МТУСИ

Факультет «Кибернетика и информационная безопасность»

Кафедра «Информационная безопасность»

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

ПРАКТИЧЕСКОЕ ЗАДАНИЕ

по дисциплине

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Москва 2025

ВВЕДЕНИЕ

Выполнение практического задания имеет целью привить студентам навыки самостоятельной работы, выявить их знания по дисциплине «Основы информационной безопасности», оценить свое умение применять эти знания на практике.

Объектом исследования является информационная система предприятия (объект информатизации), которая восприимчива к ряду угроз, способных нанести ущерб имеющемуся информационному ресурсу.

В процессе выполнения курсовой работы студенты должны:

- научиться самостоятельно работать с учебной и научно-технической литературой;
- уметь осваивать теорию по теме работы;
- проявить умение анализировать и обобщать полученные знания, делать обоснованные выводы;
- уметь формулировать рекомендации по выбору методов и средств для решения поставленной задачи;
- получить навыки и компетенции для создания основ соответствующего программного обеспечения.

1. ЦЕЛИ И ЗАДАЧИ ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОГО ЗАДАНИЯ

Целью работы является закрепление и углубление теоретических знаний в области методологии и методов обеспечения информационной безопасности, в частности, в области анализа и синтеза систем защиты информации в автоматизированных информационных системах (ИС) и компьютерных сетях, а также приобретение навыков расчета финансовых рисков, реализующихся через уязвимости информационных активов, и оценки эффективности применяемых мер.

Задачи работы:

1. Изучить теоретические основы анализа и синтеза систем защиты информации (СЗИ) информационных систем и сетей.
2. На этапе проектирования СЗИ уметь определять приемлемый для организации (компании) уровень риска, обеспечивающий выполнение своих функциональных задач.
3. Для оценки рисков информационной системы организации уметь определять защищенность ее каждого ценного ресурса при помощи анализа угроз, действующих на конкретный ресурс, и уязвимостей, через которые эти угрозы могут быть реализованы.
4. Оценить вероятность реализации актуальных для ценного ресурса угроз и степень влияния реализации угрозы на ресурсы.
5. Уметь анализировать информационные риски ресурсов организации.

6. Уметь на заключительном этапе проводить анализ эффективности предложенных мероприятия по устранению выявленных уязвимостей.

7. При выполнении задания курсовой работы необходимо получить следующие данные (ответы на поставленные вопросы):

- ***риск реализации по трем базовым угрозам*** (или по одной суммарной угрозе) *для ресурса*;
- ***суммарный риск реализации по всем угрозам*** *для ресурса*;
- ***риск реализации по трем базовым угрозам*** (или по одной суммарной угрозе) *для информационной системы*;
- ***риск реализации по всем угрозам*** для информационной системы *до контрмер*;
- ***риск реализации по всем угрозам*** для информационной системы *после контрмер*;
- ***оценка эффективности*** *контрмеры*;
- ***оценка эффективности*** *комплекса контрмер*.

2. ЗАДАНИЯ НА КУРСОВУЮ (КОНТРОЛЬНУЮ) РАБОТУ

2.1 Типовой сценарий деятельности организации

Руководитель коммерческой организации действует в условиях рынка в некоем регионе. Организация обладает собственными коммерческими секретами и занимается одним из следующих видов деятельности, например (табл.1):

A – производство электронных устройств;

B – разработка программных продуктов;

C **-** коммерческая деятельность (торговля бытовой радиоэлектроникой);

D – бытовые услуги населению.

Далее необходимо кратко:

1. Условно определить название предприятия, вид ее деятельности, число руководителей.
2. Определить и описать мероприятия для осуществления контроля качества информации предприятия.
3. Определить составляющие информационной базы данных.
4. Описать способ организации и обеспечения ответственности при управлении информацией.
5. Составить политику безопасности информации.
6. Составить перечень информационных активов предприятия, требующих защиты, и произвести их оценку.
7. Определить количество, состав и уровень угроз и уязвимостей бизнеса, оценить риски и наметить мероприятия по комплексу контрмер оцененным угрозам.

