба $С_{уи}$ за счет попадания информации к злоумышленнику и использования ее во вред владельца.

Между этими слагаемыми существует достаточно сложная связь, так как ущерб из-за недостаточной безопасности информации уменьшается с увеличением расходов на ее защиту.

Если первое слагаемое может быть точно определено, то оценка ущерба в условиях скрытности разведки и неопределенности прогноза использования злоумышленником полученной информации представляет достаточно сложную задачу. Ориентировочная оценка ущерба возможна при следующих допущениях.

Владелец информации ожидает получить от ее материализации определенную прибыль, которой он может лишиться в случае попадания ее конкуренту. Кроме того, последний, используя информацию, может нанести владельцу еще дополнительный ущерб за счет, например, изменения тактики, продажи или покупки ценных бума и т.д. Дополнительные неблагоприятные факторы чрезвычайно трудно поддаются учету. Поэтому в качестве граничной меры для оценки ущерба можно использовать величину потенциальной прибыли $С_{пи}$, которую ожидает получить от информации ее владелец, т.е.

$$С_{уи} \ge С_{пи}, \qquad (1)$$

В свою очередь величина ущерба зависит от уровня защиты, определяемой расходами на нее. Максимальный ущерб возможен при нулевых расходах на защиту, гипотетически нулевой ущерб обеспечивается при идеальной защите. Но идеальная защита требует бесконечно больших затрат.

При увеличении расходов вероятность попадания информации злоумышленнику, а, следовательно, и ущерб уменьшаются. Но одновременно увеличиваются расходы на защиту. Указанные зависимости иллюстрируются на рисунке 1.

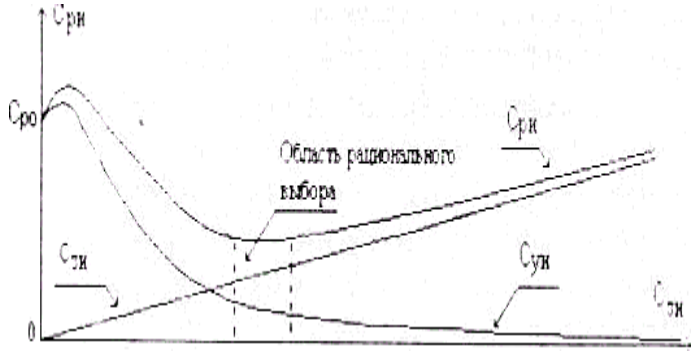


Рисунок 1 – Зависимость расходов на информацию от затрат на ее защиту

Из рисунка 1 следует, что функция $C_{ри} = f(C_{уи},C_{зи})$ имеет область, в которой $C_{ри}$ принимает максимальное и минимальное значения. Рост суммарных расходов на информацию с увеличением затрат на ее защиту имеет место в период создания или модернизации системы, когда происходит накопление мер и средств защиты, которые не оказывают существенного влияния на безопасность информации. Например, предотвращение утечки информации по отдельным канал без снижения вероятности утечки по всем остальным не приводит к заметному повышению безопасности информации, хотя затраты на закрытие отдельных каналов могут быть весьма существенными. Образно говоря, для объекта защиты существует определенная «критическая масса» затрат на защиту информации, при превышении которой эти затраты обеспечивают эффективную отдачу.

При некоторых рациональных затратах на защиту информации выше критических наблюдается минимум суммарных расходов на информацию. При затратах ниже рациональных увеличивается потенциальный ущерб за счет повышения вероятности попадания конфиденциальной информации к злоумышленнику, при более высоких затратах – увеличиваются прямые расходы на защиту.

Ограничения системы представляют собой выделяемые на защиту информации людские, материальные, финансовые ресурсы, а также ограничения в виде требований к системе. Суммарные ресурсы удобно выражать в денежном эквиваленте. Независимо от выделяемых на защиту информации ресурсов они не должны превышать суммарной цены защищаемой информации. Это верхний порог ресурсов.

Проектирование требуемой системы защиты проводится путем системного анализа существующей и разработки вариантов требуемой. Алгоритм этого процесса включает следующие этапы:

- определение перечня защищаемой информации, целей, задач, ограничений и показателей эффективности системы зашиты;
- моделирование существующей системы и выявление ее недостатков с позиции поставленных целей и задач;
- определение и моделирование угроз безопасности информации;
- разработка вариантов (алгоритмов функционирования) проектируемой системы;
- сравнение вариантов по глобальному критерию и частным показателям, выбор наилучших вариантов;
- обоснование выбранных вариантов системы в докладной записке или в проекте для руководства организации;
- доработка вариантов или проекта с учетом замечаний руководства.

Так как отсутствуют формальные способы синтеза системы зашиты, то ее оптимизация при проектировании возможна путем постепенного приближения к рациональному варианту в результате нескольких итераций.

В ходе проектирования создаются модели объектов зашиты и угроз безопасности информации, в том числе модели каналов утечки информации, оцениваются угрозы, разрабатываются способы защиты информации, выбираются технические средства, определяются эффективность защиты и необходимые затраты. Разработка способов и средств

защиты информации прекращается, когда достигается требуемый уровень ее безопасности, а затраты на защиту соответствуют ресурсам.

После рассмотрения руководством предлагаемых вариантов *(лучше* двух для предоставления выбора), учета предложений и замечаний, наилучший, с точки зрения лица, принимающего решения, вариант (проект, предложения) финансируется и реализуется путем проведения необходимых закупок материалов и оборудования, проведения строительно-монтажных работ, наладки средств защиты и сдачи в эксплуатацию системы зашиты.

Следует подчеркнуть, что специалист по защите информации должен при обосновании предлагаемых руководству организации вариантов защиты учитывать психологию лица (руководителя), принимающего решение о реализации предложений, и в большинстве случаях недостаточную информированность его об угрозах безопасности информации в организации.

Психологическим фактором, сдерживающим принятие решения руководителем о выделении достаточно больших ресурсов на защиту информации является то обстоятельство, что в условиях скрытности добывания информации угрозы ее безопасности не представляются достаточно серьезными, а приобретают некоторый абстрактный характер. Знание руководителем о существовании, в принципе, таких угроз, но без достаточно убедительных доводов специалиста о наличии угроз безопасности информации в конкретной организации, не гарантирует финансирование проекта в необходимом объеме. Кроме того, руководитель в силу собственного представления об угрозах, способах и средствах их нейтрализации может преувеличивать значимость одних мер защиты и преуменьшать другие. Однако это обстоятельство не должно уменьшать энтузиазм специалиста по защите информации, так как оно характерно для любого вида деятельности, а умение обосновывать свои предложения является необходимым качеством любого специалиста.

Корректировка мер по защите информации производится после рассмотрения проекта руководством организации, а также в ходе реализации проекта и эксплуатации системы защиты.

Для защиты информации на основе системного подхода и анализа необходимо, наряду с организационным и техническим, методическое обеспечение. В соответствии с алгоритмом проектирования системы оно должно обеспечивать:

- моделирование объекта защиты;
- выявление и моделирование угроз безопасности информации;
- разработку мер инженерно-технической защиты информации.

Моделирование объектов защиты включает:

- структурирование защищаемой информации;
- разработку моделей объектов защиты.

Для структурирования информации в качестве исходных данных используются:

- перечень сведений, составляющих государственную, ведомственную или коммерческую тайну;
- перечень источников информации в организации.

Структурирование информации проводится путем классификации информации в соответствии со структурой, функциями и задачами организации с привязкой элементов информации к ее источникам. Детализацию информации целесообразно проводить до уровня, на котором элементу информации соответствует один источник.

Схема классификации разрабатывается в виде графа-структуры, нулевой (верхний) уровень иерархии которой соответствует понятию «защищаемая информация», а n-ый (нижний) - элементам информации одного источника из перечня источников организации. Основное требование к схеме классификации - общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня, т. е. одна и та же информация не должна указываться в разных элементах классификации.

Результаты структурирования оформляются в виде:

- схемы классификации информации;
- таблицы 1.

Таблица разрабатывается на основе схемы классификации информации. В первом столбце указывается номер элемента информации в схеме классификации.

Порядковый номер элемента информации соответствует номеру тематического вопроса в структуре информации. Значность номера равна количеству уровней структуры, а каждая цифра - порядковому номеру тематического вопроса на рассматриваемом уровне среди вопросов, относящихся к одному тематическому вопросу на предыдущем уровне. Например, номер 2635 соответствует информации 5-го тематического вопроса на 4-м уровне, входящего в 3-й укрупненный вопрос 3-го уровня, который, в свою очередь, является частью 6-го тематического вопроса 2-го уровня, представляющего собой вопрос 2-и темы 1-го уровня.

Таблица 1 - Результаты структурирования информации

| № элемента информации | Наименование элемента информации | Гриф Конфиденциаль-ности информации | Цена информации | Наименование источника информации | Местонахож-дение источника информации |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |
| | | | | | |
| | | | | | |
| | | | | | |

Во 2-м, 3-м и 4-м столбцах таблицы указываются наименование элемента информации (тематического вопроса) и его характеристики: гриф и цена. Последующие столбцы таблицы относятся к источникам информации соответствующего ее элемента в схеме классификации. В столбце 5 указывается наименование источника (фамилия человека, название документа или его номер по книге учета, наименование и номер изделия и т.д.), а в графе 6 - места размещения или хранения (возможные рабочие места людей-источников информации, места расположения, размещения или хранения других носителей).

Эти места в общем случае представляют собой:

– помещения (служебные, лаборатории, офисы, цеха, склады, квартиры и др.);

– письменные столы рабочих мест сотрудников, хранилища и сейфы, шкафы деревянные и металлические в помещениях.

В помещениях размешается большинство источников информации: люди, документы, разрабатываемая продукция и ее элементы, средства обработки и хранения информации и др., а также источники функциональных и опасных сигналов.

## ПРАКТИЧЕСКАЯ ЧАСТЬ

Вами должно быть выбран и описан конкретный объект защиты. Этим объектом может являться то предприятие, на котором вы работаете или агентство «Недвижимость» (см. информацию для описания в таблице 3.2).

Таблица 2 –Наименование и краткое описание объекта защиты

Агентство «Недвижимость», являясь дочерней организацией агентства «Русская недвижимость», расположенного в г. Москве.

В связи с расширением агентство «Недвижимость» предполагает разместиться в помещениях 2-го этажа учреждения, аналогичного помещениям кафедры ОТиЗИ СГУ в аудиториях:

- № 208 (разделенная на две части, в ней - 5 агентов по работе с клиентами, специалист по информационной безопасности);
- № 209 (зал заседаний);
- № 210 (бухгалтер и кассир);
- № 211 (директор и заместитель по работе с кадрами);
- холл (секретарша).

Рабочие места каждого сотрудника планируется оборудовать ПЭВМ, объеденными в ЛВС с выходом в Internet.

Вы – специалист по информационной безопасности.

Задание:

1. Необходимо предоставить детальное описание этого предприятия (объем не менее 5 страниц). Описание предприятия должно содержать следующие разделы:

– общее описание (где находится, чем занимается, сколько человек работает, организационная структура, структура производственных процессов и их краткое описание),

– нормативная база предприятия, в том числе по защите информации;

– план территории, расположения помещений/помещения предприятия с указанием наименований соответствующих подразделений, на плане также должны быть указаны основные конструктивные элементы помещений, расположение источников информации, средств ее обработки, линий связи, коммуникации и пр.

– перечень используемых информационных систем, средств и комплексов защиты.

2. Оформить результаты структурирования информации.

На основании описания предприятия необходимо произвести структурирование информации, обрабатываемой информации. Результатом выполнения должна быть заполненная таблица 1. Количество элементов информации – не менее 20.

**Список литературы, рекомендуемый к использованию по данной теме.**

*Основная:* 1

*Дополнительная: 1, 2, 3, 4, 5, 6*

*Методическая литература: 1, 2*

*Интернет-ресурсы: 1, 2*

Практическое занятие № 4

**Название работы:** Имитационное моделирование

**Формируемые компетенции:** УК-1

**Теоретическая часть:**

## ОСНОВНЫЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

*Модель элементарной защиты.* Рассмотрим вероятностную модель системы защиты информации, в которой система защиты информации представлена неконтролируемыми преградами вокруг предмета защиты. В общем случае модель элементарной защиты предмета может быть в виде, представленном на рисунке 1. В качестве предмета защиты выступает один из компонентов информационной системы.


Рисунок 1 – Модель элементарной защиты

Вероятность непреодоления преграды нарушителем обозначается как $P_{ñçè}$, вероятность преодоления преграды нарушителем через $P_{ïð}$, соответственно сумма вероятностей двух противоположных событий равна 1, т.е. $P_{ñçè} + P_{ïð} = 1$. Отсюда $P_{ñçè} = (1 - P_{ïð})$.

В модели рассматриваются пути обхода преграды. Вероятность обхода преграды нарушителем обозначается через $P_{îáõ}$, которое представляется в виде:

$$P_{ñçè} = \min\{(1 - P_{ïð})(1 - P_{îáõ})\}. \quad (1)$$

В случае, когда у преграды несколько путей обхода:

$$P_{ñçè} = \min\{(1 - P_{ïð})(1 - P_{îáõ1}),(1 - P_{îáõ2}),(1 - P_{îáõ3}),...,(1 - P_{îáõk})\}. \quad (2)$$

где $k$ – количество путей отхода.

Для случая, когда нарушителей более одного, и они действуют одновременно (организованная группа) по каждому пути, это выражение с учетом совместимости событий выглядит как:

$$P_{ñçè} = (1 - P_{ïð})(1 - P_{îáõ1})(1 - P_{îáõ2})(1 - P_{îáõ3})..(1 - P_{îáõk}). \quad (3)$$

*Модель многозвенной защиты.* Учитывая, что на практике в большинстве случаев защитный контур (оболочка) состоит из нескольких «соединенных» между собой преград с различной прочностью рассматривается модель многозвенной защиты, отображенная на рисунке 2.

Выражение прочности многозвенной защиты из неконтролируемых преград, построенной для противостояния одному нарушителю, представлено в виде:

$$P_{ñçç} = \min\{Ð_{ñçè1}, Ð_{ñçè2},..., Ð_{ñçèi},..., (1 - P_{îáõ1}),(1 - P_{îáõ2})...,(1 - P_{îáõk})\} \quad (4)$$

,

где $P_{ñçèi}$ – прочность $i$-й преграды, $P_{îáõ}$ – вероятность обхода преграды по $k$-му пути.

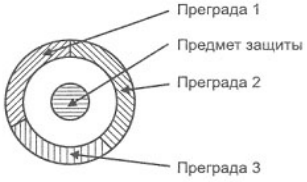



Рисунок 2 – Модель многозвенной защиты

Выражение для прочности многозвенной защиты, построенной из неконтролируемых преград для защиты от организованной группы квалифицированных нарушителей-профессионалов, с учетом совместимости событий

представлено в виде:

$$Ð_{ñçè} = Ð_{ñçè1} \times Ð_{ñçè2} \times ... \times Ð_{ñçèi} \times (1 - P_{îáõ1}) \times (1 - P_{îáõ2}) \times ... \times (1 - P_{îáõk}). \quad (5)$$

*Модель многоуровневой защиты.* Вероятностная модель многоуровневой защиты представлена на рисунке 3.

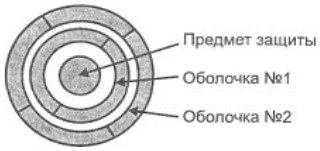



Рисунок 3 – Модель многоуровневой защиты

При расчете суммарной прочности нескольких оболочек (контуров) защиты используется формула

$$Ð = 1 - Ð_{ïð} = 1 - (1 - Ð_{k1})(1 - Ð_{k2})(1 - Ð_{k3})...(1 - Ð_{ki}), \quad (6)$$

где $P_{ki}$ – прочность каждой оболочки (контура), значение которой определяется по одной из формулы (5).

