Санкт-Петербургское государственное бюджетное
профессиональное образовательное учреждение
«Академия управления городской средой, градостроительства и печати»

УТВЕРЖДАЮ
Заместитель директора
по учебно-производственной работе
_____ О.В. Фомичева
«26» декабря 2023 г.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по выполнению практических работ
по МДК.05.01 Основы управления информационной безопасностью
ПМ.05 УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

для специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем

Санкт-Петербург
2023 г.

Методические рекомендации рассмотрены на заседании методического совета СПб ГБПОУ «АУГСГиП»

Протокол № 2 от «29» ноября 2023 г.

Методические рекомендации одобрены на заседании цикловой комиссии общетехнических дисциплин и компьютерных технологий

Протокол № 4 от «21» ноября 2023 г.

Председатель цикловой комиссии: Караченцева М.С. _____

Разработчики: преподаватели СПб ГБПОУ «АУГСГиП»

С О Д Е Р Ж А Н И Е

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА 4

1 ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ РАБОТ ПО ТЕМАМ МДК 05.01 «ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ» 6

Практическая работа № 1 8
Практическая работа № 2 8
Практическая работа № 3 9
Практическая работа № 4 10
Практическая работа № 5 10
Практическая работа № 6 10
Практическая работа № 7 10
Практическая работа № 8 11
Практическая работа № 9 11
Практическая работа № 10 12
Практическая работа № 11 12
Практическая работа № 12 12
Практическая работа № 13 12
Практическая работа № 14 12
Практическая работа № 15 13
Практическая работа № 16 13
Практическая работа № 17 15
Практическая работа № 18 18
Практическая работа № 19 19
Практическая работа № 20 19

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Рабочая тетрадь для выполнения практических работ предназначена для организации работы на практических занятиях по МДК.05.01 «Основы управления информационной безопасностью», которая является важной составной частью в системе подготовки специалистов среднего профессионального образования по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Практические занятия являются неотъемлемым этапом изучения МДК и проводятся с целью:

− формирования практических умений в соответствии с требованиями к уровню подготовки обучающихся, установленными рабочей программой учебной дисциплины;

− обобщения, систематизации, углубления, закрепления полученных теоретических знаний;

− готовности использовать теоретические знания на практике.

Практические занятия по МДК 05.01 «Основы управления информационной безопасностью» способствуют формированию в дальнейшем при изучении профессиональных модулей, следующих общих и профессиональных компетенций:

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.

ОК 11. Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.

ПК 5.1. Применять комплексный подход к обеспечению информационной безопасности объекта защиты.

В Рабочей тетради предлагаются к выполнению практические работы, предусмотренные учебной рабочей программой МДК 05.01 «Основы управления информационной безопасностью»

При разработке содержания практических работ учитывался уровень сложности освоения студентами соответствующей темы, общих и профессиональных компетенций, на формирование которых направлена дисциплина.

Выполнение практических работ в рамках учебной дисциплины МДК 05.01 «Основы управления информационной безопасностью» позволяет освоить комплекс работ по выполнению практических заданий по всем темам МДК 05.01 «Основы управления информационной безопасностью»

Рабочая тетрадь по учебной дисциплине МДК 05.01 «Основы управления информационной безопасностью» имеет практическую направленность и значимость. Формируемые в процессе практических занятий умения могут быть использованы студентами в будущей профессиональной деятельности.

Рабочая тетрадь предназначена для студентов, изучающих МДК 05.01 «Основы управления информационной безопасностью».

Оценки за выполнение практических работ выставляются по пятибалльной системе. Оценки за практические работы являются обязательными текущими оценками по учебной дисциплине и выставляются в журнале теоретического обучения.

1 ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ РАБОТ ПО ТЕМАМ МДК 05.01 «ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»