2.2 Что требуется определить в результате выполнения практической работы

В соответствии с исходными данными (табл.1), необходимо осуществить:

- *расчет уровня угрозы по уязвимости* T_h на основе критичности и вероятности реализации угрозы через данную уязвимость;
- *расчет уровня угрозы по всем уязвимостям* UU_h, через которые возможна реализация данной угрозы на ресурсе с одной базовой угрозой или с тремя базовыми угрозами;
- *расчет общего уровня угроз по ресурсу* CT_hR (учитываются все угрозы, действующие на ресурс);
- *расчет риска по ресурсу* R с одной базовой угрозой или с тремя базовыми угрозами;
- *расчет риска* по информационной системе SR с одной базовой угрозой или с тремя базовыми угрозами;
- *расчет эффективности введенной контрмеры*;
- *расчет эффективности комплекса контрмер*.

2.3 Варианты заданий для выполнения курсовой (контрольной) работы

Варианты заданий для выполнения практического задания содержаться в табл.1., где:

N - количество базовых угроз (1 или 3);

$КУг$ - число угроз, действующих на ресурсы, i = 1,2…;

$КУя$ - число уязвимостей, через которые реализуется каждая угроза (считается одинаковым для каждой угрозы), , j = 1,2…;

$Куу$ - число устраненных уязвимостей (введенных контрмер).

Таблица 1

№ варианта	Деятельность предприятия	*N*	*КУг, i всего*	*КУя, j всего*	*Куу*
1	A	1	2	5	1
2	B	3	3	4	2
3	C	1	4	3	3
4	D	3	5	2	1
5	A	1	3	4	2
6	B	3	4	3	3
7	C	1	5	2	1
8	D	3	2	4	2
9	A	1	4	3	3
10	B	3	5	4	1
11	C	1	2	3	2
12	D	3	3	5	3
13	A	1	5	3	1
14	B	3	2	5	2
15	C	1	3	4	3
16	D	3	4	3	1
17	A	1	5	2	2
18	B	3	4	3	3
19	C	1	3	4	1
20	D	3	2	5	2
21	A	1	5	3	1
22	B	3	4	2	2
23	C	1	3	3	3
24	D	3	2	4	1
25	A	1	5	3	2

3. ВЫПОЛНЕНИЕ РАБОТЫ

3.1. Основные шаги выполнения курсовой (контрольной) работы

1. Определить название предприятия, вид ее деятельности, количество руководителей. Например:

Название: ООО «Фикус-ИТ» (условно).
Вид деятельности – Разработка программных продуктов.
Количество руководителей – один.

2. Определить мероприятия для осуществления контроля качества информации предприятия.

Качественная производственная информация характеризуется такими основными характеристиками (качествами), как *целостность, надежность и конфиденциальность*, которые нуждаются в защите. Для поддержания данных качеств потребуется проведение организационных мероприятий, например:

– развертывание системы контроля и разграничение физического доступа к автоматизированной информационной системе;

– создание службы охраны и физической безопасности;

– организация механизмов контроля над перемещением сотрудников и посетителей;

– разработка и внедрение регламентов, должностных инструкций и других регулирующих документов;

– регламентация порядка работы с носителями, содержащими конфиденциальную информацию;

– периодическое копирование базы данных и др.

3. Определить составляющие информационной базы предприятия.

Чтобы определить составляющие информационной базы предприятия, необходимо определить организационную структуру, пример приведен ниже.

1. *Генеральный директор – Петров А.В.*
2. *Коммерческий директор – Сидоров И.А.*
3. *Менеджер по продажам/закупкам – Штельман Д.И.*
4. *Главный бухгалтер – Абрамов Н.Ф.*
5. *Главный программист – Лисин А.Н.*
6. *Тестировщик ПО – Гостев С.А.*
7. *Оператор на телефоне – Зуева С.А.*

4. Используемые при разработке ПО платформы и технологии.

Разработка программного обеспечения реализуется нами на современных платформах и технологиях, например:

- серверы приложений: Microsoft: .Net, IIS, COM+, J2EE: Oracle Application Server;
- базы данных: Oracle, Microsoft SQL Server, Interbase, MySQL;

- системы построения отчетности: CrystalReports, OracleReports;
- инструменты компьютерного моделирования и проектирования: UML, RationalRose, ERwin, BPwin, ARIS, PowerDesigner, Visio;
- среды разработки: Microsoft Visual Studio, Oracle JDeveloper, Delphi, Borland JBuilder;
- платформы: Microsoft Windows NT/2000/XP/Vista/7, Sun Solaris/ UNIX/ AIX/Linux/HP UX;
- языки программирования: Java, C, VB.Net, VB, C/C++, SQL/PL/SQL/TransactSQL;
- технологии: Microsoft: ASP.NET, Microsoft Silverlight и .NET Framework;
- средства защиты информации: SSL, CryptoPRO.