При $P_{ki} = 0$ данная оболочка (контур) в расчет не принимается. При $P_{ki} = 1$ остальные оболочки защиты являются избыточными. Данная модель справедлива лишь для замкнутых оболочек защиты, перекрывающих одни и те же каналы несанкционированного доступа к одному и тому же предмету защиты.

## ПРАКТИЧЕСКАЯ ЧАСТЬ

**Задание 1.**

Имеется:

– статистика успешных атак на информационную систему при отсутствии путей обхода преграды (см. табл. 1),

– статистика успешного обхода преград (см. табл. 2);

Найти:

а) вероятность непреодоления преграды нарушителем при отсутствии путей обхода преграды;

б) вероятность непреодоления преграды нарушителем в случае, когда у преграды имеется 1 путь обхода;

в) вероятность непреодоления преграды нарушителем в случае, когда у преграды имеется несколько путей обхода;

г) вероятность непреодоления преграды организованной группой нарушителей, действующих одновременной по всем путям обхода преграды.

**Задание 2.** Защитный контур (оболочка) состоит из нескольких соединенных между собой звеньев преграды с различной прочностью (см. табл. 3). Известны вероятности обхода преграды по каждому из путей (см. табл. 4).

Найти:

а) прочность многозвенной защиты из неконтролируемых преград, построенной для противостояния одному нарушителю;

б) прочность многозвенной защиты, построенной из неконтролируемых преград для защиты от организованной группы квалифицированных нарушителей-профессионалов.

**Задание 3.** Вычислить вероятность многоуровневой защиты информации. Количество уровней защиты, прочности звеньев каждого уровня и вероятности обходов преград заданы в табл. 5.

Таблица 1 – Статистика успешных атак на информационную систему при отсутствии

путей обхода преграды

| Номер варианта | Успешное количество атак | Общее количество атак | Номер варианта | Успешное количество атак | Общее количество атак |
|---|---|---|---|---|---|
| 1 | 150 | 1099 | 16 | 451 | 4983 |
| 2 | 200 | 1894 | 17 | 876 | 2418 |
| 3 | 210 | 4732 | 18 | 569 | 5874 |
| 4 | 280 | 6594 | 19 | 213 | 6520 |
| 5 | 188 | 3291 | 20 | 457 | 9172 |
| 6 | 169 | 9838 | 21 | 432 | 4627 |
| 7 | 300 | 8737 | 22 | 125 | 1020 |
| 8 | 543 | 7640 | 23 | 678 | 3037 |
| 9 | 345 | 5836 | 24 | 987 | 4726 |
| 10 | 985 | 7328 | 25 | 765 | 4395 |
| 11 | 225 | 4939 | 26 | 453 | 5584 |
| 12 | 326 | 4980 | 27 | 448 | 2290 |
| 13 | 557 | 2381 | 28 | 552 | 7739 |
| 14 | 541 | 2918 | 29 | 229 | 2871 |
| 15 | 236 | 2817 | 30 | 784 | 2019 |

Таблица 2 – Статистика успешного обхода преград

| Номер варианта | Успешное количество обхода | Общее количество попыток обхода | Номер варианта | Успешное количество обхода | Общее количество попыток обхода |
|---|---|---|---|---|---|
| 1 | 152 | 3467 | 16 | 660 | 1357 |
| 2 | 143 | 8742 | 17 | 703 | 6573 |
| 3 | 543 | 1369 | 18 | 210 | 4871 |
| 4 | 98 | 8763 | 19 | 222 | 2468 |
| 5 | 786 | 3468 | 20 | 259 | 9754 |
| 6 | 541 | 7385 | 21 | 805 | 5468 |
| 7 | 210 | 6790 | 22 | 468 | 4478 |
| 8 | 763 | 9872 | 23 | 438 | 6690 |
| 9 | 479 | 3683 | 24 | 459 | 7941 |
| 10 | 125 | 6890 | 25 | 805 | 2468 |
| 11 | 642 | 3218 | 26 | 120 | 7901 |
| 12 | 340 | 9574 | 27 | 340 | 2378 |
| 13 | 806 | 4692 | 28 | 670 | 8904 |
| 14 | 508 | 3579 | 29 | 543 | 3784 |
| 15 | 547 | 8751 | 30 | 321 | 3343 |

Таблица 3 – Количество звеньев преграды и их прочности

| Номер варианта | Количество звеньев преграды | Прочности звеньев преграды | | | | |
|---|---|---|---|---|---|---|
| | | $Ð_{ñçè1}$ | $Ð_{ñçè2}$ | $Ð_{ñçè3}$ | $Ð_{ñçè4}$ | $Ð_{ñçè5}$ |
| 1 | 3 | 0,32 | 0,17 | 0,54 | - | - |
| 2 | 4 | 0,48 | 0,15 | 0,15 | 0,72 | - |
| 3 | 2 | 0,33 | 0,49 | - | - | - |
| 4 | 5 | 0,15 | 0,37 | 0,25 | 0,89 | 0,65 |
| 5 | 4 | 0,39 | 0,82 | 0,75 | 0,87 | - |
| 6 | 2 | 0,58 | 0,74 | - | - | - |

| | | | | | | |
|---|---|---|---|---|---|---|
| 7 | 3 | 0,77 | 0,83 | 0,52 | - | - |
| 8 | 4 | 0,48 | 0,61 | 0,69 | 0,74 | - |
| 9 | 5 | 0,58 | 0,83 | 0,61 | 0,73 | 0,88 |
| 10 | 4 | 0,55 | 0,81 | 0,69 | 0,67 | - |
| 11 | 3 | 0,64 | 0,50 | 0,72 | - | - |
| 12 | 2 | 0,57 | 0,63 | - | - | - |
| 13 | 4 | 0,61 | 0,57 | 0,53 | 0,81 | - |
| 14 | 3 | 0,72 | 0,69 | 0,50 | - | - |
| 15 | 2 | 0,92 | 0,78 | - | - | - |
| 16 | 4 | 0,68 | 0,57 | 0,51 | 0,50 | - |
| 17 | 5 | 0,77 | 0,50 | 0,50 | 0,49 | 0,58 |
| 18 | 3 | 0,39 | 0,46 | 0,81 | - | - |
| 19 | 4 | 0,41 | 0,64 | 0,56 | 0,63 | - |
| 20 | 5 | 0,68 | 0,65 | 0,59 | 0,42 | 0,70 |
| 21 | 4 | 0,44 | 0,59 | 0,71 | 0,69 | - |
| 22 | 3 | 0,69 | 0,49 | 0,85 | - | - |
| 23 | 2 | 0,68 | 0,57 | - | - | - |
| 24 | 4 | 0,81 | 0,54 | 0,66 | 0,49 | - |
| 25 | 5 | 0,70 | 0,59 | 0,48 | 0,87 | - |
| 26 | 5 | 0,23 | 0,64 | 0,15 | 0,62 | 0,55 |
| 27 | 4 | 0,20 | 0,57 | 0,81 | 0,44 | - |
| 28 | 3 | 0,48 | 0,71 | 0,85 | - | - |
| 29 | 2 | 0,54 | 0,86 | - | - | - |
| 30 | 4 | 0,61 | 0,49 | 0,55 | 0,64 | - |

Таблица 4 – Количество путей обхода преграды и их вероятности

| Номер варианта | Количество обходов | Вероятности обходов | | | | |
|---|---|---|---|---|---|---|
| | | $Đ_{íáõ\,1}$ | $Đ_{íáõ\,2}$ | $Đ_{íáõ\,3}$ | $Đ_{íáõ\,4}$ | $Đ_{íáõ\,5}$ |
| 1 | 3 | 0,87 | 0,19 | 0,44 | - | - |
| 2 | 5 | 0,56 | 0,25 | 0,35 | 0,72 | 0,36 |
| 3 | 4 | 0,68 | 0,59 | 0,44 | 0,48 | - |
| 4 | 3 | 0,43 | 0,67 | 0,45 | - | - |
| 5 | 5 | 0,76 | 0,42 | 0,65 | 0,57 | - |
| 6 | 4 | 0,48 | 0,54 | 0,66 | 0,38 | - |
| 7 | 3 | 0,15 | 0,63 | 0,51 | - | - |
| 8 | 2 | 0,19 | 0,69 | - | - | - |
| 9 | 5 | 0,45 | 0,73 | 0,51 | 0,63 | 0,53 |
| 10 | 4 | 0,25 | 0,87 | 0,69 | 0,47 | - |
| 11 | 3 | 0,51 | 0,40 | 0,75 | - | - |
| 12 | 4 | 0,57 | 0,43 | 0,55 | 0,61 | - |
| 13 | 5 | 0,89 | 0,59 | 0,53 | 0,76 | 0,53 |
| 14 | 5 | 0,43 | 0,49 | 0,50 | 0,58 | 0,49 |
| 15 | 4 | 0,56 | 0,58 | 0,42 | 0,74 | - |
| 16 | 3 | 0,77 | 0,51 | 0,51 | - | - |
| 17 | 2 | 0,47 | 0,30 | - | - | - |
| 18 | 5 | 0,61 | 0,26 | 0,81 | 0,89 | 0,17 |
| 19 | 3 | 0,37 | 0,54 | 0,56 | - | - |
| 20 | 4 | 0,68 | 0,55 | 0,59 | 0,32 | 0,75 |
| 21 | 5 | 0,54 | 0,49 | 0,71 | 0,49 | 0,63 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 22 | 4 | 0,42 | 0,39 | 0,75 | 0,39 | - |
| 23 | 3 | 0,55 | 0,67 | 0,56 | - | - |
| 24 | 5 | 0,76 | 0,64 | 0,66 | 0,39 | 0,37 |
| 25 | 2 | 0,38 | 0,39 | 0,48 | 0,67 | - |
| 26 | 4 | 0,35 | 0,54 | 0,15 | 0,62 | - |
| 27 | 5 | 0,44 | 0,37 | 0,81 | 0,34 | 0,55 |
| 28 | 3 | 0,52 | 0,61 | 0,75 | - | - |
| 29 | 4 | 0,58 | 0,66 | 0,55 | 0,43 | - |
| 30 | 5 | 0,46 | 0,39 | 0,55 | 0,54 | 0,67 |

Таблица 5 – Количество уровней защиты

| Номер варианта | Количество уровней защиты | Данные уровней защиты (см. варианты таблицы 4) |
|---|---|---|
| 1 | 2 | 1 уровень –20, 2 уровень – 9 |
| 2 | 3 | 1 уровень – 2, 2 уровень – 5, 3 уровень – 25 |
| 3 | 2 | 1 уровень – 4, 2 уровень – 3 |
| 4 | 3 | 1 уровень – 1, 2 уровень – 30, 3 уровень – 8 |
| 5 | 3 | 1 уровень – 7, 2 уровень – 24, 3 уровень – 11 |
| 6 | 2 | 1 уровень –9, 2 уровень – 14, 3 уровень – 15 |
| 7 | 2 | 1 уровень –19, 2 уровень – 6 |
| 8 | 3 | 1 уровень –17, 2 уровень – 19, 3 уровень – 4 |
| 9 | 4 | 1 уровень –27, 2 уровень – 13, 3 уровень – 18, 4 уровень – 5 |
| 10 | 3 | 1 уровень – 7, 2 уровень – 3, 3 уровень – 28 |
| 11 | 2 | 1 уровень –11, 2 уровень – 23 |
| 12 | 3 | 1 уровень – 27, 2 уровень – 12, 3 уровень – 6 |
| 13 | 4 | 1 уровень – 9, 2 уровень – 19, 3 уровень – 11, 4 уровень – 10 |
| 14 | 2 | 1 уровень –25, 2 уровень – 26 |
| 15 | 3 | 1 уровень – 11, 2 уровень – 19, 3 уровень – 24 |
| 16 | 3 | 1 уровень – 21, 2 уровень – 12, 3 уровень – 29 |
| 17 | 3 | 1 уровень – 1, 2 уровень – 22, 3 уровень – 27 |
| 18 | 2 | 1 уровень – 30, 2 уровень – 28 |
| 19 | 2 | 1 уровень – 8, 2 уровень – 17 |
| 20 | 4 | 1 уровень – 5, 2 уровень – 9, 3 уровень – 10, 4 уровень – 28 |
| 21 | 3 | 1 уровень – 17, 2 уровень – 13, 3 уровень – 18 |
| 22 | 4 | 1 уровень – 15, 2 уровень – 5, 3 уровень – 8, 4 уровень – 18 |
| 23 | 4 | 1 уровень – 14, 2 уровень – 15, 3 уровень – 18, 4 уровень – 28 |
| 24 | 2 | 1 уровень – 28, 2 уровень – 27 |
| 25 | 3 | 1 уровень – 13, 2 уровень – 12, 3 уровень – 8 |
| 26 | 3 | 1 уровень – 10, 2 уровень – 11, 3 уровень – 16 |
| 27 | 3 | 1 уровень – 7, 2 уровень – 6, 3 уровень – 15 |
| 28 | 4 | 1 уровень – 4, 2 уровень – 30, 3 уровень – 28, 4 уровень – 5 |
| 29 | 3 | 1 уровень – 27, 2 уровень – 6, 3 уровень – 9 |
| 30 | 3 | 1 уровень – 25, 2 уровень – 14, 3 уровень – 7 |

**Контрольные вопросы**

1. Атака на информационную систему.
2. Модель элементарной защиты информации.
3. Модель многозвенной защиты информации.
4. Модель многоуровневой защиты информации.

**Список литературы, рекомендуемый к использованию по данной теме.**
*Основная:* 1
*Дополнительная: 1, 2, 3, 4, 5, 6*
*Методическая литература: 1, 2*
*Интернет-ресурсы: 1, 2*

**Тема 3. Математическое моделирование**

Практическое занятие № 5

**Название работы:** Сложные системы
***Формируемые компетенции: УК-1***
**Теоретическая часть:**

**ОСНОВНЫЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ**

Парные игры с нулевой суммой. Решение в чистых стратегиях

*Пример 1.* Определите нижнюю и верхнюю цену игры, которая задана следующей платежной матрицей:

$$A=\begin{pmatrix} 0,5 & 0,6 & 0,8 \\ 0,9 & 0,7 & 0,8 \\ 0,7 & 0,6 & 0,6 \end{pmatrix}$$

*Решение.*

Выясним, имеет ли игра седловую точку. Решение удобно проводить в таблице. Таблица 1 включает платежную матрицу игры, а также дополнительные строку и столбец, которые иллюстрируют процесс поиска оптимальных стратегий.

Таблица 1 – Платежная матрица с дополнительными строкой и столбцом

| | $B_1$ | $B_2$ | $B_3$ | $\alpha_i$ |
|---|---|---|---|---|
| $A_1$ | 0,5 | 0,6 | 0,8 | 0,5 |
| $A_2$ | 0,9 | 0,7 | 0,8 | 0,7 |
| $A_3$ | 0,7 | 0,6 | 0,6 | 0,6 |
| $\beta_j$ | 0,9 | 0,7 | 0,8 | $\alpha=\beta=0,7$ |

Приведем некоторые пояснения.

Столбец $\alpha_i$ заполнен на основе анализа строк матрицы (стратегии игрока А): $\alpha_1 = 0,5$; $\alpha_2 = 0,7$; $\alpha_3 = 0,6$ – минимальные числа в строках.

Аналогично, $\beta_1 = 0,9$; $\beta_2 = 0,7$; $\beta_3 = 0,8$ – максимальные числа в столбцах.

Нижняя цена игры $\alpha=\max\limits_{i=1,2,3}\alpha_i = \max(0,5; 0,7; 0,6) = 0,7$ (наибольший элемент в столбце $\alpha_i$).

Верхняя цена игры $\beta=\min\limits_{j=1,2,3}\beta_j = \min(0,9; 0,7; 0,8) = 0,7$ (наименьший элемент в строке $\beta_j$). Эти значения равны, т.е. $\alpha=\beta$, и достигаются на паре стратегий $(A_2,B_2)$. Цена игры $v = 0,7$.

Таким образом, оптимальное решение состоит в выборе игроками А и В стратегий $A_2$ и $B_2$ соответственно.