№ раздела, темы	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов
Тема 1.1	ОК1-ОК11 ПК 5.1	Практическое занятие 1 Стандартизация в области управления ИБ.	4
Тема 1.2	ОК1-ОК11 ПК 5.1	Практическое занятие 2 Анализ политики ИБ предприятия	2
		Практическое занятие 3 Разработка политики ИБ предприятия	2
		Практическое занятие 4 Разработка регламентов политики ИБ	2
		Практическое занятие 5 Разработка инструкций политики ИБ	2
Тема 1.3		Практическое занятие 6 Анализ рынка и подбор средств для анализа СЗИ предприятия	2
		Практическое занятие 7 Контроль целостности программной среды	2
		Практическое занятие 8 Аудит ИБ	4
		Практическое занятие 9 Определение угроз ИБ	2
Тема 1.4	ОК1-ОК11 ПК 5.1	Практическое занятие 10 Подбор средств для проведения ручного тестирования безопасности	2
		Практическое занятие 11 Подбор средств для проведения полуавтоматического тестирования безопасности	2
		Практическое занятие 12 Подбор средств для проведения автоматического тестирования безопасности	2
Тема 1.5	ОК1-ОК11 ПК 5.1	Практическое занятие 13 Анализ активов организации	2
		Практическое занятие 14 Установление ценности активов	4
		Практическое занятие 15 Оценка рисков по ГОСТ	4
		Практическое занятие 16 Количественная оценка рисков	4
		Практическое занятие 17 Качественная оценка рисков	4
		Практическое занятие 18 Минимизация рисков ИБ	4
Тема 1.6	ОК1-ОК11 ПК 5.1	Практическое занятие 19 Разработка контрольных процедур	2
		Практическое занятие 20 Построение комплексной системы защиты ИБ органи-	2

№ раздела, темы	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов
		зации	

2 ОПИСАНИЕ ПОРЯДКА ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ РАБОТ

Практическая работа № 1
Стандартизация в области управления ИБ.

Задание

Изучить международные и национальные стандарты и спецификации в области ИБ — от «Оранжевой книги» до ISO 15408. Получить навыки определения сильных и слабых стороны этих документов.

Оформить результаты в виде таблицы по каждому стандарту ИБ.

Практическая работа № 2
Анализ политики ИБ предприятия

Задание

Изучите представленную информацию о предприятии. Опишите возможные пробоемы безопасности информации, выделите возможные активы предприятия.

Полное наименование: Общество с ограниченной ответственностью «Строитель».

ООО «Строитель» было учреждено по Указу Президента РФ от 20 августа 2010 года №664 «Об организационных мерах по преобразованию государственных предприятий, добровольных объединений государственных предприятий в акционерные общества». Данное предприятие официально зарегистрировано распоряжением Администрации города Москвы № 95 от 01.12.2010 года.

Юридический адрес: 101000, город Москва, улица Пушкина, дом 106. Фактический адрес местонахождения приравнивается к юридическому.

Перечень видов деятельности общества следующий:

- управление недвижимым имуществом;
- общестроительные работы.

Факторы, которые влияют на работу фирмы:

- спрос на покупку объектов долевого строительства;
- высокий уровень конкуренции благодаря задействованной дешевой зарубежной рабочей силой.

Общие тенденции развития отрасли строительства в 2020 году компания оценивает как оптимистичные, ведутся переговоры с инвесторами по вопросам постройки объектов долевого строительства.

ООО «Строитель» успешно работал на нижеперечисленных объектах:

- жилой район «Тихий уголок». Строительство и облагораживание Летнего сквера;
- жилой комплекс «Дачный». Строительство временной дороги с шоссе на поселок Солнечный;
- ремонт автомобильной дороги М-74 «Москва» от Москвы до Санкт-Петербурга. Км 452

- км 510;

- строительство подъездного железнодорожного пути, станция Новоильинская — станция Главредино. Участок ПК 120+63 — ПК 200+78;
- строительство торгово-развлекательного центра в городе Москве по улице Лермонтова, дом 35.

Новым толчком в экономике России в 2020-2040 годах может стать строительство. Среднегодовой прирост от этой отрасли на предстоящие 20 лет прогнозируется на уровне 3,9%. Вклад строительных работ в валовой внутренний продукт предположительно составит 0,45–0,75%. Однако не все экономисты согласны с этой статистикой.

Организационная характеристика компании ООО "Строитель"

Организационную структуру фирмы можно представить следующим образом:

1. Совет директоров ООО "Строитель".
2. Генеральный директор.
3. Начальник производственно-технического отдела.
4. Руководитель отдела менеджмента качества.
5. Начальник отдела охраны труда и техники безопасности.
6. Руководитель отдела организации труда и заработной платы.
7. Главный экономист.
8. Главный бухгалтер.

Организационная структура компании имеет линейный характер. Во главе расположен Совет директоров и Генеральный директор. Согласно вышеизложенной информации, по критериям количества выручки от продаж, а также численности персонала, ООО "Строитель" следует отнести к предприятиям крупного бизнеса.