Предприятие обладает современной информационно-коммуникационной инфраструктурой, которая позволяет выполнять проекты любой сложности и обеспечивать эффективное взаимодействие с клиентами. Разработка и тестирование ПО может вестись на оборудовании предприятия, с последующим переносом готового продукта на платформу заказчика.

5. Составить перечень информации, требующей защиты.

Наибольшую ценность для предприятия представляют сервер БД и сервер приложений, так как нарушение конфиденциальности, целостности и доступности в случае инцидента, повлечёт за собой существенные затраты.

Например, раскрытие или уничтожение перечня заказчиков или производственных спецификаций может означать для предприятия потерю части рынка или утрату стратегического преимущества.

6. Составить классификационную политику защиты информации для предприятия.

Например, политика по ЗИ реализуется в соответствии с табл.2.

Таблица 2

Метка конфиденциальности			
Субъективные классификации	**Конфиденциальная 1**	**Конфиденциальная 2**	**Конфиденциальная 3 (ПД)**
Определение	Раскрытие может нанести в перспективе ущерб экономике предприятия	Раскрытие может нанести в перспективе ущерб экономике предприятия	Раскрытие может негативно повлиять на сотрудников или претендентов на должность

7. Описать способ организации и обеспечения ответственности в области управления информацией предприятия.

Например, на предприятии типично действуют три уровня доступа к информации:

1) высший (генеральный директор, коммерческий директор),

2) средний (главный программист, главный бухгалтер, тестировщик ПО),

3) низший (менеджер по продажам/закупкам, дизайнер, оператор на телефоне).

Высший уровень: руководитель по информации определяет структуру основных элементов информации для производства; определяет схему классификации информации; идентифицирует для каждого элемента информации его обладателя, который производит засекречивание и принимает решения относительно авторизованного доступа; выполняет исполнительный контроль над информационным ресурсом производства.

Средний уровень: администратор данных устанавливает структуру административного контроля по управлению основной информационной базой; через администратора баз данных фиксирует оптимальное размещение данных на центральных базах данных (чему может способствовать публикация словаря данных, который описывает создание элементов данных и стандартные процессы их получения из баз данных).

Низший уровень: специалист по информационной безопасности выполняет меры защиты, требуемые для аппаратных и программных средств.

8. Определить информационные активы компании.

Чтобы определить ценность актива, организация сначала должна сама идентифицировать свои активы (на соответствующем уровне детализации).

Можно выделить два типа активов:

- ***первичные активы:***
  - бизнес-процессы и действия;
  - информация;
- ***активы поддержки*** (на которые полагаются первичные элементы области применения) всех типов:
  - аппаратные средства;
  - программное обеспечение;
  - сеть;
  - персонал;
  - сайт;
  - организационная структура.

К *первичным активам* относятся сведения о сотрудниках и заказчиках, а также конфиденциальная информация, связанная с бизнес-процессом.

К *активам поддержки* относятся:

- ***Аппаратное обеспечение.***

1. Стационарное оборудование:
   - сервер БД;
   - сервер приложений;
   - рабочие станции (персональные компьютеры).
2. Периферийные устройства обработки данных: МФУ.

3. Электронные носители информации:
   - USB-flash; CD-диски; съемные жесткие диски.

- ***Программное обеспечение:***

1 ОС рабочих станций и серверов:
   - Microsoft Windows /XP/Vista/7; Sun Solaris/UNIX/AIX/Linux/HP UX; Palm OS/Pocket PC/Windows CE.

2. Базы данных:
   - Oracle; Microsoft SQL Server; Interbase; MySQL

3. Системы построения отчетности:
   - CrystalReports; OracleReports.