Решение игр в смешанных стратегиях

Для игры с седловой точкой нахождение решения состоит в выборе максиминной и минимаксной стратегий, которые и являются оптимальными.

Если игра не имеет седловой точки, то применение чистых стратегий не дает оптимального решения игры. В этом случае можно получить оптимальное решение, чередуя

чистые стратегии.

Смешанной стратегией игрока А называется применение чистых стратегий $A_1$, $A_2$, …, $A_m$ с вероятностями $u_1$, $u_2$, …, $u_m$.

Обычно смешанную стратегию первого игрока обозначают как вектор: $U = (u_1, u_2, \ldots, u_m)$, а стратегию второго игрока как вектор: $Z = (z_1, z_2, \ldots, z_m)$.

Очевидно, что:

$u_i \geq 0$, $i = \overline{1,m}$,

$z_j \geq 0$, $j = \overline{1,n}$,

$\sum_{i=1}^{m} u_i = 1$, $\sum_{j=1}^{n} z_j = 1$.

Чистые стратегии можно считать частным случаем смешанных и задавать вектором, в котором единица соответствует чистой стратегии.

*Оптимальное решение игры* – это пара оптимальных стратегий $U^*$, $Z^*$, в общем случае смешанных, обладающих следующим свойством: если один из игроков придерживается своей оптимальной стратегии, то другому не может быть выгодно отступать от своей. Выигрыш, соответствующий оптимальному решению, называется *ценой игры* **v**. Цена игры удовлетворяет неравенству:

$\alpha \leq v \leq \beta$,

Справедлива следующая основная теорема теории игр.

*Теорема Неймана*. Каждая конечная игра с нулевой суммой имеет решение в смешанных стратегиях.

Такая игра является простейшим случаем конечной игры. Если такая игра имеет седловую точку, то оптимальное решение – это пара чистых стратегий, соответствующих этой точке.

Выигрыш игрока А (проигрыш игрока В) – случайная величина, математическое ожидание которой является ценой игры. Поэтому средний выигрыш игрока А (при использовании оптимальной стратегии) будет равен v и для первой, и для второй стратегии противника.

Пусть игра задача платежной матрицей:

$$Aa = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}.$$

Средний выигрыш игрока А, если он использует оптимальную смешанную стратегию $U^* = (u_1^*, u_2^*)$, а игрок В – чистую стратегию $B_1$ (что соответствует первому столбцу платежной матрицы), равен цене игры v, т.е.:

$$a_{11} u_1^* + a_{21} u_2^* = v.$$

Тот же средний выигрыш получает игрок А, если противник применяет стратегию $B_2$, т.е. $a_{12} u_1^* + a_{22} u_2^* = v$. Учитывая, что $u_1^* + u_2^* = 1$, получим систему уравнений:

$$\begin{cases} a_{11} u_1^* + a_{21} u_2^* = v, \\ a_{12} u_1^* + a_{22} u_2^* = v, \\ u_1^* + u_2^* = 1. \end{cases} \quad (1)$$

Решая систему (1), можно найти оптимальную стратегию $U^*$ и цену игры v.

Аналогичная система уравнений может быть получена для определения оптимальной стратегии игрока В:

(2)

$$\begin{cases} a_{11}z_1^* + a_{12}z_2^* = v, \\ a_{21}z_1^* + a_{22}z_2^* = v, \\ z_1^* + z_2^* = 1. \end{cases}$$

*Пример 2*. Найдите решение игры, заданной платежной матрицей:

$$A = \begin{pmatrix} 2 & 5 \\ 6 & 4 \end{pmatrix}$$

*Решение.*

Прежде всего, проверим наличие седловой точки. Для этого найдем минимальные элементы в каждой из строк (2 и 4) и максимальные в каждом из столбцов (6 и 5). Таким образом, нижняя цена игры $\alpha = \max(2, 4) = 4$, верхняя цена игры $\beta = \min(6, 5) = 5$. Поскольку $\alpha \neq \beta$, решение игры следует искать в смешанных стратегиях, при этом цена игры находится в следующих пределах: $4 \le v \le 5$.

Предположим, что для игрока А стратегия задается вектором $U = (u_1, u_2)$. Тогда на основании теоремы об активных стратегиях можно записать систему уравнений:

$$\begin{cases} 2u_1^* + 6u_2^* = v, \\ 5u_1^* + 4u_2^* = v, \\ u_1^* + u_2^* = 1. \end{cases}$$

Решая систему из трех уравнений с тремя неизвестными, получим: $u_1^* = 2/5$, $u_2^* = 3/5$, $v = 22/5$.

Теперь найдем оптимальную стратегию игрока В. Пусть стратегия данного игрока задается вектором $Z = (z_1, z_2)$. Система уравнений (2), основанная на использовании теоремы об активных стратегиях, запишется следующим образом:

$$\begin{cases} 2z_1^* + 5z_2^* = 22/5, \\ 6z_1^* + 4z_2^* = 22/5, \\ z_1^* + z_2^* = 1. \end{cases}$$

Решая систему, состоящую из любых двух уравнений, взятых из последней системы, получим $z_1^* = 1/5$, $z_2^* = 4/5$.

Следовательно, решением игры примера 2 являются смешанные стратегии: $U^* = (2/5, 3/5)$, $Z^* = (1/5, 4/5)$, цена игры $v = 22/5$.

Геометрическая интерпретация игр

Решение игр размера *2xn* или *nx2* допускает наглядную геометрическую интерпретацию. Такие игры можно решать графически.

Дадим геометрическую интерпретацию игры, рассмотренной выше в рамках примера 2.

На плоскости XY по оси абсцисс отложим единичный отрезок $A_1A_2$ (рисунок 1). Каждой точке отрезка поставим в соответствие некоторую смешанную стратегию $U = (u_1, u_2)$. Причем расстояние от некоторой промежуточной точки U до правого конца этого отрезка – это вероятность $u_1$ выбора стратегии $A_1$, расстояние до левого конца – вероятность $u_2$ выбора стратегии $A_2$. Точка $A_1$ соответствует чистой стратегии $A_1$, точка $A_2$ – чистой стратегии $A_2$.

В точках $A_1$ и $A_2$ восстановим перпендикуляры и будем откладывать на них выигрыши игроков. На первом перпендикуляре (совпадающем с осью OY) покажем выигрыш игрока А при использовании стратегии $A_1$, на втором – при использовании стратегии $A_2$. Если игрок А применяет стратегию $A_1$, то его выигрыш при стратегии $B_1$ игрока В равен 2, а при стратегии

$B_2$ он равен 5. Числам 2 и 5 на оси OY соответствуют точки $B_1$ и $B_2$. Аналогично на втором перпендикуляре найдем точки $B'_1$ и $B'_2$ (выигрыши 6 и 4).

Соединяя между собой точки $B_1$ и $B'_1$, $B_2$ и $B'_2$, получим две прямые, расстояние от которых до оси OX определяет средний выигрыш при любом сочетании соответствующих стратегий.

Например, расстояние от любой точки отрезка $B_1B'_1$ до оси OX определяет средний выигрыш игрока A при любом сочетании стратегий $A_1$ и $A_2$ (с вероятностями $u_1$ и $u_2$) и стратегии $B_1$ игрока B.

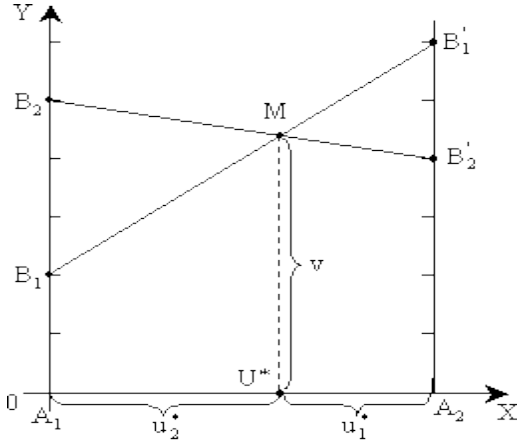



Рисунок 1 – Геометрическая интерпретация игры примера 2
(нахождение оптимальной стратегии игрока A)

Ординаты точек, принадлежащих ломаной $B_1MB'_2$ определяют минимальный выигрыш игрока A при использовании им любых смешанных стратегий. Эта минимальная величина является наибольшей в точке M, следовательно, этой точке соответствует оптимальная стратегия $U^* = (u_1^*, u_2^*)$, а ее ордината равна цене игры v.

Координаты точки M найдем, как координаты точки пересечения прямых $B_1B'_1$ и $B_2B'_2$.

Для этого необходимо знать уравнения прямых. Составить такие уравнения можно, используя формулу для уравнения прямой, проходящей через две точки:

$$\frac{x - x_1}{x_2 - x_1} = \frac{y - y_1}{y_2 - y_1}$$

Составим уравнения прямых для нашей задачи.

Прямая $B_1B'_1$:

$$\frac{x - 0}{1 - 0} = \frac{y - 2}{6 - 2} \quad \text{или} \quad y = 4x + 2.$$

Прямая $B_2B'_2$:

$$\frac{x - 0}{1 - 0} = \frac{y - 5}{4 - 5} \quad \text{или} \quad y = -x + 5.$$

Получим систему:

$$\begin{cases} y = 4x + 2, \\ y = -x + 5. \end{cases}$$

Решим ее:

$$4x + 2 = -x + 5,$$
$$5x = 3,$$
$$x = 3/5,\ y = -3/5 + 5 = 22/5.$$

Таким образом, $U^* = (2/5, 3/5)$, $v = 22/5$.

Аналогично решается задача по нахождению оптимальной стратегии игрока B. Разница состоит в том, что находится точка, сводящая к минимуму средний проигрыш, поэтому на

рисунке 5.2 рассматривается ломаная $A_2MA'_1$.

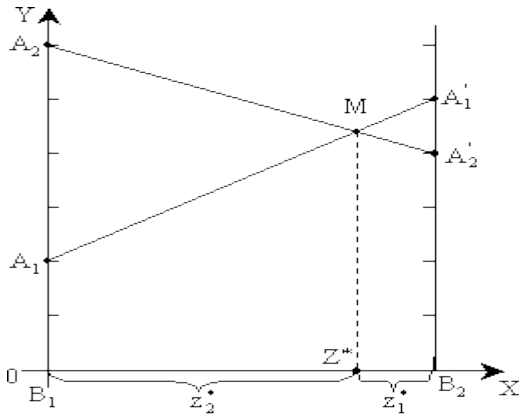



Рисунок 2 – Геометрическая интерпретация игры примера 2(нахождение оптимальной стратегии игрока В)

Найдем координаты точки М.

Прямая $A_1A'_1$:

$\frac{x}{1} = \frac{y-2}{5-2}$, откуда $y = 3x + 2$.

Прямая $A_2A'_2$:

$\frac{x}{1} = \frac{y-6}{4-6}$, откуда $y = -2x + 6$,

$3x + 2 = -2x + 6,$

$5x = 4,$

$x = 4/5.$

Таким образом, $z_1^* = 1/5$, $z_2^* = 4/5$.

В общем случае схема решения игры *2xn* или *mx2* графическим методом состоит в следующем.

1. Строят прямые, соответствующие стратегиям второго (первого) игрока.

2. Находят две стратегии второго (первого) игрока, которым соответствуют две прямые, пересекающиеся в точке с максимальной (минимальной) ординатой. Эти стратегии являются активными в оптимальной смешанной стратегии второго (первого) игрока.

3. Находят координаты точки пересечения, тем самым определяя оптимальную стратегию первого (второго) игрока и цену игры.

4. Оптимальную стратегию другого игрока находят, решая систему уравнений, включающую его активные стратегии.

## ПРАКТИЧЕСКАЯ ЧАСТЬ

**Задание.** Составить платежную матрицу $G = \|p_{ik} \cdot c_k\|$ и решить игру.

*Вариант 1*

Пусть в рассмотрении владельца ИС имеется проекты построения системы защиты информации: $x_i$, $i = 1,...,5$. Известны типы злоумышленников $d_k$, $k = 1,...,6$. Получены вероятности столкновения с определенным типом злоумышленника при той или иной стратегии владельца ИС:

$$P = \begin{pmatrix} 0,4 & 0,35 & 0,33 & 0,21 & 0,25 & 0,54 \\ 0,5 & 0,14 & 0,15 & 0,5 & 0,27 & 0,19 \\ 0,27 & 0,34 & 0,33 & 0,26 & 0,28 & 0,51 \\ 0,43 & 0,15 & 0,17 & 0,12 & 0,39 & 0,38 \\ 0,49 & 0,12 & 0,31 & 0,25 & 0,33 & 0,44 \end{pmatrix}$$

Объемы потерь от реализации угрозы $k$-ым типом злоумышленника: $C_1 = 1500$ руб., $C_2 = 2400$, $C_3 = 1450$ руб, $C_4 = 20000$, $C_5 = 3500$, $C_6 = 1200$ руб.

*Вариант 2*

Пусть в рассмотрении владельца ИС имеется проекты построения системы защиты информации: $x_i$, $i = 1,...,5$. Известны типы злоумышленников $d_k$, $k = 1,...,6$. Получены вероятности столкновения с определенным типом злоумышленника при той или иной стратегии владельца ИС:

$$P = \begin{pmatrix} 0,21 & 0,35 & 0,33 & 0,21 & 0,25 & 0,54 \\ 0,5 & 0,32 & 0,45 & 0,45 & 0,27 & 0,49 \\ 0,27 & 0,34 & 0,33 & 0,26 & 0,28 & 0,51 \\ 0,43 & 0,15 & 0,17 & 0,51 & 0,39 & 0,38 \\ 0,19 & 0,12 & 0,67 & 0,25 & 0,33 & 0,44 \end{pmatrix}$$

Объемы потерь от реализации угрозы $k$-ым типом злоумышленника: $C_1 = 1410$ руб., $C_2 = 18900$, $C_3 = 1450$ руб, $C_4 = 2000$, $C_5 = 2500$, $C_6 = 1200$ руб.

*Вариант 3*

Пусть в рассмотрении владельца ИС имеется проекты построения системы защиты информации: $x_i$, $i = 1,...,5$. Известны типы злоумышленников $d_k$, $k = 1,...,6$. Получены вероятности столкновения с определенным типом злоумышленника при той или иной стратегии владельца ИС:

$$P = \begin{pmatrix} 0,11 & 0,35 & 0,33 & 0,21 & 0,15 & 0,54 \\ 0,5 & 0,72 & 0,45 & 0,45 & 0,27 & 0,18 \\ 0,22 & 0,34 & 0,33 & 0,26 & 0,28 & 0,32 \\ 0,13 & 0,15 & 0,17 & 0,26 & 0,39 & 0,38 \\ 0,19 & 0,12 & 0,67 & 0,12 & 0,33 & 0,27 \end{pmatrix}$$

Объемы потерь от реализации угрозы $k$-ым типом злоумышленника: $C_1 = 13500$ руб., $C_2 = 2140$, $C_3 = 1650$ руб, $C_4 = 1000$, $C_5 = 3000$, $C_6 = 1100$ руб.