Практическая работа № 3
Разработка политики ИБ предприятия

Задание

Для предприятия из работы №2 составьте политику информационной безопасности.

Политика должна содержать следующие пункты:

- Концепцию, которая определяет миссию и ключевые цели политики.
- Стандарты, то есть сами принципы обеспечения безопасности.
- Перечень конкретных действий, которые сотрудники должны совершать в процессе взаимодействия с конфиденциальными данными организации.
- Порядок работы с носителями данных.
- Правила доступа к корпоративным документам и другим важным ресурсам.
- Инструкции, касающиеся реализации методов защиты и применения принятых стандартов.

- Аварийные планы — порядок действий по реагированию и оперативному восстановлению информационных систем в случае непредвиденных обстоятельств (например, утечки, кибератаки, физических воздействий и т. д.).

Практическая работа № 4
Разработка регламентов политики ИБ

Задание

На основе разработанной политики ИБ предприятия составьте не менее 6 регламентов безопасности, раскрывающие политику ИБ.

Примеры регламентов:

- Антивирусная защита
- Парольная защита
- Безопасность ПДн

Практическая работа № 5
Разработка инструкций политики ИБ

Задание

На основе разработанной политики ИБ предприятия составьте не менее 5 инструкций безопасности, раскрывающие политику ИБ.

Примеры регламентов:

- Инструкция администратора системы
- Инструкция пользователя
- Парольная инструкция
- Инструкция на случай нештатных ситуаций

Практическая работа № 6
Анализ рынка и подбор средств для анализа СЗИ предприятия

Задание

Проведите сравнительный анализ средств для анализа безопасности СЗИ предприятия. Сравните средства в зависимости от типа средства, способа анализа. Сравните не менее 5 средств.

Практическая работа № 7
Контроль целостности программной среды

Задание

Настройте Secret Net Studio для контроля целостности программной среды.

Зафиксируйте все этапы выполнения скриншотами.

Практическая работа № 8
Аудит ИБ

Задание

Проведите аудит по ИБ по структуре:

1. Структура и описание ИС.((Структура и описание ИС из лаб. работы №1)
2. Перечень типов угроз нарушающих доступность элементов ИС и их вероятности:
3. Перечень типов угроз нарушающих конфиденциальность элементов ИС и их вероятности:
4. Перечень типов угроз нарушающих целостность элементов ИС и их вероятности:
5. Перечень ИР и элементов ИС и их стоимость на количественной шкале (в деньгах) и качественной (по шкале «высокая», «средняя», «низкая»):
6. Оценка рисков с использованием методики от Microsoft:
7. Обоснование эффективности введенных контрмер:
8. Отчет о проведенном аудите ИС в программе COBRA:
9. Предложенные контрмеры для категории риска «доступность»:
10. Предложенные контрмеры для категории риска «конфиденциальность»:
11. Предложенные контрмеры для категории риска «целостность»:

Практическая работа № 9
Определение угроз ИБ

Задание

Для каждого из этих объектов указать не менее 7 угроз, которые могут быть реализованы по отношению к обрабатываемой в них информации, а также методы борьбы с данными угрозами.

Обозначить источник каждой из приведенных угроз.

Объекты:

- Банковская карта
- Банкомат
- Компьютер директора

- Компьютер домашний
- Мобильный телефон

Практическая работа № 10
Подбор средств для проведения ручного тестирования безопасности

Задание

Проведите сравнительный анализ не менее 4 средств для проведения ручного тестирования безопасности инфраструктуры организации.

Оформите сравнение по 7 характеристикам. Дайте выводы по результатам.

Практическая работа № 11
Подбор средств для проведения полуавтоматического тестирования безопасности
Задание

Проведите сравнительный анализ не менее 4 средств для проведения полуавтоматического тестирования безопасности инфраструктуры организации.

Оформите сравнение по 7 характеристикам. Дайте выводы по результатам.

Практическая работа № 12
Подбор средств для проведения автоматического тестирования безопасности

Задание

Проведите сравнительный анализ не менее 4 средств для проведения автоматического тестирования безопасности инфраструктуры организации.

Оформите сравнение по 7 характеристикам. Дайте выводы по результатам.

Практическая работа № 13
Анализ активов организации

Задание

На основании данных, полученных ранее об организации, проведите анализ активов организации.

Определяемые активы:

Материальные.

Информационные.

Человеческие.