4. Инструменты компьютерного моделирования и проектирования:
   - UML; RationalRose; Erwin; BPwin; ARIS; PowerDesigner; Visio

5. Среды разраотки:
   - Microsoft Visual Studio; Oracle JDeveloper; Delphi, Borland JBuilder.

9. Оценка актива. Уязвимости и методы для оценки уязвимости

9.1 Ниже в табл.3 показаны типовые угрозы, которые могут нанести ущерб предприятию через имеющиеся уязвимости.

Таблица 3

№	Угрозы	Уязвимости
1	**Кража носителей или документов**	Незащищённое хранение
		Недостаточная осторожность при утилизации
		Неконтролируемое копирование
		Отсутствие физической защиты здания
		Неконтролируемая работа стороннего или уборочного персонала
		Отсутствие или недостаточная политика "чистого стола и чистого экрана"
		Отсутствие подтверждения прав на использование средств обработки информации
		Недостаточный контроль со стороны физической защиты
		Отсутствие установленных механизмов мониторинга за нарушениями безопасности
2	**Злоупотребление правами**	Неправильное распределение прав доступа
		Отсутствие или недостаточное тестирование ПО
		Известные «дыры» в ПО
		Отсутствие журнала аудита
		Отсутствие "выхода из системы" при покидании рабочей станции
		Утилизация или повторное использование носителей без надлежащего удаления данных
		Отсутствие официальной процедуры для регистрации и отмены регистрации пользователей
		Отсутствие официального процесса для проверки прав доступа (надзора)
		Отсутствие или недостаточные положения (об обеспечении безопасности) в договорах с клиентами и/или третьими лицами

		Отсутствие процедуры мониторинга средств обработки информации
		Отсутствие регулярных проверок
		Отсутствие процедур идентификации и оценки рисков
		Отсутствие сообщений о неисправностях, регистрируемых в журналах администратора и оператора
3	**Неправильное функционирование программного обеспечения**	Недоработанное или новое ПО
		Нечеткие или неполные спецификации для разработчиков
		Отсутствие контроля инсталляции неразрешенного ПО
		Отсутствие правил и контроля обновления ПО
		Отсутствие действенного контроля изменений
4	**Незаконная обработка данных**	Наличие ненужных разрешённых сервисов
		Отсутствие механизмов мониторинга
		Отсутствие достаточных положений в договорах с сотрудниками
5	**Ошибка при использовании**	Недостаточное обучение вопросам обеспечения безопасности
		Неверная настройка параметров
		Отсутствие политики использования электронной почты
		Отсутствие эффективного контроля за изменением конфигурации
		Усложненный пользовательский интерфейс
		Отсутствие документации
		Неправильное использование программного и аппаратного обеспечения
		Отсутствие осведомленности о безопасности
		Отсутствие процедур включения ПО в действующие системы
		Отсутствие обязанностей по обеспечению информационной безопасности в должностных инструкциях

Например, в ходе проведения плановых мероприятий, уязвимости, *отмеченные серым цветом*, были устранены (условное число $\boldsymbol{K_{yy}}$ в табл.1).

Далее приведен типовой пример расчета риска информационной безопасности на основе модели угроз и уязвимостей. Расчет рисков проводится *для одного* информационного актива (ресурса) предприятия, для остальных активов риск рассчитывается аналогично.

Считается, что для одного ресурса (сервера БД с критичностью 100 у.е.) действуют 5 видов угроз, которые реализуются через соответствующие уязвимости, как показано ниже в табл.4.

Задаются вероятности реализации 5-и угроз через соответствующие уязвимости (в течение года), а также критичности реализации угроз. Эти значения представлены в табл.5.