## Контрольные вопросы

1. Конфликтная ситуация.
2. Игры с нулевой суммой.
3. Платежная матрица.
4. Стратегия игры. Чистые стратегии.
5. Седловая точка.
6. Смешанные стратегии.
7. Теорема Неймана.
8. Графическое решение игр *2xn* или *mx2.*

**Список литературы, рекомендуемый к использованию по данной теме.**

*Основная:* 1

*Дополнительная: 1, 2, 3, 4, 5, 6*

*Методическая литература: 1, 2*

*Интернет-ресурсы: 1, 2*

**Тема 4. Имитационное моделирование**

Практическое занятие № 6

**Название работы:** Оценка эффективности систем контроля и управления доступом на основе детерминистического подхода

**Формируемые компетенции:** УК-1

**Теоретическая часть:**

## ОСНОВНЫЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Детерминистический подход к оценке эффективности систем контроля и управления доступом (СКУД) связан с заданием и последующей проверкой обязательных требований, содержащихся в ведомственных руководящих документах, техническом задании на проектирование, рабочем проекте. Этот подход предполагает проведение комплексных проверок (инспекций), например, органами государственного надзора или ведомственного контроля. Такие проверки могут проводиться с различной регулярностью (плановые проверки), а кроме того – при изменении перечня угроз объекту, модернизации СКУД и в ряде других случаев (внеплановые проверки). Контролю при этом подвергаются организационные мероприятия, комплекс инженерно-технических средств охраны, действия персонала службы безопасности. Для этого разрабатываются опросные листы, содержащие формализованные перечни требований по организации доступа на объекте, в том числе по оснащению периметра объекта, его зданий, сооружений инженерно-техническими средствами охраны, по оценке состояния личного состава службы безопасности, по наличию и качеству проводимых организационных мероприятий. По своему характеру этот метод является экспертным. Процедура экспертного оценивания может быть построена по-разному. В одних случаях результаты могут интерпретироваться на качественном уровне, в других, на основании полученных данных, могут конструироваться интегральные критерии, отражающие состояние СКУД объекта в целом. В качестве конкретной реализации данного подхода рассмотрим разработанный в Госатомнадзоре экспертный метод оценки состояния физической защиты (РД-07-01-2004 «Методические указания по проведению оценки состояния физической защиты ядерно- и радиационно-опасных объектов по результатам проведенной инспекции»). Целями оценки состояния являются:

– проверка соответствия физической защиты предъявляемым к ней требованиям;

– выявление элементов, не соответствующих требованиям к физической защите (т.н. «критических элементов» СКУД).

Для этого разработана целая система факторов состояния (ФС), которые определяют организацию и обеспечение физической защиты в соответствии с требованиями нормативных документов. В том числе различают:

– ФС организационных мероприятий (группа a);

– ФС инженерно-технических средств охраны (группа b);

– ФС действий подразделений охраны (группа c).

Процедура оценки следующая:

1. Эксперт выбирает некоторое количество ФС по группам a,b,c соответственно. Каждому ФС каждый эксперт назначает определенный «вес».

2. Каждому ФС эксперты дают оценку степени реального состояния ФС ($d_{ij}$= *0*, 1, 2, 3).

3. Определяется среднее значение показателя реального состояния каждого ФС $d_i$:

$$d_i = \frac{\Sigma_{j-1}^{n} d_i}{n} \qquad ((1)$$

где $d_{ij}$ – показатель реального состояния *i*-го ФС, назначенного *j*-м экспертом; *n* – число экспертов.

7. Состояние СКУД объекта в целом оценивается следующим образом (табл. 1):

– члены комиссии определяют значения средних весов ФС $a_i$, $b_i$, $c_i$ аналогично $d_i$;

– определяются показатели состояния составных частей физической защиты $N_1$, $N_2$, $N_3$;

– за показатель состояния физической защиты принимается среднее арифметическое

значений $N_1$, $N_2$, $N_3$.

Таблица 1 – Оценки показателей состояния составных частей СКУД

| Показатель состояния: | Формула для его оценки: |
|---|---|
| организационных мероприятий | $N_1 = \frac{\sum_{i-1}^{k} a_i d_i}{d_m k a_m}$ |
| инженерно-технических средств | $N_2 = \frac{\sum_{i-1}^{l} b_i d_i}{d_m l b_m}$ |
| действий подразделений охраны | $N_3 = \frac{\sum_{i-1}^{m} c_i d_i}{d_m m c_m}$ |
| k – число ФС в организационных мероприятиях;<br>l – число ФС в инженерно-технических средствах ФЗ;<br>m – число ФС в действиях подразделений охраны;<br>$d_m$ – максимально возможное значение показателя реального состояния ФС ($d_m = 3$);<br>$a_m$, $b_m$, $c_m$ – максимально возможные значения весов ФС в группе ФС (5, 6, 4 соответственно). | |

Интерпретация результатов оценки приведена в таблице 2.

Таблица 2 – Интерпретация результатов оценки состояния физической защиты

| *Значение показателя состояния N:* | *Соответствие ФЗ требованиям:* |
|---|---|
| $N \leq 0,05$ | ФЗ в основном соответствует требованиям норм и правил |
| $0,05 < N < 0,07$ | ФЗ имеет отдельные отступления от требований норм и правил |
| $0,07 < N < 0,1$ | Имеет значительные отступления от требований норм и правил, требующие использования компенсирующих мероприятий |
| $N \geq 0,1$ | ФЗ не обеспечивается |

3. С помощью данного метода можно судить, насколько полно выполняются требования к СКУД на конкретном объекте. Однако он не позволяет учитывать такие факторы, как правильность установки и настройки технических средств охраны, просчеты в применении сил охраны объекта и др. Свою роль может сыграть и недостаточная компетентность экспертов. Поэтому даже отвечающая всем требованиям СКУД в реальных условиях может оказаться неспособной решать поставленные перед ней задачи.

## ПРАКТИЧЕСКАЯ ЧАСТЬ

Оцените эффективность СКУД на основе детерминистического подхода, используя данные, приведённые ниже. Сделайте вывод о соответствии физической защиты требованиям норм и правил согласно таблице 2.

ФС организационных мероприятий

1. Наличие инструкций на все возможные нештатные ситуации при функционировании СКУД.
2. Обученность сотрудников охраны действиям при нарушении контрольно-пропускного режима.
3. Регулярное обновление модели угроз и модели нарушителя.
4. Организация отлаженной системы выдачи, смены и отзыва пропусков.

5. Знание сотрудниками организации регламента по получению доступа в различные помещения предприятия.

ФС инженерно-технических средств охраны

1. Наличие ограды территории.
2. Наличие контрольно-пропускных пунктов для атвотранспорта и персонала.
3. Наличие системы обнаружения попытки несанкционированного доступа на территорию предприятия.
4. Наличие системы видеонаблюдения.
5. Наличие единой компьютерной базы данных пропусков и времени посещения территории предприятия.
6. Наличие на территории предприятия зон с различным уровнем допуска.

ФС действий подразделений охраны

1. Своевременное реагирование на сигналы тревоги.
2. Организация непрерывного посменного дежурства на постах охраны.
3. Неукоснительное соблюдение всех инструкций по реагированию на нештатные ситуации.
4. Разъяснение персоналу предприятия и посетителям особенностей доступа на территорию предприятия и в его различные зоны.

Таблица 3 – Экспертная оценка степени реального состояния ФС организационных мероприятий

| Эксперты | ФС организационных мероприятий | | | | |
|---|---|---|---|---|---|
| | *1* | *2* | *3* | *4* | *5* |
| Эксп. 1 | 3 | 2 | 0 | 3 | 1 |
| Эксп. 2 | 2 | 2 | 0 | 2 | 2 |
| Эксп. 3 | 3 | 3 | 0 | 3 | 2 |
| Эксп. 4 | 1 | 3 | 1 | 3 | 1 |

Таблица 4 – Экспертная оценка «веса» ФС организационных мероприятий

| Эксперты | ФС организационных мероприятий | | | | |
|---|---|---|---|---|---|
| | *1* | *2* | *3* | *4* | *5* |
| Эксп. 1 | 5 | 2 | 1 | 4 | 3 |
| Эксп. 2 | 5 | 4 | 1 | 2 | 3 |
| Эксп. 3 | 4 | 3 | 2 | 1 | 5 |
| Эксп. 4 | 3 | 4 | 1 | 2 | 5 |

Таблица 5 – Экспертная оценка степени реального состояния ФС инженерно-технических средств охраны

| Эксперты | ФС инженерно-технических средств охраны | | | | | |
|---|---|---|---|---|---|---|
| | *1* | *2* | *3* | *4* | *5* | *6* |
| Эксп. 1 | 1 | 1 | 2 | 3 | 1 | 3 |
| Эксп. 2 | 1 | 2 | 2 | 2 | 2 | 2 |
| Эксп. 3 | 2 | 1 | 3 | 3 | 2 | 2 |
| Эксп. 4 | 1 | 1 | 1 | 2 | 1 | 2 |

Таблица 6 – Экспертная оценка «веса» ФС инженерно-технических средств охраны

| Эксперты | ФС инженерно-технических средств охраны | | | | | |
|---|---|---|---|---|---|---|
| | *1* | *2* | *3* | *4* | *5* | *6* |
| Эксп. 1 | 1 | 2 | 4 | 5 | 3 | 6 |
| Эксп. 2 | 2 | 1 | 4 | 6 | 3 | 5 |
| Эксп. 3 | 1 | 2 | 5 | 6 | 4 | 3 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Эксп. 4 | 1 | 3 | 6 | 5 | 4 | 2 |

Таблица 7 – Экспертная оценка степени реального состояния ФС действий подразделений охраны

| Эксперты | ФС действий подразделений охраны | | | |
|---|---|---|---|---|
| | *1* | *2* | *3* | *4* |
| Эксп. 1 | 2 | 2 | 2 | 2 |
| Эксп. 2 | 1 | 2 | 2 | 3 |
| Эксп. 3 | 2 | 3 | 3 | 0 |
| Эксп. 4 | 1 | 3 | 3 | 1 |

Таблица 8 – Экспертная оценка «веса» ФС действий подразделений охраны

| Эксперты | ФС действий подразделений охраны | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| Эксп. 1 | 1 | 3 | 2 | 4 |
| Эксп. 2 | 2 | 3 | 1 | 4 |
| Эксп. 3 | 2 | 4 | 1 | 3 |
| Эксп. 4 | 1 | 4 | 2 | 3 |

**Контрольные вопросы**

1. Система контроля и управления доступом.
2. Факторы состояния системы контроля и управления доступом.
3. Показатели состояния системы контроля и управления доступом.
4. Организационные мероприятия.
5. Инженерно-технические средства охраны.

**Список литературы, рекомендуемый к использованию по данной теме.**

*Основная:* 1
*Дополнительная: 1, 2, 3, 4, 5, 6*
*Методическая литература: 1, 2*
*Интернет-ресурсы: 1, 2*

Практическое занятие № 7

**Название работы:** Оценка эффективности охраны объекта с помощью метода имитационного моделирования

**Формируемые компетенции:** УК-1

**Теоретическая часть:**

## ОСНОВНЫЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Вероятностный подход к анализу базируется на предположениях о случайности и независимости временных параметров в системе «охрана-нарушитель». Эффективность здесь понимается как вероятность пресечения несанкционированных действий нарушителя:

$P_{ïðåñ} = Ð_{îáí} \cdot Ð_{íåéòð}$ , где $Ð_{îáí}$ – вероятность обнаружения нарушителя; $Ð_{íåéòð}$ – вероятность нейтрализации нарушителя.

Как оценить эти вероятности? Один из методов – имитационное моделирование. Это вычислительный эксперимент, основанный на том известном факте, что при увеличении числа испытаний n относительная частота $W = \frac{m}{n}$ появления случайного события А в серии испытаний стремится к его вероятности в единичном испытании $W \Rightarrow p(A)$ при $n \Rightarrow \infty$. С помощью генератора случайных чисел получают выборки случайных величин, распределенных по известному закону с известными математическим ожиданием и дисперсией. Приведем пример. Периметр объекта оборудован системой охранной сигнализации с вероятностью обнаружения $Ð_{îáí} = 0{,}95$. Для имитационного моделирования работы такой системы «разыгрывается» равномерно распределенное случайное число $\hat{e}$ от 0 до 1. Если $\hat{e} \le 0{,}95$ система сработала, в противном случае – нет. Таким же образом моделируется время движения сил охраны и нарушителя и другие случайные процессы в функционировании СКУД.

Каждая конфликтная ситуация в функционировании СКУД просчитывается много раз, по результатам набирается статистика захватов нарушителя. Эффективность СКУД оценивается статистически, как отношение числа захватов к общему числу испытаний. Количество опытов определяется исходя из того, что при заданной доверительной вероятности необходимо обеспечить требуемую точность оценки.

## ПРАКТИЧЕСКАЯ ЧАСТЬ

Используя метод имитационного моделирования, оцените эффективность охраны объекта для следующих ситуаций:

1. Несанкционированное проникновение на внутренний двор предприятия с целью похищения пропуска из автомашины.
2. Несанкционированное проникновение в производственный цех предприятия с целью кражи образцов продукции.
3. Несанкционированное проникновение в кабинет финансового директора предприятия с целью кражи договоров о поставщиках. Для доступа в кабинет необходимо пройти по коридору здания.
4. Санкционированное проникновение во внутренний двор предприятия с последующим несанкционированным проникновением в кабинет генерального директора с целью кражи правоустанавливающих документов.

Таблица 1 – Вероятность обнаружения преодоления рубежей охраны

| Рубеж охраны | Вероятность обнаружения преодоления рубежа, $P_{обн}$ |
|---|---|
| Ограда территории | 0,86 |
| Внутренний двор | 0,9 |
| Производственный цех | 0,5 |
| Коридор здания управления | 0,93 |

| | |
|---|---|
| Кабинет финансового директора | 0,95 |
| Кабинет генерального директора | 0,97 |
| Контрольно-пропускной пункт | 0,99 |

Таблица 2 – Вероятность пресечения несанкционированного доступа на рубеже охраны

| Рубеж охраны | Вероятность пресечения НСД на рубеже, $P_{прес}$ |
|---|---|
| Ограда территории | 0,2 |
| Внутренний двор | 0,5 |
| Производственный цех | 0,3 |
| Коридор здания управления | 0,7 |
| Кабинет финансового директора | 0,9 |
| Кабинет генерального директора | 0,95 |
| Контрольно-пропускной пункт | 0,99 |

## Контрольные вопросы

1. Метод имитационного моделирования.
2. Вероятность обнаружения нарушителя.
3. Вероятность нейтрализации нарушителя.
4. Санкционированное проникновение на охраняемый объект.
5. Несанкционированное проникновение на охраняемый объект.
6. Эффективность охраны объекта.

**Список литературы, рекомендуемый к использованию по данной теме.**

*Основная:* 1
*Дополнительная: 1, 2, 3, 4, 5, 6*
*Методическая литература: 1, 2*
*Интернет-ресурсы: 1, 2*

Практическое занятие № 8

**Название работы:** Оценка уровня безопасности информационной системы предприятия на базе модели с нечеткой лингвистической шкалой

**Формируемые компетенции:** УК-1

**Теоретическая часть:**

## ОСНОВНЫЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Рассмотрим нечеткую модель с лингвистической шкалой, схема модели представлена в таблице 1. Модель используется для определения состояния безопасности информационной системы, по результатам опроса пользователей согласно составленного экспертами запроса

Таблица 1 – Методика нечеткой лингвистической оценки уровня безопасности информационной системы предприятия

| Этапы | Содержание этапа |
|---|---|
| Этап 1 | Выделение основных направлений защиты информации |
| Этап 2 | Определение списка основных угроз информационной безопасности для предприятия |
| Этап 3 | На основе выделенных направлений защиты и составленного списка угроз разработка опросников «Самооценка комплекса реализованных превентивных мер защиты» для пользователей информационной системы предприятия. Ответы пользователей будут представлены в виде лингвистических переменных: «почти никогда», «редко», «не редко и не часто», «часто», «почти всегда». |
| Этап 4 | Разработка нечетких эталонов для термов лингвистической переменной «Уровень безопасности»: Низкий (Н), Ниже среднего (НС), Средний (С), Выше среднего (ВС), Высокий (В). |
| Этап 5 | Заполнение опросников «Самооценка комплекса реализованных превентивных мер защиты» пользователями информационной системы, обработка результатов и получение суммарной нечеткой оценки комплекса реализованных превентивных мер защиты |
| Этап 6 | Сравнение полученных суммарных нечетких оценок комплекса реализованных превентивных мер защиты по каждому из основных направлений защиты с нечеткими эталонами лингвистической переменной «Уровень безопасности». Вывод о достаточности мер по защите информации и уровне безопасности информационной системы предприятия |

*Методические рекомендации по применению методики нечеткой лингвистической оценки уровня безопасности информационной системы предприятия:*

**Этап 1**

В качестве основных направлений защиты информации можно выделить:

– организационная защита,

– компьютерная защита;

– физическая защита.

**Этап 2**

Пример составленного списка основных угроз информационной безопасности для предприятия приведен в таблице 2.

Таблица 2 – Список основных угроз информационной безопасности для предприятия

| № п/п | Класс угроз | Способ распространения |
|---|---|---|
| 1 | | Заражение через файл, скаченный из глобальной сети «Internet» |
| | | Заражение через файл, скаченный с FTP сервера |
| | | Заражение через нелицензионное программное |

| | | |
|---|---|---|
| | Компьютерные вирусы | обеспечение |
| | | Заражение через Flash-накопители |
| | | Заражение через электронную почту |
| | | Заражение через системы обмена мгновенными сообщениями |
| | | Заражение через Web-страницы |
| 2 | Непреднамеренные действия персонала | Порча оборудования, носителей информации |
| | | Искажение файлов с важной информацией |
| | | Изменение режимов работы устройств и программ |
| | | Запуск неучтенных программ, системных служб |
| | | Разглашение конфиденциальной информации |
| | | Разглашение, передача или утрата атрибутов разграничения доступа (паролей, пропусков и т.д.) |
| | | Игнорирование организационных ограничений |
| | | Некомпитентное использование, настройка или неправомерное отключение средств защиты информации |
| | | пересылка данных по ошибочному адресу абонента (устройства) |
| | | Ввод ошибочных данных |
| | | Повреждение каналов связи |
| 3 | Преднамеренные действия персонала | Физическое разрушение системы или наиболее важных компонентов |
| | | Отключение или вывод из строя систем обеспечения функционирования (электропитание, охлаждение и т.д.) |
| | | Изменение режимов работы устройств или программ |
| | | Хищение носителей информации |
| | | Несанкционированное копирование носителей информации |
| | | Хищение производственных отходов (распечаток, записей и т.д.) |
| | | Несанкционированное использование терминалов пользователей |
| | | Незаконное получение реквизитов разграничения доступа |
| 4 | Сетевые атаки | Переполнение буфера (buffer overflows) |
| | | Перехват пакетов в локальной сети (сниффер пакетов) |
| | | Вставка ложной информации или вредоносных команд в обычный поток данных (IP-спуфинг) |
| | | Отказ в обслуживании (Denial of Service (DoS)) |
| | | Перебор паролей (brute force attack) |
| | | Отключение систем защиты |
| 5 | Кражи и чрезвычайные ситуации | Воровство активов |
| | | Несчастные случаи с персоналом |
| | | Пожар |
| | | Землетрясение |
| | | Наводнение |

**Этап 3**

Примеры разработанных опросников «Самооценка комплекса реализованных превентивных мер защиты» приведены в таблицах 3, 4, 5.

Таблица 3 – Опросник «Оценка реализованных превентивных мер по организационной защите информации»

| № п/п | Компонент запроса | Варианты ответов пользователя | | | | |
|---|---|---|---|---|---|---|
| | | Почти никогда | Редко | Не часто и не редко | Часто | Почти всегда |
| 1 | Проводятся ли совещания руководства касательно защиты информации в организации? | | | | | |
| 2 | Получаются ли консультации по защите информации от внешних специалистов? | | | | | |
| 3 | Поддерживаются ли контакты с правоохранительными органами? | | | | | |
| 4 | Оцениваются ли риски информационной безопасности в организации? | | | | | |
| 5 | Проводится ли аудит организационных мер на соответствие политике безопасности принятой на предприятии? | | | | | |
| 6 | Проводится ли информирование персонала по вопросам информационной безопасности? | | | | | |

Таблица 4 – Опросник «Оценка реализованных превентивных мер по использования средств защиты информации в компьютерной системе»

| № п/п | Компонент запроса | Варианты ответов пользователя | | | | |
|---|---|---|---|---|---|---|
| | | Почти никогда | Редко | Не часто и не редко | Часто | Почти всегда |
| 1 | Сохраняются ли свежие копии данных за пределами организации? | | | | | |
| 2 | Часто ли выполняется резервное копирование? | | | | | |
| 3 | Проводится ли антивирусный контроль? | | | | | |
| 4 | Всегда ли удаляются ненужные или устарелые файлы? | | | | | |

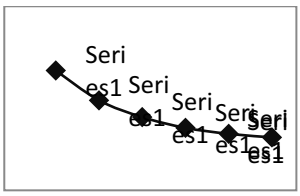
| | | | | | | |
|---|---|---|---|---|---|---|
| 5 | Используются ли средства криптографической защиты? | | | | | |
| 6 | Применяются в организации персональные межсетевые экраны? | | | | | |

Таблица 5 – Опросник «Оценка реализованных превентивных мер физической защиты информации»

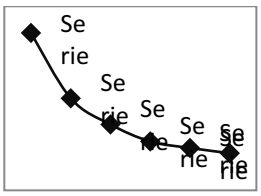
| № п/п | Компонент запроса | Варианты ответов пользователя | | | | |
|---|---|---|---|---|---|---|
| | | Почти никогда | Редко | Не часто и не редко | Часто | Почти всегда |
| 1 | Как часто применяются методы защиты для предотвращения утечки информации по телекоммуникационным и сетевым кабелям? | | | | | |
| 2 | Используются ли системы обнаружения проникновения на дверях, окнах, в рабочих помещениях? | | | | | |
| 3 | Часто ли пересматриваются доступ пользователей к ресурсам в охраняемом периметре? | | | | | |
| 4 | Используются ли процедуры аутентификации? | | | | | |
| 5 | Применяются ли средства защиты для оборудования организации? | | | | | |
| 6 | Проводятся ли проверки на наличие несанкционированных подключений к линиям связи? | | | | | |

**Этап 4**

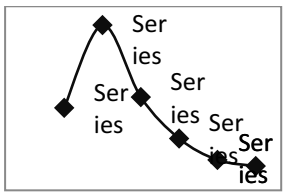
Нечеткие эталоны могут иметь вид (см. рис.1).



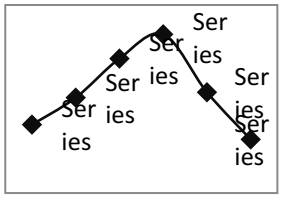
а) терм «Низкий»



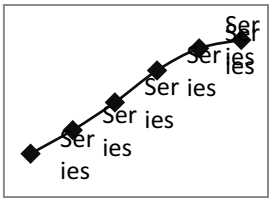
б) терм «Ниже среднего»



в) терм «Средний»



г) терм «Выше среднего»



д) терм «Высокий»

Рисунок 1 – Нечеткие эталоны лингвистической переменной «Уровень безопасности»

Таблица 6 – Числовые значения нечетких эталонов лингвистической переменной «Уровень безопасности»

| **Терм** | **1** | **2** | **3** | **4** | **5** | **6** |
|---|---|---|---|---|---|---|
| Н | 0,62 | 0,37 | 0,23 | 0,14 | 0,09 | 0,06 |
| НС | 1,00 | 0,50 | 0,30 | 0,17 | 0,12 | 0,08 |
| С | 0,46 | 1,00 | 0,53 | 0,26 | 0,12 | 0,08 |
| ВС | 0,31 | 0,51 | 0,80 | 0,98 | 0,55 | 0,20 |
| В | 0,12 | 0,29 | 0,49 | 0,72 | 0,88 | 0,94 |

**Этап 5**

Пользователями информационной системы заполняются опросники «Самооценка комплекса реализованных превентивных мер защиты» по выделенным основным направлениям защиты информации. Каждый пользователь в соответствующем Опроснике выбирает только 1 ответ: «почти никогда», «редко», «не редко не часто», «часто», «почти всегда». В таблице 7 приведен пример результата опроса по одному из основных направлений защиты информации.

Таблица 7 – Результат опроса 10 пользователей

| Номер вопроса | Количество пользователей, заполнивших опросники | | | | |
|---|---|---|---|---|---|
| | Почти никогда | Редко | Не часто и не редко | Часто | Почти всегда |
| 1 | | 6 | 4 | | |
| 2 | | | | 9 | 1 |
| 3 | | | | 7 | 3 |
| 4 | | 4 | 5 | 1 | |
| 5 | | | | | 10 |
| 6 | | | 3 | 4 | 3 |

Ответу «Почти никогда» соответствует терм «Низкий», ответу «Редко» – терм «Ниже среднего», ответу «Не часто и не редко» – терм «Средний», ответу «Часто» – терм «Выше среднего», ответу «Почти всегда» – терм «Высокий».

Получение нечетких оценок по каждому вопросу Опросника:

Вопрос 1:

| **Терм** | **1** | **2** | **3** | **4** | **5** | **6** | Доля пользователей |
|---|---|---|---|---|---|---|---|
| НС | 1,00 | 0,50 | 0,30 | 0,17 | 0,12 | 0,08 | 0,6 |
| С | 0,46 | 1,00 | 0,53 | 0,26 | 0,12 | 0,08 | 0,4 |
| Результат 0,6×НС+0,4×С | 0,78 | 0,70 | 0,39 | 0,21 | 0,12 | 0,08 | |

Вопрос 2:

| **Терм** | **1** | **2** | **3** | **4** | **5** | **6** | Доля пользователей |
|---|---|---|---|---|---|---|---|
| ВС | 0,31 | 0,51 | 0,80 | 0,98 | 0,55 | 0,20 | 0,9 |
| В | 0,12 | 0,29 | 0,49 | 0,72 | 0,88 | 0,94 | 0,1 |
| Результат 0,9×ВС+0,1×В | 0,29 | 0,49 | 0,77 | 0,95 | 0,58 | 0,27 | |

Вопрос 3:

| **Терм** | **1** | **2** | **3** | **4** | **5** | **6** | Доля пользователей |
|---|---|---|---|---|---|---|---|
| ВС | 0,31 | 0,51 | 0,80 | 0,98 | 0,55 | 0,20 | 0,7 |
| В | 0,12 | 0,29 | 0,49 | 0,72 | 0,88 | 0,94 | 0,3 |
| Результат 0,7×ВС+0,3×В | 0,25 | 0,44 | 0,71 | 0,90 | 0,65 | 0,42 | |

Вопрос 4:

| **Терм** | **1** | **2** | **3** | **4** | **5** | **6** | Доля пользователей |
|---|---|---|---|---|---|---|---|
| НС | 1,00 | 0,50 | 0,30 | 0,17 | 0,12 | 0,08 | 0,4 |
| С | 0,46 | 1,00 | 0,53 | 0,26 | 0,12 | 0,08 | 0,5 |
| ВС | 0,31 | 0,51 | 0,80 | 0,98 | 0,55 | 0,20 | 0,1 |
| Результат 0,4×НС+0,5×С + 0,1×ВС | 0,66 | 0,75 | 0,47 | 0,30 | 0,16 | 0,09 | |

Вопрос 5:

| **Терм** | **1** | **2** | **3** | **4** | **5** | **6** | Доля пользователей |
|---|---|---|---|---|---|---|---|
| В | 0,12 | 0,29 | 0,49 | 0,72 | 0,88 | 0,94 | 1 |
| Результат 1×В | 0,12 | 0,29 | 0,49 | 0,72 | 0,88 | 0,94 | |

Вопрос 6:

| **Терм** | **1** | **2** | **3** | **4** | **5** | **6** | Доля пользователей |
|---|---|---|---|---|---|---|---|
| С | 0,46 | 1,00 | 0,53 | 0,26 | 0,12 | 0,08 | 0,3 |
| ВС | 0,31 | 0,51 | 0,80 | 0,98 | 0,55 | 0,20 | 0,4 |
| В | 0,12 | 0,29 | 0,49 | 0,72 | 0,88 | 0,94 | 0,3 |
| Результат 0,3×С+0,4×ВС + 0,3×В | 0,30 | 0,59 | 0,63 | 0,69 | 0,52 | 0,39 | |

Получение суммарной нечеткой оценки комплекса реализованных превентивных мер защиты по таблице 7.

| № вопроса в Опроснике | **1** | **2** | **3** | **4** | **5** | **6** |
|---|---|---|---|---|---|---|
| 1 | 0,78 | 0,70 | 0,39 | 0,21 | 0,12 | 0,08 |
| 2 | 0,29 | 0,49 | 0,77 | 0,95 | 0,58 | 0,27 |
| 3 | 0,25 | 0,44 | 0,71 | 0,90 | 0,65 | 0,42 |
| 4 | 0,66 | 0,75 | 0,47 | 0,30 | 0,16 | 0,09 |
| 5 | 0,12 | 0,29 | 0,49 | 0,72 | 0,88 | 0,94 |
| 6 | 0,30 | 0,59 | 0,63 | 0,69 | 0,52 | 0,39 |
| Итоговое нечеткое множество | 0,40 | 0,54 | 0,58 | 0,63 | 0,49 | 0,37 |

**Этап 6**

Сравнение полученных суммарных нечетких оценок комплекса реализованных превентивных мер защиты по каждому из основных направлений защиты с нечеткими эталонами лингвистической переменной «Уровень безопасности»

| № вопроса | **1** | **2** | **3** | **4** | **5** | **6** | Соответствует терму |
|---|---|---|---|---|---|---|---|
| 1 | 0,78 | 0,70 | 0,39 | 0,21 | 0,12 | 0,08 | НС |
| 2 | 0,29 | 0,49 | 0,77 | 0,95 | 0,58 | 0,27 | ВС |
| 3 | 0,25 | 0,44 | 0,71 | 0,90 | 0,65 | 0,42 | ВС |
| 4 | 0,66 | 0,75 | 0,47 | 0,30 | 0,16 | 0,09 | С |
| 5 | 0,12 | 0,29 | 0,49 | 0,72 | 0,88 | 0,94 | В |
| 6 | 0,30 | 0,59 | 0,63 | 0,69 | 0,52 | 0,39 | ВС |
| Итоговое нечеткое множество | 0,40 | 0,54 | 0,58 | 0,63 | 0,49 | 0,37 | ВС |

Пример определения соответствующих термов вопросу 1

| **Терм** | **1** | **2** | **3** | **4** | **5** | **6** | **Сумма** | **Терм** |
|---|---|---|---|---|---|---|---|---|
| Н | 0,62 | 0,37 | 0,23 | 0,14 | 0,09 | 0,06 | | |
| Н- $\tilde{1}$ | -0,16 | -0,33 | -0,16 | -0,07 | -0,03 | -0,02 | -0,77 | |
| НС | 1,00 | 0,50 | 0,30 | 0,17 | 0,12 | 0,08 | | |
| НС- $\tilde{1}$ | 0,22 | -0,20 | -0,09 | -0,04 | 0,00 | 0,00 | -0,11 | НС |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| C | 0,46 | 1,00 | 0,53 | 0,26 | 0,12 | 0,08 | | |
| C- $\tilde{1}$ | -0,32 | 0,30 | 0,14 | 0,05 | 0,00 | 0,00 | 0,17 | |
| BC | 0,31 | 0,51 | 0,80 | 0,98 | 0,55 | 0,20 | | |
| BC- $\tilde{1}$ | -0,47 | -0,19 | 0,41 | 0,77 | 0,43 | 0,12 | 1,07 | |
| B | 0,12 | 0,29 | 0,49 | 0,72 | 0,88 | 0,94 | | |
| B- $\tilde{1}$ | -0,66 | -0,41 | 0,10 | 0,51 | 0,76 | 0,86 | 1,16 | |

**Вывод:**

Уровень безопасности информационной системы – «Выше среднего». Для повышения уровня безопасности необходимо оптимизировать мероприятия, указанные в вопросе 1.

## ПРАКТИЧЕСКОЕ ЗАДАНИЕ

Используется следующая игровая ситуация. Вы являетесь руководителем коммерческой фирмы, обладающей собственными коммерческими секретами и занимающейся, например, одним из следующих видов деятельности: производство электронных устройств, разработка программных продуктов, производство продуктов питания, коммерческая деятельность (торговля бытовой радиоэлектроникой), бытовые услуги населению.

Пользуясь описанной выше методикой, оцените уровень безопасности информационной системы Вашего предприятия. Разработайте рекомендации по повышению уровня безопасности.