Таблица 4

Изменить	Угрозы (5)	Уязвимости
Сервер БД (критичность ресурса 100 у.е.)	**Угроза 1:** Кража носителей или документов	1.1 Недостаточная осторожность при утилизации
		1.2 Неконтролируемое копирование
		1.3 Отсутствие подтверждения прав на использование средств обработки информации
		1.4 Недостаточный контроль со стороны физической защиты
		1.5 Отсутствие установленных механизмов мониторинга за нарушениями безопасности
	Угроза 2: Злоупотребление правами	2.1 Недостаточное тестирование ПО
		2.2 Отсутствие журнала аудита
		2.3 Отсутствие "выхода из системы" при покидании рабочей станции
		2.4 Утилизация или повторное использование носителей без надлежащего удаления данных
		2.5 Отсутствие процедуры мониторинга средств обработки информации
	Угроза 3: Неправильное функционирование ПО	3.1 Недоработанное / новое ПО
		3.2 Нечеткие или неполные спецификации для разработчиков
		3.3 Отсутствие контроля инсталляции неразрешенного ПО
		3.4 Отсутствие правил и контроля обновления ПО
	Угроза 4: Незаконная обработка данных	4.1 Наличие ненужных разрешённых сервисов
		4.2 Отсутствие достаточных в договорах с сотрудниками
	Угроза 5: Ошибка при использовании	5.1 Недостаточное обучение вопросам обеспечения безопасности
		5.2 Отсутствие политики использования электронной почты
		5.3 Усложненный пользовательский интерфейс
		5.4 Отсутствие процедур включения программного обеспечения в действующие системы
		5.5 Отсутствие обязанностей по обеспечению ИБ в должностных инструкциях

Таблица 5

Угроза/Уязвимость	Вероятность реализации ***i***-й угрозы через ***j***-ю уязвимость в течение года (%), $P(V)_{ij}$	Критичность реализации ***i***-й угрозы через ***j***-ю уязвимость (%), KR_{ij}
Угроза 1/Уязвимость 1	25	60
Угроза 1/Уязвимость 2	40	60
Угроза 1/Уязвимость 3	10	50
Угроза 1/Уязвимость 4	15	40
Угроза 1/Уязвимость 5	30	40
Угроза 2/Уязвимость 1	30	30
Угроза 2/Уязвимость 2	45	20
Угроза 2/Уязвимость 3	50	60
Угроза 2/Уязвимость 4	40	30
Угроза 2/Уязвимость 5	50	60
Угроза 3/Уязвимость 1	70	80
Угроза 3/Уязвимость 2	50	65
Угроза 3/Уязвимость 3	40	50
Угроза 3/Уязвимость 4	60	65
Угроза 4/Уязвимость 1	30	70
Угроза 4/Уязвимость 2	20	50
Угроза 5/Уязвимость 1	35	55
Угроза 5/Уязвимость 2	25	40
Угроза 5/Уязвимость 3	20	40
Угроза 5/Уязвимость 4	30	60
Угроза 5/Уязвимость 5	25	50

9.2. Оценка уровней угроз (для выбранного ресурса) через соответствующие уязвимости представлена в табл.6 ниже.

Таблица 6

Угроза/Уязвимость	**Уровень *i*-й угрозы через *j*-ю уязвимости** $Th_{ij} = \frac{P(V)_{ij}}{100} \times \frac{KR_{ij}}{100}$	**Уровень *i*-й угрозы по всем *Куя* уязвимостям, через которые она реализуется:** *Куя* $UUh_i = 1 - \prod_{j=1}(1 - Th_{ij})$
Угроза 1/Уязвимость 1	0,15	0,423
Угроза 1/Уязвимость 2	0,24	
Угроза 1/Уязвимость 3	0,05	
Угроза 1/Уязвимость 4	0,06	
Угроза 2/Уязвимость 1	0,09	0,420
Угроза 2/Уязвимость 2	0,09	
Угроза 2/Уязвимость 3	0,30	

Угроза 3/Уязвимость 1	0,56	0,703
Угроза 3/Уязвимость 2	0,32	
Угроза 4/Уязвимость 1	0,21	0,289
Угроза 4/Уязвимость 2	0,10	
Угроза 5/Уязвимость 1	0,19	0,272
Угроза 5/Уязвимость 2	0,02	
Угроза 5/Уязвимость 3	0,08	

9.3. Результаты расчета общего уровня угроз, действующих на ресурс, показан в табл.7.