## Контрольные вопросы

1. Нечеткое множество.
2. Способы построения нечетких множеств.
3. Классификация нечетких множеств.
4. Лингвистическая переменная.
5. Нечеткий эталон.
6. Превентивные меры защиты.
7. Операции над нечеткими множествами

**Тема. 5 Сложные системы**

Практическое занятие № 9

**Название работы:** Оценка уровня безопасности информационной системы предприятия на базе модели с балльной шкалой

**Формируемые компетенции:** УК-1

**Теоретическая часть:**

## ОСНОВНЫЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Рассмотрим нечеткую модель с балльной шкалой, схема модели представлена в таблице 1. Модель используется для определения состояния безопасности информационной системы, по результатам опроса пользователей согласно составленного экспертами запроса.

Таблица 1 – Методика нечеткой балльной оценки уровня безопасности информационной системы предприятия

| Этапы | Содержание этапа |
|---|---|
| Этап 1 | Выделение основных направлений защиты информации |
| Этап 2 | Определение списка основных угроз информационной безопасности для предприятия |
| Этап 3 | На основе выделенных направлений защиты и составленного списка угроз разработка опросников «Самооценка комплекса реализованных превентивных мер защиты» для пользователей информационной системы предприятия. Ответы пользователей будут представлены в виде лингвистических переменных: «почти никогда», «редко», «не редко и не часто», «часто», «почти всегда». |
| Этап 4 | Разработка нечетких эталонов для термов балльной переменной «Уровень безопасности» |
| Этап 5 | Заполнение опросников «Самооценка комплекса реализованных превентивных мер защиты» пользователями информационной системы, обработка результатов и получение суммарной нечеткой оценки комплекса реализованных превентивных мер защиты |
| Этап 6 | Сравнение полученных суммарных нечетких оценок комплекса реализованных превентивных мер защиты по каждому из основных направлений защиты с нечеткими эталонами балльной переменной «Уровень безопасности». Вывод о достаточности мер по защите информации и уровне безопасности информационной системы предприятия |

*Методические рекомендации по применению методики нечеткой лингвистической оценки уровня безопасности информационной системы предприятия:*

**Этап 1**

В качестве основных направлений защиты информации можно выделить:

– организационная защита,

– компьютерная защита;

– физическая защита.

**Этап 2**

Пример составленного списка основных угроз информационной безопасности для предприятия приведен в таблице 2.

Таблица 2 – Список основных угроз информационной безопасности для предприятия

| № п/п | Класс угроз | Способ распространения |
|---|---|---|
| 1 | | Заражение через файл, скаченный из глобальной сети |

| | | |
|---|---|---|
| | Компьютерные вирусы | «Internet» |
| | | Заражение через файл, скаченный с FTP сервера |
| | | Заражение через нелицензионное программное обеспечение |
| | | Заражение через Flash-накопители |
| | | Заражение через электронную почту |
| | | Заражение через системы обмена мгновенными сообщениями |
| | | Заражение через Web-страницы |
| 2 | Непреднамеренные действия персонала | Порча оборудования, носителей информации |
| | | Искажение файлов с важной информацией |
| | | Изменение режимов работы устройств и программ |
| | | Запуск неучтенных программ, системных служб |
| | | Разглашение конфиденциальной информации |
| | | Разглашение, передача или утрата атрибутов разграничения доступа (паролей, пропусков и т.д.) |
| | | Игнорирование организационных ограничений |
| | | Некомпитентное использование, настройка или неправомерное отключение средств защиты информации |
| | | пересылка данных по ошибочному адресу абонента (устройства) |
| | | Ввод ошибочных данных |
| | | Повреждение каналов связи |
| 3 | Преднамеренные действия персонала | Физическое разрушение системы или наиболее важных компонентов |
| | | Отключение или вывод из строя систем обеспечения функционирования (электропитание, охлаждение и т.д.) |
| | | Изменение режимов работы устройств или программ |
| | | Хищение носителей информации |
| | | Несанкционированное копирование носителей информации |
| | | Хищение производственных отходов (распечаток, записей и т.д.) |
| | | Несанкционированное использование терминалов пользователей |
| | | Незаконное получение реквизитов разграничения доступа |
| 4 | Сетевые атаки | Переполнение буфера (buffer overflows) |
| | | Перехват пакетов в локальной сети (сниффер пакетов) |
| | | Вставка ложной информации или вредоносных команд в обычный поток данных (IP-спуфинг) |
| | | Отказ в обслуживании (Denial of Service (DoS)) |
| | | Перебор паролей (brute force attack) |
| | | Отключение систем защиты |
| 5 | Кражи и чрезвычайные ситуации | Воровство активов |
| | | Несчастные случаи с персоналом |
| | | Пожар |
| | | Землетрясение |
| | | Наводнение |

**Этап 3**

Примеры разработанных опросников «Самооценка комплекса реализованных превентивных мер защиты» приведены в таблицах 3, 4, 5.

Таблица 3 – Опросник «Оценка реализованных превентивных мер по организационной защите информации»

| № п/п | Компонент запроса | Варианты ответов пользователя | | | | |
|---|---|---|---|---|---|---|
| | | Почти никогда | Редко | Не часто и не редко | Часто | Почти всегда |
| 1 | Проводятся ли совещания руководства касательно защиты информации в организации? | | | | | |
| 2 | Получаются ли консультации по защите информации от внешних специалистов? | | | | | |
| 3 | Поддерживаются ли контакты с правоохранительными органами? | | | | | |
| 4 | Оцениваются ли риски информационной безопасности в организации? | | | | | |
| 5 | Проводится ли аудит организационных мер на соответствие политике безопасности принятой на предприятии? | | | | | |
| 6 | Проводится ли информирование персонала по вопросам информационной безопасности? | | | | | |

Таблица 4 – Опросник «Оценка реализованных превентивных мер по использования средств защиты информации в компьютерной системе»

| № п/п | Компонент запроса | Варианты ответов пользователя | | | | |
|---|---|---|---|---|---|---|
| | | Почти никогда | Редко | Не часто и не редко | Часто | Почти всегда |
| 1 | Сохраняются ли свежие копии данных за пределами организации? | | | | | |
| 2 | Часто ли выполняется резервное копирование? | | | | | |
| 3 | Проводится ли | | | | | |

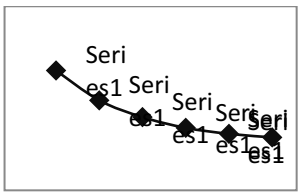
| | | | | | | |
|---|---|---|---|---|---|---|
| | антивирусный контроль? | | | | | |
| 4 | Всегда ли удаляются ненужные или устарелые файлы? | | | | | |
| 5 | Используются ли средства криптографической защиты? | | | | | |
| 6 | Применяются в организации персональные межсетевые экраны? | | | | | |

Таблица 5 – Опросник «Оценка реализованных превентивных мер физической защиты информации»

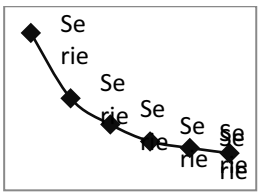
| № п/п | Компонент запроса | Варианты ответов пользователя | | | | |
|---|---|---|---|---|---|---|
| | | Почти никогда | Редко | Не часто и не редко | Часто | Почти всегда |
| 1 | Как часто применяются методы защиты для предотвращения утечки информации по телекоммуникационным и сетевым кабелям? | | | | | |
| 2 | Используются ли системы обнаружения проникновения на дверях, окнах, в рабочих помещениях? | | | | | |
| 3 | Часто ли пересматриваются доступ пользователей к ресурсам в охраняемом периметре? | | | | | |
| 4 | Используются ли процедуры аутентификации? | | | | | |
| 5 | Применяются ли средства защиты для оборудования организации? | | | | | |
| 6 | Проводятся ли проверки на наличие несанкционированных подключений к линиям связи? | | | | | |

**Этап 4**

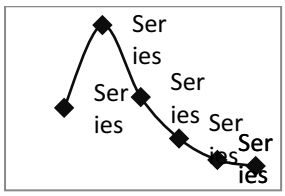
Нечеткие эталоны могут иметь вид (см. рис.1).



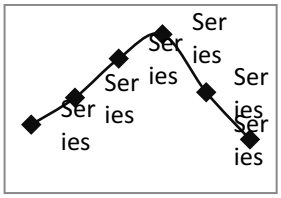

а) Нечеткое множество W1



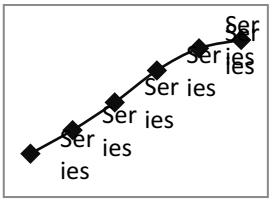

б) Нечеткое множество W2




в) Нечеткое множество W3




г) Нечеткое множество W4




д) Нечеткое множество W5

Рисунок 1 – Нечеткие эталоны балльной переменной «Уровень безопасности»

Таблица 6 – Числовые значения нечетких эталонов балльной переменной «Уровень безопасности»

| **Нечеткое множество** | **1** | **2** | **3** | **4** | **5** | **6** |
|---|---|---|---|---|---|---|
| W1 | 0,62 | 0,37 | 0,23 | 0,14 | 0,09 | 0,06 |
| W2 | 1,00 | 0,50 | 0,30 | 0,17 | 0,12 | 0,08 |
| W3 | 0,46 | 1,00 | 0,53 | 0,26 | 0,12 | 0,08 |
| W4 | 0,31 | 0,51 | 0,80 | 0,98 | 0,55 | 0,20 |
| W5 | 0,12 | 0,29 | 0,49 | 0,72 | 0,88 | 0,94 |

**Этап 5**

Пользователями информационной системы заполняются опросники «Самооценка комплекса реализованных превентивных мер защиты» по выделенным основным направлениям защиты информации. Каждый пользователь в соответствующем Опроснике выбирает только 1 ответ: «почти никогда», «редко», «не редко не часто», «часто», «почти всегда». В таблице 7 приведен пример результата опроса по одному из основных направлений защиты информации.

Таблица 7 – Результат опроса 10 пользователей

| Номер вопроса | Количество пользователей, заполнивших опросники | | | | |
|---|---|---|---|---|---|
| | Почти никогда | Редко | Не часто и не редко | Часто | Почти всегда |
| 1 | | 6 | 4 | | |
| 2 | | | | 9 | 1 |
| 3 | | | | 7 | 3 |
| 4 | | 4 | 5 | 1 | |
| 5 | | | | | 10 |
| 6 | | | 3 | 4 | 3 |

Ответу «Почти никогда» соответствует терм «Низкий», ответу «Редко» – терм «Ниже среднего», ответу «Не часто и не редко» – терм «Средний», ответу «Часто» – терм «Выше среднего», ответу «Почти всегда» – терм «Высокий».

Получение нечетких оценок по каждому вопросу Опросника:

Вопрос 1:

| **Терм** | **1** | **2** | **3** | **4** | **5** | **6** | Доля |
|---|---|---|---|---|---|---|---|

| | | | | | | | пользователей |
|---|---|---|---|---|---|---|---|
| НС | 1,00 | 0,50 | 0,30 | 0,17 | 0,12 | 0,08 | 0,6 |
| С | 0,46 | 1,00 | 0,53 | 0,26 | 0,12 | 0,08 | 0,4 |

Вопрос 2:

| **Терм** | **1** | **2** | **3** | **4** | **5** | **6** | Доля пользователей |
|---|---|---|---|---|---|---|---|
| W1 | 0,31 | 0,51 | 0,80 | 0,98 | 0,55 | 0,20 | 0,9 |
| W2 | 0,12 | 0,29 | 0,49 | 0,72 | 0,88 | 0,94 | 0,1 |

Вопрос 3:

| **Терм** | **1** | **2** | **3** | **4** | **5** | **6** | Доля пользователей |
|---|---|---|---|---|---|---|---|
| W4 | 0,31 | 0,51 | 0,80 | 0,98 | 0,55 | 0,20 | 0,7 |
| W5 | 0,12 | 0,29 | 0,49 | 0,72 | 0,88 | 0,94 | 0,3 |

Вопрос 4:

| **Терм** | **1** | **2** | **3** | **4** | **5** | **6** | Доля пользователей |
|---|---|---|---|---|---|---|---|
| W2 | 1,00 | 0,50 | 0,30 | 0,17 | 0,12 | 0,08 | 0,4 |
| W3 | 0,46 | 1,00 | 0,53 | 0,26 | 0,12 | 0,08 | 0,5 |
| W4 | 0,31 | 0,51 | 0,80 | 0,98 | 0,55 | 0,20 | 0,1 |

Вопрос 5:

| **Терм** | **1** | **2** | **3** | **4** | **5** | **6** | Доля пользователей |
|---|---|---|---|---|---|---|---|
| W5 | 0,12 | 0,29 | 0,49 | 0,72 | 0,88 | 0,94 | 1 |

Вопрос 6:

| **Терм** | **1** | **2** | **3** | **4** | **5** | **6** | Доля пользователей |
|---|---|---|---|---|---|---|---|
| W3 | 0,46 | 1,00 | 0,53 | 0,26 | 0,12 | 0,08 | 0,3 |
| W4 | 0,31 | 0,51 | 0,80 | 0,98 | 0,55 | 0,20 | 0,4 |
| W5 | 0,12 | 0,29 | 0,49 | 0,72 | 0,88 | 0,94 | 0,3 |

Получение суммарной нечеткой оценки комплекса реализованных превентивных мер защиты по таблице 7.

| № вопроса в Опроснике | **1** | **2** | **3** | **4** | **5** | **6** |
|---|---|---|---|---|---|---|
| 1 | 0,78 | 0,70 | 0,39 | 0,21 | 0,12 | 0,08 |
| 2 | 0,29 | 0,49 | 0,77 | 0,95 | 0,58 | 0,27 |
| 3 | 0,25 | 0,44 | 0,71 | 0,90 | 0,65 | 0,42 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 4 | 0,66 | 0,75 | 0,47 | 0,30 | 0,16 | 0,09 |
| 5 | 0,12 | 0,29 | 0,49 | 0,72 | 0,88 | 0,94 |
| 6 | 0,30 | 0,59 | 0,63 | 0,69 | 0,52 | 0,39 |
| Итоговое нечеткое множество | 0,40 | 0,54 | 0,58 | 0,63 | 0,49 | 0,37 |

**Этап 6**

Сравнение полученных суммарных нечетких оценок комплекса реализованных превентивных мер защиты по каждому из основных направлений защиты с нечеткими эталонами лингвистической переменной «Уровень безопасности»

| № вопроса | **1** | **2** | **3** | **4** | **5** | **6** |
|---|---|---|---|---|---|---|
| 1 | 0,78 | 0,70 | 0,39 | 0,21 | 0,12 | 0,08 |
| 2 | 0,29 | 0,49 | 0,77 | 0,95 | 0,58 | 0,27 |
| 3 | 0,25 | 0,44 | 0,71 | 0,90 | 0,65 | 0,42 |
| 4 | 0,66 | 0,75 | 0,47 | 0,30 | 0,16 | 0,09 |
| 5 | 0,12 | 0,29 | 0,49 | 0,72 | 0,88 | 0,94 |
| 6 | 0,30 | 0,59 | 0,63 | 0,69 | 0,52 | 0,39 |
| Итоговое нечеткое множество | 0,40 | 0,54 | 0,58 | 0,63 | 0,49 | 0,37 |

Пример определения соответствующих термов вопросу 1

| **Терм** | **1** | **2** | **3** | **4** | **5** | **6** | **Сумма** |
|---|---|---|---|---|---|---|---|
| W1 | 0,62 | 0,37 | 0,23 | 0,14 | 0,09 | 0,06 | |
| W1- $\tilde{1}$ | -0,16 | -0,33 | -0,16 | -0,07 | -0,03 | -0,02 | -0,77 |
| W1W3 | 1,00 | 0,50 | 0,30 | 0,17 | 0,12 | 0,08 | |
| W1W2- $\tilde{1}$ | 0,22 | -0,20 | -0,09 | -0,04 | 0,00 | 0,00 | -0,11 |
| W3 | 0,46 | 1,00 | 0,53 | 0,26 | 0,12 | 0,08 | |
| W3- $\tilde{1}$ | -0,32 | 0,30 | 0,14 | 0,05 | 0,00 | 0,00 | 0,17 |
| W4W5 | 0,31 | 0,51 | 0,80 | 0,98 | 0,55 | 0,20 | |
| 4W5- $\tilde{1}$ | -0,47 | -0,19 | 0,41 | 0,77 | 0,43 | 0,12 | 1,07 |
| W5 | 0,12 | 0,29 | 0,49 | 0,72 | 0,88 | 0,94 | |
| W5- $\tilde{1}$ | -0,66 | -0,41 | 0,10 | 0,51 | 0,76 | 0,86 | 1,16 |

**Вывод:**

Уровень безопасности информационной системы – «Выше среднего». Для повышения уровня безопасности необходимо оптимизировать мероприятия, указанные в вопросе 1.

## ПРАКТИЧЕСКОЕ ЗАДАНИЕ

Используется следующая игровая ситуация. Вы являетесь руководителем коммерческой фирмы, обладающей собственными коммерческими секретами и занимающейся, например, одним из следующих видов деятельности: производство электронных устройств, разработка программных продуктов, производство продуктов питания, коммерческая деятельность (торговля бытовой радиоэлектроникой), бытовые услуги населению.

Пользуясь описанной выше методикой, оцените уровень безопасности информационной системы Вашего предприятия. Разработайте рекомендации по повышению

уровня безопасности.

**Список литературы, рекомендуемый к использованию по данной теме.**
*Основная:* 1
*Дополнительная: 1, 2, 3, 4, 5, 6*
*Методическая литература: 1, 2*
*Интернет-ресурсы: 1, 2*

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**
**«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»**

# МЕТОДИЧЕСКИЕ УКАЗАНИЯ

для обучающихся по выполнению и проведению самостоятельной работы
по дисциплине «Моделирование процессов и систем защиты информации»
для студентов направления подготовки
10.03.01 Информационная безопасность
Направленность (профиль)
«Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)»

Ставрополь,
2026

**СОДЕРЖАНИЕ**

## ВВЕДЕНИЕ

Целью изучения дисциплины «Моделирование процессов и систем защиты информации» является обучение студентов принципам построения и анализа основных подходов к моделированию процессов и систем защиты информации, способствовать развитию логического мышления и формирования научного мировоззрения, а также приобретение набора профессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01 Информационная безопасность.

Задачами дисциплины являются:

1.Ознакомление с имеющимся опытом теоретических исследований и практического решения задач защиты информации;

2.Приобретение теоретических знаний и практических навыков в области интенсификации процессов обеспечения информационной безопасности.

### 1. Общая характеристика самостоятельной работы студента

Основными видами учебной работы по достижению результатов освоения дисциплины являются лекции, практические занятия и самостоятельная работа студентов (СРС).

На лекциях раскрываются основные положения и понятия курса, формируются знания в области математических моделей систем и процессов защиты информации. На практических занятиях формируются умения и навыки, необходимые для решения задач профессиональной деятельности.

Приступая к изучению учебной дисциплины, необходимо ознакомиться с учебной программой, получить в библиотеке рекомендованные учебные пособия, а также получить у ведущего преподавателя в электронном виде конспекты лекций, методические рекомендации к практическим занятиям и тестовые, завести новую тетрадь для конспектирования лекций и выполнения практических занятий.

Для изучения дисциплины предлагается список основной и дополнительной литературы. Основная литература предназначена для обязательного изучения, дополнительная – поможет более глубоко освоить отдельные вопросы, подготовить исследовательские задания и выполнить задания для самостоятельной работы.

В ходе лекционных занятий студент обязан осуществлять конспектирование учебного материала, особое внимание, обращая на категории, формулировки, раскрывающие содержание тех или иных понятий, физических явлений, процессов, эффектов. В рабочих конспектах желательно оставлять поля, на которых следует делать пометки из рекомендованной литературы, дополнять материал прослушанной лекции, формулировать научные выводы и практические рекомендации. Студент имеет право задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Самостоятельная работа студентов над материалом учебной дисциплины является неотъемлемой частью учебного процесса и должна предполагать углубление знания учебного материала, излагаемого на аудиторных занятиях, и приобретение дополнительных знаний по отдельным вопросам самостоятельно.

Основными видами самостоятельной работы курсантов по учебной дисциплине являются:

- самостоятельное изучение учебного материала по заданным темам;
- подготовка к практическим занятиям, оформление отчета по выполненному практическому занятию и подготовка к собеседованию по результатам работы.

Основными методами самостоятельной работы студентов являются:

1) для овладения знаниями:
   - чтение текста (конспекта лекций, учебника, дополнительной литературы) и конспектирование текста;
   - работа с нормативными документами;

– поиск информации в Интернет;

2) для закрепления и систематизации знаний:
   – работа с конспектом лекции (обработка текста);
   – повторная работа над учебным материалом (учебника, дополнительной литературы, слайдами);
   – составление плана и тезисов ответа или графическое изображение структуры ответа;
   – составление таблиц для систематизации учебного материала;
   – изучение нормативных документов;
   – ответы на контрольные вопросы;
3) для формирования умений:
   – подготовка к практическим занятиям;
   – решение задач и практических заданий;
   – подготовка отчетов по практическим занятиям;
   – рефлексивный анализ профессиональных умений.

В случае пропуска учебного занятия студент может воспользоваться содержанием различных блоков учебно-методического комплекса (лекции, практические занятия, контрольные вопросы и тесты) для самоподготовки и освоения темы. Для самоконтроля необходимо использовать вопросы и задания, предлагаемые к практическим занятиям, а также варианты тестовых заданий.

**2. Технологическая карта самостоятельной работы студента**

| Коды реализуемых компетенций, индикатора(ов) | Вид деятельности студентов | Средства и технологии оценки | Обьем часов, в том числе | | |
|---|---|---|---|---|---|
| | | | СРС | Контактная работа с преподавателем | Всего |
| 5 семестр | | | | | |
| УК-1 ИД-1 УК-1 ИД-3 | Подготовка к практическим занятиям | Собеседование | 14.0 | 7.0 | 21.0 |
| УК-1 ИД-1 УК-1 ИД-3 | Подготовка к лекции | Конспект | 14.0 | 7.0 | 21.0 |
| УК-1 ИД-1 УК-1 ИД-3 | Подготовка доклада | Доклад | 14.0 | 7.0 | 21.0 |
| УК-1 ИД-1 УК-1 ИД-3 | Самостоятельное изучение литературы | Конспект | 14.0 | 7.0 | 21.0 |
| УК-1 ИД-1 УК-1 ИД-3 | Самостоятельное выполнение заданий по заданным темам. | Конспект. Письменный отчет | 16.0 | 8.0 | 24.0 |
| **Итого за семестр** | | | 72.0 | 36.0 | 108.0 |
| **Итого** | | | 72.0 | 36.0 | 108.0 |

**3. Порядок выполнения самостоятельной работы**

*3.1 Методические рекомендации по изучению теоретического материала*

Комплексное изучение предлагаемой студентам учебной дисциплины «Моделирование процессов и систем защиты информации» предполагает овладение материалами лекций, учебников, программы, творческую работу студентов в ходе проведения практических занятий, а также систематическое выполнение заданий для самостоятельной работы.

В ходе лекций раскрываются основные вопросы в рамках рассматриваемых тем, делаются акценты на наиболее сложные и интересные положения изучаемого материала, которые должны быть приняты студентами во внимание. Материалы лекций являются основой для подготовки студентов к практическим занятиям.

***Работа с конспектом лекций***

Просмотрите конспект сразу после занятий. Отметьте материал конспекта лекций, который вызывает затруднения для понимания. Попытайтесь найти ответы на затруднительные вопросы, используя предлагаемую литературу. Если самостоятельно не удалось разобраться в материале, сформулируйте вопросы и обратитесь на текущей консультации или на ближайшей лекции за помощью к преподавателю.

Каждую неделю отводите время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам и тестам.

***Выполнение практических занятий по дисциплине «Моделирование процессов и систем защиты информации»***

На первом занятии получите у преподавателя задания по курсу, планы подготовки к практическим занятиям. Обзаведитесь всем необходимым методическим обеспечением.

Перед практическими занятиями изучите теорию вопроса, предполагаемого к исследованию, ознакомьтесь с опытом других исследователей в этом направлении.

Целью практических занятий является:

- закрепление методов приложения теории к решению практических задач анализа и синтеза психологического знания;
- проверка уровня понимания студентами вопросов, рассмотренных на лекциях и по учебной литературе, степени и качества усвоения материала;
- обучение навыкам освоения методики эксперимента и работы с нормативно-справочной литературой;
- восполнение пробелов в пройденной теоретической части курса и оказание помощи в его усвоении.

*3.2 Методические рекомендации по написанию и оформлению доклада*

1. Общие положения

1.1. Доклад, как вид самостоятельной работы в учебном процессе, способствует формированию навыков исследовательской работы, расширяет познавательные интересы, учит критически мыслить.

1.2. При написании доклада по заданной теме студент составляет план, подбирает основные источники.

1.3. В процессе работы с источниками систематизирует полученные сведения, делает выводы и обобщения.

1.4. К докладу по крупной теме могут привлекать несколько студентов, между которыми распределяются вопросы выступления.

2. Выбор темы доклада

2.1. Тематика доклада обычно определяется преподавателем, но в определении темы инициативу может проявить и студент.

2.2. Прежде чем выбрать тему доклада, автору необходимо выявить свой интерес, определить, над какой проблемой он хотел бы поработать, более глубоко ее изучить.

3. Этапы работы над докладом

3.1. Формулирование темы, причем она должна быть не только актуальной по

своему значению, но и оригинальной, интересной по содержанию.

3.2. Подбор и изучение основных источников по теме (как правильно, при разработке доклада используется не менее 8-10 различных источников).

3.3. Составление списка использованных источников.

3.4. Обработка и систематизация информации

3.5. Разработка плана доклада.

3.6. Написание доклада.

3.7. Публичное выступление с результатами исследования.

4. Структура доклада:

- титульный лист

- оглавление (в нем последовательно излагаются названия пунктов доклада, указываются страницы, с которых начинается каждый пункт);

- введение (формулирует суть исследуемой проблемы, обосновывается выбор темы, определяются ее значимость и актуальность, указываются цель и задачи доклада, дается характеристика используемой литературы);

- основная часть (каждый раздел ее, доказательно раскрывая отдельную проблему или одну из ее сторон, логически является продолжением предыдущего; в основной части могут быть представлены таблицы, графики, схемы);

- заключение (подводятся итоги или дается обобщенный вывод по теме доклада, предлагаются рекомендации);

- список использованных источников

5. Структура и содержание доклада

5.1. Введение - это вступительная часть научно-исследовательской работы. Автор должен приложить все усилия, чтобы в этом небольшом по объему разделе показать актуальность темы, раскрыть практическую значимость ее, определить цели и задачи эксперимента или его фрагмента.

5.2. Основная часть. В ней раскрывается содержание доклада. Как правило, основная часть состоит из теоретического и практического разделов. В теоретическом разделе раскрываются история и теория исследуемой проблемы, дается критический анализ литературы и показываются позиции автора. В практическом разделе излагаются методы, ход, и результаты самостоятельно проведенного эксперимента или фрагмента.

В основной части могут быть также представлены схемы, диаграммы, таблицы, рисунки и т.д.

5.3. В заключении содержатся итоги работы, выводы, к которым пришел автор, и рекомендации. Заключение должно быть кратким, обязательным и соответствовать поставленным задачам.

5.4. Список использованных источников представляет собой перечень использованных книг, статей, фамилии авторов приводятся в алфавитном порядке, при этом все источники даются под общей нумерацией литературы. В исходных данных источника указываются фамилия и инициалы автора, название работы, место и год издания.

5.5. Приложение к докладу оформляются на отдельных листах, причем каждое должно иметь свой тематический заголовок и номер, который пишется в правом верхнем углу, например: «Приложение 1»

6. Требования к оформлению доклада

6.1. Объем доклада может колебаться в пределах 5-15 печатных страниц; все приложения к работе не входят в ее объем.

6.2. Доклад должен быть выполнен грамотно, с соблюдением культуры изложения.

6.3. Обязательно должны иметься ссылки на используемую литературу.

6.4. Должна быть соблюдена последовательность написания библиографического

аппарата.

7. Критерии оценки доклада

- актуальность темы исследования;
- соответствие содержания теме;
- глубина проработки материала; правильность и полнота использования источников;
- соответствие оформления доклада стандартам.

По усмотрению преподавателя доклады могут быть представлены на семинарах, научно-практических конференциях, а также использоваться как зачетные работы по пройденным темам.

*3.3 Методические рекомендации по конспектированию первоисточников*

Изучение и анализ литературных источников является обязательным видом самостоятельной работы студентов. Изучение литературы по избранной теме имеет своей задачей проследить характер постановки и решения определенной проблемы различными авторами, аргументацию их выводов и обобщений, провести анализ и систематизировать полученный материал на основе собственного осмысления с целью выяснения современного состояния вопроса.

Проработка отобранного материала обязательно должна идти с одновременным ведением записей прочитанного и своих замечаний. Запись может иметь как форму конспекта, так и выписок, а также картотеку положений, тезисов, идей, методик, что в дальнейшем облегчит классификацию и систематизацию полученного материала. Такого рода записи являются лучшим способом накопления и первичной обработки материал, одной из обязательных форм организации умственного труда.

**Планом** удобно пользоваться при подготовке к устному выступлению по выбранной теме. Каждый пункт плана должен раскрывать одну из сторон избранной темы, а весь план должен охватывать ее целиком.

**Тезисы** предполагают сжатое изложение основных положений текста в форме утверждения или отрицания. Они являются более совершенной формой записей и представляют основу для дискуссии. К тому же их легко запомнить.

**Конспектирование** – процесс мысленной переработки и письменной фиксации информации, в виде краткого изложения основного содержания, смысла какого-либо текста.

Результат конспектирования – запись, позволяющая конспектирующему немедленно или через некоторый срок с нужной полнотой восстановить полученную информацию. Конспект в переводе с латыни означает «обзор». По существу его и составлять надо как обзор, содержащий основные мысли текста без подробностей и второстепенных деталей. Конспект носит индивидуализированный характер: он рассчитан на самого автора и поэтому может оказаться малопонятным для других.

Для того чтобы осуществлять этот вид работы, в каждом конкретном случае необходимо грамотно решить следующие задачи:

1. Сориентироваться в общей композиции текста (уметь определить вступление, основную часть, заключение).
2. Увидеть логико-смысловую канву сообщения, понять систему изложения автором информации в целом, а также ход развития каждой отдельной мысли.
3. Выявить «ключевые» мысли, т. е. основные смысловые вехи, на которые «нанизано» все содержание текста.
4. Определить детализирующую информацию.
5. Лаконично сформулировать основную информацию, не перенося на письмо все целиком и дословно.

Во всяком научном тексте содержится информация 2-х видов: основная и вспомогательная. Основной является информация, имеющая наиболее существенное

значение для раскрытия содержания темы или вопроса. К ней относятся: определения научных понятий, формулировки законов, теоретических принципов и т. д. Назначение вспомогательной информации – помочь читателю лучше усвоить предлагаемый материал. К этому типу информации относятся разного рода комментарии. Основную – записываем как можно полнее, вспомогательную, как правило, опускаем. Содержание конспектирования составляет переработка основной информации в целях ее обобщения и сокращения. Обобщить – значит представить ее в более общей, схематической форме, в виде тезисов, выводов, отдельных заголовков, изложения основных результатов и т. п. Читая, мы интуитивно используем некоторые слова и фразы в качестве опорных. Такие опорные слова и фразы называются ключевыми. Ключевые слова и фразы несут основную смысловую и эмоциональную нагрузку содержания текста.

Выбор ключевых слов – это первый этап смыслового свертывания, смыслового сжатия материала.

Важными требованиями к конспекту являются наглядность и обозримость записей и такое их расположение, которое давало бы возможность уяснить логические связи и иерархию понятий.