Таблица 7

Угроза/Уязвимость	**Уровень *i-й* угрозы по всем уязвимостям, через которые она реализуется, UUh_i**	**Общий уровень угроз *UUhR* по ресурсу *Куг* $UUhR = 1 - \prod_{i=1}^{}(1 - UUh_i)$**
Угроза 1/Уязвимость 1	0,423	0,9486
Угроза 1/Уязвимость 2		
Угроза 1/Уязвимость 3		
Угроза 1/Уязвимость 4		
Угроза 2/Уязвимость 1	0,420	
Угроза 2/Уязвимость 2		
Угроза 2/Уязвимость 3		
Угроза 3/Уязвимость 1	0,703	
Угроза 3/Уязвимость 2		
Угроза 4/Уязвимость 1	0,289	
Угроза 4/Уязвимость 2		
Угроза 5/Уязвимость 1	0,272	
Угроза 5/Уязвимость 2		
Угроза 5/Уязвимость 3		

9.4. Оценка риска ресурса (сервера БД).

Заданная критичность ресурса (ущерб, который понесет компания от потери ресурса) составляет 100 у.е., что определяет его риск (табл.8).

Таблица 8

Угроза/Уязвимость	**Общий уровень угроз по выбранному ресурсу, *UUhR***	**Риск ресурса (у.е.), *R***
Угроза 1/Уязвимость 1	0,9486	94,9
Угроза 1/Уязвимость 2		
Угроза 1/Уязвимость 3		
Угроза 1/Уязвимость 4		
Угроза 2/Уязвимость 1		
Угроза 2/Уязвимость 2		
Угроза 2/Уязвимость 3		
Угроза 3/Уязвимость 1		
Угроза 3/Уязвимость 2		

Угроза 4/Уязвимость 1		
Угроза 4/Уязвимость 2		
Угроза 5/Уязвимость 1		
Угроза 5/Уязвимость 2		
Угроза 5/Уязвимость 3		

Таким образом, получен риск ресурса (94,9 у.е.), рассчитанный по модели 5-и угроз и соответствующих уязвимостей. В данных условиях годичный риск угрозам серверу велик и приближается к его стоимости.

Выводы

Оценка потенциальных (финансовых) рисков является эффективным механизмом управления информационной безопасностью на предприятии, позволяющим:

- идентифицировать и оценить существующие информационные активы предприятия;
- оценить необходимость внедрения средств защиты информации;
- оценить эффективность уже внедренных средств защиты информации.

СПИСОК ЛИТЕРАТУРЫ

1. Ховард М., Лебланк Д. Защищенный код. - М.: Издательско-торговый дом «Русская редакция», 2004. – 704 с.
2. SO/IEC 27005 Информационная технология: Методы защиты – Менеджмент рисков информационной безопасности. Международный стандарт.
3. Малюк А.А. Теория защиты информации: Учебное пособие. - М.: Горячая линия-Телеком, 2014. - 184 с.
4. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. - М.: Горячая линия-Телеком, 2000. – 452 с.

ПРИЛОЖЕНИЕ

Теоретические сведения, необходимые для написания курсовой (контрольной) работы

В общем виде процесс анализа рисков информационной безопасности (ИБ) некой информационной системы (актива предприятия) сводится к следующей последовательности (алгоритму):

1. Описание исследуемой информационной системы (ИС).
2. Идентификация и оценка угроз.
3. Идентификация и оценка уязвимостей.
4. Идентификация существующих и планируемых мер защиты информации.
5. Расчет и оценка рисков ИБ.
6. Выработка предложений по снижению рисков.

1.1. Модель анализа угроз и уязвимостей

Чтобы оценить риск потери информации, необходимо проанализировать:

- *все угрозы,* действующие на информационную систему,
- *все уязвимости*, через которые возможна реализация угроз.

Исходя из имеющихся данных (например, введенных владельцем информационной системы) можно построить модель угроз и уязвимостей, актуальных для компании. На основе полученной модели анализируются вероятности реализации угроз информационной безопасности на каждый ресурс и рассчитываются соответствующие риски.

1.2. Основные понятия и особенности модели

Базовые угрозы информационной безопасности предприятия: нарушение *конфиденциальности*, *целостности* и *доступности* (отказ в обслуживании) информации.

Ресурс: любой условный контейнер, предназначенный для хранения информации, подверженный угрозам информационной безопасности (сервер, рабочая станция, переносной компьютер и пр.).

Свойства ресурса: перечень угроз, воздействующих на него, и критичность ресурса.

Угроза: действие, которое потенциально может привести к нарушению безопасности. Свойством угрозы является перечень уязвимостей, при помощи которых может быть реализована угроза.