**По форме *конспекты подразделяются* на формализованные и графические.**

**1. Формализованные** (все записи вносятся в заранее подготовленные таблицы).

Это удобно, во-первых, при конспектировании материалов, когда перечень характеристик описываемых предметов или явлений более или менее постоянен, во-вторых, при подготовке единого конспекта по нескольким источникам. Особенно если есть необходимость сравнения отдельных данных. Разновидностью формализованного конспекта является запись, составленная в форме ответов на заранее подготовленные вопросы, обеспечивающие исчерпывающие характеристики однотипных предметов или явлений.

**2. Графические** (элементы конспектируемой работы располагаются в таком виде, при котором видна иерархия понятий и взаимосвязь между ними).

По каждой работе может быть не один, а несколько графических конспектов, отображающих книгу в целом и отдельные ее части. Ведение графического конспекта - наиболее совершенный способ изображения внутренней структуры книги, а сам этот процесс помогает усвоению ее содержания.

Можно выделить следующие основные **типы конспектов: плановый, текстуальный, сводный, тематический.**

**Плановый** – легко получить с помощью предварительно сделанного плана произведения, каждому вопросу плана отвечает определенная часть конспекта:

а) вопросно-ответный (на пункты плана, выраженные в вопросительной форме, конспект дает точные ответы);

б) схематичный плановый конспект (отражает логическую структуру и взаимосвязь отдельных положений).

**Текстуальный** – это конспект, созданный в основном из цитат.

**Сводный конспект** – сочетает выписки, цитаты, иногда тезисы; часть его текста может быть снабжена планом.

**Тематический** – дает более или менее исчерпывающий ответ (в зависимости из числа привлеченных источников и другого материала, например, своих же записей) на поставленный вопрос – тему: обзорный; хронологический.

Роль конспекта – чисто учебная: он помогает зафиксировать основные понятия и положения первичного текста и в нужный момент их воспроизвести, например, при написании реферата или подготовке к экзамену.

**Способы конспектирования.**

**- *Тезисы*** – это кратко сформулированные основные мысли, положения изучаемого материала. Тезисы лаконично выражают суть читаемого, дают возможность раскрыть содержание. Приступая к освоению записи в виде тезисов, полезно в самом

тексте отмечать места, наиболее четко формулирующие основную мысль, которую автор доказывает (если, конечно, это не библиотечная книга). Часто такой отбор облегчается шрифтовым выделением, сделанным в самом тексте.

***- Линейно-последовательная запись текста.*** При конспектировании линейно – последовательным способом целесообразно использование плакатно-оформительских средств, которые включают в себя следующие:

- сдвиг текста конспекта по горизонтали, по вертикали;
- выделение жирным (или другим) шрифтом особо значимых слов;
- использование различных цветов;
- подчеркивание;
- заключение в рамку главной информации.

- С***пособ «вопросов – ответов».*** Он заключается в том, что, поделив страницу тетради пополам вертикальной чертой, конспектирующий в левой части страницы самостоятельно формулирует вопросы или проблемы, затронутые в данном тексте, а в правой части дает ответы на них.

Одна из модификаций способа «вопросов – ответов» - таблица, где место вопроса занимает формулировка проблемы, поднятой автором (лектором), а место ответа – решение данной проблемы. Иногда в таблице могут появиться и дополнительные графы: например, «мое мнение» и т. п.

- С***хема с фрагментами –*** способ конспектирования, позволяющий ярче выявить структуру текста, - при этом фрагменты текста (опорные слова, словосочетания, пояснения всякого рода) в сочетании с графикой помогают созданию рационально - лаконичного конспекта.

- ***Простая схема –*** способ конспектирования, близкий к схеме с фрагментами, объяснений к которой конспектирующий не пишет, но должен уметь давать их устно. Этот способ требует высокой квалификации конспектирующего. В противном случае такой конспект нельзя будет использовать.

- ***Параллельный способ*** конспектирования. Конспект оформляется на двух листах параллельно или один лист делится вертикальной чертой пополам и записи делаются в правой и в левой части листа.

***Однако л***учше использовать разные способы конспектирования для записи одного и того же материала.

***Комбинированный конспект*** – вершина овладения рациональным конспектированием. При этом умело используются все перечисленные способы, сочетая их в одном конспекте (один из видов конспекта свободно перетекает в другой в зависимости от конспектируемого текста, от желания и умения конспектирующего). Именно при комбинированном конспекте более всего проявляется уровень подготовки и индивидуальность студента.

**Принципы составления конспекта прочитанного.**

1. Записать все выходные данные источника: автор, название, год и место издания. Если текст взят из периодического издания (газеты или журнала), то записать его название, год, месяц, номер, число, место издания.

2. Выделить поля слева или справа, можно с обеих сторон. Слева на полях отмечаются страницы оригинала, структурные разделы статьи или книги (названия параграфов, подзаголовки и т. п.), формулируются основные проблемы. Справа – способы фиксации прочитанной информации.

Один из видов чтения – углубленное – предполагает глубокое усвоение прочитанного и часто сохранение информации в целях последующего обращения к ней. Эффективность такого чтения повышается, если прочитанное зафиксировано не только в памяти, но и на бумаге. Психологи утверждают, что записанное лучше и полнее усваивается, прочнее откладывается в памяти. Установлено, что если прочитать 1000 слов и затем записать 50, подытоживающих прочитанное, то коэффициент усвоения

будет выше, чем, если прочитать 10000 слов, не записав ни одного. Кроме того, при записи прочитанного формируется навык свертывания информации. И, наконец, чередование чтения и записывания уменьшает усталость, повышает работоспособность и производительность умственного труда.

*1. Резюмирование.*

Резюме – краткий итог прочитанного, содержащий его оценку. Резюме характеризует основные выводы книги, главные итоги.

Выбор языковых средств для построения резюме-выводов подчинен основной задаче свертывания информации: минимум языковых средств – максимум информации. Это обычно одно – три четких, кратких, выразительных предложения, раскрывающих, по мнению автора, самую суть описываемого объекта.

*2. Аннотация.*

Аннотация – краткая обобщенная характеристика печатной работы (книги, статьи), включающая иногда и его оценку. Это наикратчайшее изложение содержания первичного документа, дающее общее представление о теме.

Основное ее назначение – дать некоторое представление о книге (статье, научной работе) с тем, чтобы рекомендовать ее определенному кругу читателей или воспользоваться своими записями при выполнении работы исследовательского, реферативного характера. Поэтому аннотации не требуется изложения содержания произведения, в ней лишь перечисляются вопросы, которые освещены в первоисточнике (содержание этих вопросов не раскрывается). Аннотация отвечает на вопрос: «О чем говорится в первичном тексте?», дает представление только о главной теме и перечне вопросов, затрагиваемых в тексте первоисточника.

Текст аннотации не стандартизирован. В научной литературе можно встретить различные требования к составлению аннотаций. Например, текст справочной аннотации может включать следующие сведения:

· тип и название аннотируемого документа (монография, диссертация, сборник, статья и т. п.)

· задачи, поставленные автором аннотируемого документа

· метод, которым пользовался автор (эксперимент, сравнительный анализ, компиляция других источников)

· принадлежность автора к определенной научной школе или направлению

· структуру аннотируемого документа

· предмет и тему произведения, основные положения и выводы автора

· характеристику вспомогательных иллюстративных материалов, дополнений, приложений, справочного аппарата, включая указатели и библиографию.

### 4.1 Вопросы для собеседования для проверки подготовки к практическим занятиям

**Тема 2: Обобщенные модели защиты информации**

***Базовый уровень***

7. Понятие системы и процессов защиты информации.
8. Управляемые параметры обобщенной модели системы защиты информации.
9. Параметры, на которые система защиты информации может оказывать воздействие.
10. Параметры внешней среды для системы защиты информации.

***Повышенный уровень***

1. Модификации обобщенной модели системы защиты информации.
2. Критерии защищенности объекта информатизации.

**Тема 4: Вероятностные модели систем защиты информации**

***Базовый уровень***

5. Атака на информационную систему.
6. Модель элементарной защиты информации.
7. Модель многозвенной защиты информации.

***Повышенный уровень***

1. Модель многоуровневой защиты информации.

**Тема 5: Реализация игровых моделей в задачах защиты информации**

***Базовый уровень***

9. Конфликтная ситуация.
10. Игры с нулевой суммой.
11. Платежная матрица.
12. Стратегия игры. Чистые стратегии.
13. Седловая точка.

***Повышенный уровень***

1. Смешанные стратегии.
2. Теорема Неймана.
3. Графическое решение игр *2xn* или *mx2.*

**Тема 6: Оценка эффективности систем контроля и управления доступом на основе детерминистического подхода**

***Базовый уровень***

6. Система контроля и управления доступом.
7. Факторы состояния системы контроля и управления доступом.
8. Показатели состояния системы контроля и управления доступом.
9. Организационные мероприятия.

***Повышенный уровень***

1. Инженерно-технические средства охраны.

**Тема 7: Оценка эффективности охраны объекта с помощью метода имитационного моделирования**

***Базовый уровень***

7. Метод имитационного моделирования.
8. Вероятность обнаружения нарушителя.
9. Вероятность нейтрализации нарушителя.
10. Санкционированное проникновение на охраняемый объект.

***Повышенный уровень***

1. Несанкционированное проникновение на охраняемый объект.
2. Эффективность охраны объекта.

**Тема 8: Оценка уровня безопасности информационной системы предприятия на базе модели с лингвистической шкалой**

***Базовый уровень***

8. Нечеткое множество.
9. Способы построения нечетких множеств.
10. Классификация нечетких множеств.

***Повышенный уровень***

1. Лингвистическая переменная.
2. Нечеткий эталон.
3. Превентивные меры защиты.

**Тема 10: Сетевое планирование и управление комплексной защитой информацией**

***Базовый уровень***

1. Сетевой график.
2. События, работы.
3. Продолжительность работы.
4. Действительные и фиктивные работы.
5. Раннее время свершения события.

***Повышенный уровень***

1. Позднее время свершения события.
2. Резервы времени.
3. Критический путь.

**a. Вопросы для собеседования по самостоятельному изучению тем**

**Тема 4: Применение игровых моделей для решения задач защиты информации**

1. Основные термины теории игр.
2. Парные игры с нулевой суммой. Решение в чистых стратегиях.
3. Решение парных игр в смешанных стратегиях. Содержательное описание игровой модели для задачи защиты информационной системы.

**Тема 6: Детерминистический подход к оценке эффективности систем контроля и управления доступом**

1. Особенности выбора систем контроля и управления доступом для конкретных объектов.
2. Основные компоненты систем контроля и управления доступом. Типовые варианты систем контроля и управления доступом.
3. Общая идея детерминистического подхода при оценивании эффективности систем контроля и управления доступом.

**Тема 7: Оценка эффективности охраны объекта с помощью метода имитационного моделирования**

1. Основные сведения об имитационном моделировании.
2. Простейшие задачи, решаемые имитационным моделированием.
3. Метод имитационного моделирования для оценивания эффективности охраны объекта.

**b. Комплект разноуровневых задач и заданий для практических занятий**

***Базовый уровень**:*

1. Понятие системы, ее элементы.
2. Прямые связи между элементами системы.
3. Обратные связи между элементами системы.
4. Эффективность системы.
5. Функционирование системы.
6. Входы и выходы системы.
7. Свойства систем.
8. Классификация систем по различным признакам.
9. Система защиты информации.
10. Понятие системы и процессов защиты информации.
11. Управляемые параметры обобщенной модели системы защиты информации.

12. Параметры, на которые система защиты информации может оказывать воздействие.
13. Параметры внешней среды для системы защиты информации.
14. Модификации обобщенной модели системы защиты информации.
15. Критерии защищенности объекта информатизации.
16. Случайное событие.
17. Элементарное событие.
18. Пространство элементарных событий.
19. Достоверное событие.
20. Равносильные события.
21. Совместные события.
22. Несовместные события.
23. Полная группа событий.
24. Числовые характеристики случайных величин.
25. Теоремы сложения несовместных событий.
26. Теоремы сложения совместных событий.
27. Теорему умножения зависимых событий.
28. Теорема умножения независимых событий.
29. Формула полной вероятности.
30. Формула Байеса.
31. Вероятностные модели защиты информации.
32. Атака на информационную систему.
33. Модель элементарной защиты информации.
34. Модель многозвенной защиты информации.
35. Модель многоуровневой защиты информации.
36. Конфликтная ситуация.
37. Игра. Правила игры.
38. Парная, множественная игры.
39. Игры с нулевой суммой.
40. Платежная матрица.
41. Чистые стратегии игроков.
42. Нижняя цена игры.
43. Верхняя цена игры.
44. Принцип минимакса.
45. Седловая точка.
46. Теорема Неймана.
47. Терема об активных стратегиях игроков.
48. Общая схема решения игр с нулевой суммой.
49. Система контроля и управления доступом.
50. Назначение системы контроля и управления доступом.
51. Устройства идентификации доступа.
52. Устройства контроля и управления доступом.
53. Устройства центрального управления.
54. Исполнительные устройства.
55. Системы контроля и управления доступом для автономного режима работы.
56. Системы контроля и управления доступом для сетевого режима работы.
57. Понятие эффективности системы контроля и управления.
58. Детерминистический подход к оценке эффективности системы контроля и управления доступом.
59. Системы массового обслуживания.
60. Показатели эффективности систем массового обслуживания.

*Повышенный уровень:*

61. Системы массового обслуживания с отказами.
62. Системы массового обслуживания с ожиданием.
63. Фаза валидации в имитационном моделировании.
64. Фаза проектирования в имитационном моделировании.
65. Фаза верификации в имитационном моделировании.
66. Идея метода Монте-Карло для имитации процессов, проходящих во времени.
67. Метод имитационного моделирования для оценивания эффективности охраны объекта.
68. Метод имитационного моделирования.
69. Вероятность обнаружения нарушителя.
70. Вероятность нейтрализации нарушителя.
71. Санкционированное проникновение на охраняемый объект.
72. Несанкционированное проникновение на охраняемый объект.
73. Эффективность охраны объекта.
74. Понятие нечеткого множества.
75. Функция принадлежности.
76. Основные характеристики нечетких множеств.
77. Операции над нечеткими множествами.
78. Нечеткая и лингвистическая переменные.
79. Нечеткая модель с лингвистической шкалой.
80. Нечеткая модель с балльной шкалой.
81. Нечеткий эталон.
82. Этапы сетевого планирования.
83. Сетевая модель.
84. Сетевой график.
85. Исходные характеристики работ.
86. Виды путей в сетевом графике.
87. Правила построения сетевого графика.
88. Собственные характеристики работ.
89. Системные характеристики работ.
90. Системные характеристики событий.
91. Характеристики путей сетевого графика.
92. Содержание организационной процедуры «Сетевое планирование и управление».

**Перечень литературы необходимый для освоения дисциплины**

**Основная литература:**

1. Киреева, Н. В. Эффективность системы защиты информации на основе экспертных систем : методические указания / Н. В. Киреева, И. С. Поздняк. — Самара : ПГУТИ, 2021. — 29 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/301109

2. Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика : учебное пособие : [16+] / В. Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. : схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=571485

**Дополнительная литература:**

1. Мамонова, В. Г. Моделирование бизнес - процессов : учебное пособие / В. Г. Мамонова . - Новосибирск : Изд-во НГТУ, 2012 . Режим доступа:
2. http://www.rucont.ru/efd/205851

**Методическая литература**:

Электронный курс лекций.

Электронные методические рекомендации для выполнения практических заданий.

**Интернет-ресурсы:**

Белов Е.Б. Основы информационной безопасности. Учебное пособие для вузов/Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2013, - 544 с. – Доступно: http://www.alleng.ru/d/comp/comp51.htm

Воройский Ф.С. Информатика. Энциклопедический словарь-справочник: введение в современные информационные и телекоммуникационные технологии в терминах и фактах. - М.: ФИЗМАТЛИТ, 2013. - 768 с. – Доступно: http://physics-for-students.ru/bookpc/informatika/slovar.zip