Уязвимость: слабое место в информационной системе, которое может привести к нарушению безопасности путем реализации некоторой угрозы.

Свойства уязвимости: вероятность (простота) реализации угрозы через данную уязвимость и критичность реализации угрозы через данную

уязвимость.

Критичность ресурса AC: степень значимости ресурса для информационной системы (как сильно реализация угроз на ресурс повлияет на работу информационной системы). Задается в уровнях (количество уровней может быть в диапазоне от 2 до 100) или в деньгах.

В зависимости от выбранного режима работы критичность ресурса состоит из критичности по:

- *конфиденциальности* AC_c*, целостности* AC_i*, доступности* AC_a.

Критичность реализации угрозы KR – степень влияния реализации угрозы на ресурс, т.е. как сильно реализация угрозы повлияет на работу ресурса. Задается в % и состоит из критичности реализации угрозы по:

- *конфиденциальности* KR_c*, целостности* KR_i*, доступности* KR_a.

***Вероятность реализации угрозы через данную уязвимость в течение года P(V)*:** вероятность реализации угрозы через данную уязвимость в тех или иных условиях; указывается в %.

Максимальное критичное время простоя T_{max}**:** значение времени простоя, которое является критичным для организации, когда ущерб, нанесенный организации, максимальный.

При простаивании ресурса в течение времени, превышающего критичное, ущерб, нанесенный организации, не увеличивается.

1.3. Расчет рисков (потенциальных, финансовых)

Входные данные:

- ресурсы;
- критичность ресурсов;
- отделы, к которым относятся ресурсы;
- угрозы, действующие на ресурсы;
- уязвимости, через которые реализуются угрозы;
- вероятность реализации угрозы через данную уязвимость;
- критичность реализации угрозы через данную уязвимость.

С точки зрения базовых угроз информационной безопасности существует два режима расчета и работы алгоритма (табл.1):

- ***одна базовая угроза*** *(суммарная);*
- ***три базовые угрозы***.

1.4.Расчет рисков угроз информационной безопасности

1. Первый этап

Рассчитывается уровень i-й угрозы по j-й уязвимости Th_{ij} на основе критичности и вероятности реализации угрозы. *Уровень* Th_{ij} показывает, насколько критичным является воздействие на ресурс *i-й* угрозы через *j-ю*

уязвимость:

$$\boldsymbol{Th_{ij}} = \frac{\boldsymbol{P(V)_{ij}}}{\mathbf{100}} \times \frac{\boldsymbol{KR_{ij}}}{\mathbf{100}}$$

где $\boldsymbol{KR_{ij}}$ – критичность реализации угрозы (указывается в %);

$\mathbf{P}(\boldsymbol{V})_{ij}$ – вероятность реализации ***i***-й угрозы через ***j***-ю уязвимость (указывается в %).

В зависимости от количества базовых угроз (***Кбу***, табл.1) вычисляются одно или три значения. В результате получаются значения уровней угроз в интервале **0…1**.

2. Второй этап

Рассчитывается уровень $\boldsymbol{UUh_i}$ реализации ***i-й*** угрозы *по всем уязвимостям* (на ресурсе), путем суммирования полученных уровней угроз через все ***Куя*** уязвимости.

2.1.Для режима с *одной базовой угрозой* (***Кбу*** =1, табл.1):

$$\boldsymbol{UUh_i} = \mathbf{1} - \prod_{\boldsymbol{j=1}}^{\boldsymbol{Куя}} \left(\mathbf{1} - \boldsymbol{Th_{ij}}\right)$$

2.2.Для режима с *тремя базовыми угрозами* 1,2,3

$$\boldsymbol{UUh_{1i}} = \mathbf{1} - \prod_{\boldsymbol{j=1}}^{\boldsymbol{Куя_1}} \left(\mathbf{1} - \boldsymbol{Th_{ij1}}\right)$$

$$\boldsymbol{UUh_{2i}} = \mathbf{1} - \prod_{\boldsymbol{j=1}}^{\boldsymbol{Куя_2}} \left(\mathbf{1} - \boldsymbol{Th_{ij2}}\right)$$

$$\boldsymbol{UUh_{3i}} = \mathbf{1} - \prod_{\boldsymbol{j=1}}^{\boldsymbol{Куя_3}} \left(\mathbf{1} - \boldsymbol{Th_{ij3}}\right)$$

Все величины уровней угроз находится в интервале значений **0…1**.

3. Третий этап. Расчет общего уровня угроз по ресурсу *UUhR*

Общий уровень угроз рассчитывается аналогично пункту 2 - учитываются все ***Куг*** угроз, действующих на ресурс:

3.1 Для режима с *одной базовой угрозой*:

$$UUhR = 1 - \prod_{i=1}^{Kуг} (1 - UUh_i)$$

3.2 Для режима с *тремя базовыми угрозами* 1,2,3:

$$UUhR_1 = 1 - \prod_{i=1}^{Kуг_1} (1 - UUh_{1i})$$

$$UUhR_2 = 1 - \prod_{i=1}^{Kуг_2} (1 - UUh_{2i})$$

$$UUhR_3 = 1 - \prod_{i=1}^{Kуг_3} (1 - UUh_{3i})$$

Значение общего уровня угроз также находится в интервале **0…1**.

4. Четвертый этап. Расчет риска *R* по всему ресурсу

Риск рассчитывается следующим образом:

4.1 Для режима с *одной базовой угрозой*:

$$R = UUhR \times D,$$

где D − критичность ресурса, которая задается в уровнях или деньгах (например, у.е.).

В случае угрозы доступности (отказ в обслуживании) критичность ресурса за год вычисляется по формуле:

$$D_{a/год} = D_{a/час} \times T$$

Для остальных угроз критичность ресурса задается за год.

4.2 Для режима с *тремя базовыми угрозами*:

$$R_1 = UUhR_1 \times D_1,$$
$$R_2 = UUhR_2 \times D_2,$$
$$R_3 = UUhR_3 \times D_3,$$

где D_1, D_2, D_3 – критичность ресурса по каждой из трех угроз соответственно. Суммарный риск по трем угрозам (в деньгах или уровнях) есть:

$$R = (1 - \prod_{i=1}^{3} (1 - \frac{R_i}{100})) \times 100$$

В результате получается значение ***риска по ресурсу*** в уровнях (заданных пользователем) или деньгах.

5 Пятый этап. Риск *SR* по всей информационной системе

Риск по всей ИС рассчитывается так:

5.1 *Для режима с одной базовой угрозой:*

5.1.1) Для режима работы в деньгах:

$$\boldsymbol{SR = \sum_{k=1}^{n} R_k}$$

где k = 1,2…n - количество ресурсов

5.1.2) Для режима работы в уровнях:

$$\boldsymbol{SR = \left(1 - \prod_{i=1}^{n}(1 - R_i)\right) \times 100}$$

5.2 *Для режима работы с тремя угрозами:*

5.2.1) Для режима работы *в деньгах*:

Риск системы по каждому виду угроз:

$$\boldsymbol{S = \sum_{k=1}^{n} R_k}$$

Суммарный риск системы по трем видам угроз:

$$\boldsymbol{SR = \sum_{k=1}^{3} SR_{a,c,i}}$$

5.2.2) Для режима работы *в уровнях*:

по каждой угрозе:

$$\boldsymbol{SR_{a,c,i} = \left(1 - \prod_{k=1}^{n}(1 - 100R_k)\right) \times 100}$$

по всем трем угрозам:

$$\boldsymbol{SR = \left(1 - \prod_{k=1}^{3}\left(1 - {}^{R_{a,c,i}}/_{100}\right)\right) \times 100}$$

1.6 Задание контрмер

Для расчета эффективности введенной контрмеры необходимо пройти последовательно по всему алгоритму с учетом заданных контрмер, которые устраняют одну или несколько уязвимостей, - их общее количество (***Куя***, табл.1) при этом уменьшается.

На выходе получаются значения 2-х рисков:

- риска без учета контрмеры **(R_{old})** – значение, полученное ранее;
- риска с учетом заданных контрмер **(R_{new})** или с учетом того, что некоторые уязвимости закрыты.

Эффективность (Э) введения контрмеры рассчитывается по формуле:

$$Э = \frac{R_{old} - R_{new}}{R_{old}}.$$

Вычисленное значение эффективности введенных контрмер является результатом выполнения практического задания