Практическая работа № 14

Установление ценности активов

Задание

Определите ценность определенных активов в соответствии с ГОСТ.

ГОСТ: https://docs.cntd.ru/document/1200075254/titles/7IIHHP

Практическая работа № 15
Оценка рисков по ГОСТ

Задание

1. Ознакомиться с ГОСТ Р Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности
2. Провести анализ рисков на предприятии на основании ранее полученных данных.
3. Сделать вывод по работе.

Практическая работа № 16
Количественная оценка рисков

Задание

Проведите анализ следующих типов угроз ИБ для организации:
Умышленные несанкционированные действия людей.
Непредвиденные случайности.
Ошибки со стороны персонала.
Нарушение работоспособности оборудования, ошибки в ПО и отказы средств связи.
Первым этапом составляется перечень ИР. Для каждого ресурса перечисляются относящиеся к нему уязвимости и соответствующие им угрозы. Если существует уязвимость без связанной с ней угрозы, или существует угроза, не связанная с какими-либо уязвимостями, то рисков нет. Но и эти случаи следует предусмотреть.
Относящиеся к каждому типу негативных воздействий уровни рисков, соответствующих показателям ценности ресурсов, показателям угроз и уязвимостей, оцениваются при помощи таблицы, аналогичной таблице 1.

Показатель ценности ресурса (для каждого ресурса и угрозы)	**Уровень угрозы (вероятность ее осуществления)**								
	Низкий (Н)			**Средний (С)**			**Высокий (В)**		
	Уровень уязвимости			**Уровень уязвимости**			**Уровень уязвимости**		
	Н	**С**	**В**	**Н**	**С**	**В**	**Н**	**С**	**В**
0	0	1	2	1	2	3	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8

Таблица 1. Уровни рисков, соответствующие показателям ценности ресурсов, угроз и уязвимостей.

Количественный показатель риска определяется в шкале от 1 до 8 и вносится в соответствующую ячейку таблицы. Каждая строка в таблице определяет показатель ценности ресурса, а каждый столбец – степень опасности угрозы и уязвимости для ресурса. Например, ресурс имеет показатель ценности – 3, угроза имеет степень – «высокая», а уязвимость – «низкая». Показатель риска в этом случае будет равен – 5. Размер таблицы, учитывающей количество степеней опасности угроз, степеней опасности уязвимостей и категорий ценности ресурсов, может быть изменен в соответствии со спецификой конкретной организации.

Описанный подход определяется классификацией рассматриваемых рисков. После того, как оценивание рисков было выполнено первый раз, его результаты целесообразно сохранить, например, в базе данных. Эта мера в дальнейшем позволит легко повторить последующее оценивание рисков компании.

В матрице или таблице можно наглядно отразить связь между угрозами, негативными воздействиями и возможностями их реализации. Для этого нужно выполнить следующие шаги.

На первом шаге оценить показатель негативного воздействия по заранее определенной шкале, например, от 1 до 5, для каждого ресурса, которому угрожает опасность.

На втором шаге по заранее заданной шкале, например, также от 1 до 5, оценить вероятность реализации каждой угрозы.

На третьем шаге вычислить показатель риска путем перемножения чисел в колонках II и III, по которому и производится ранжирование угроз.

В этом примере (таблица 2) для наименьшего негативного воздействия и для наименьшей вероятности реализации выбран показатель 1.

I **Описание угрозы**	**II** **Показатель негативного воздействия**	**III** **Вероятность реализации угрозы**	**IV** **Показатель риска**	**V** **Ранг угрозы**
Угроза A	5	2	10	2
Угроза B	2	4	8	3
Угроза C	3	5	15	1
Угроза D	1	3	3	5
Угроза E	4	1	4	4
Угроза F	2	4	8	3

Таблица 2. Ранжирование угроз.

Данная процедура позволяет сравнивать и ранжировать по приоритету угрозы с различными негативными воздействиями и возможностями реализации. В определенных случаях дополнительно могут потребоваться стоимостные показатели.

Оценка негативного воздействия угрозы

Эта задача решается при помощи оценивания двух значений: ценности ресурса и частоты повторяемости риска.

Сначала каждому ресурсу присваивается определенное значение, соответствующее потенциальному ущербу от воздействия угрозы. Такие показатели присваиваются ресурсу по отношению ко всем возможным угрозам. Суммированием баллов всех ресурсов анализируемой ИС определяется количественный показатель риска для всей системы.

Далее оценивается показатель частоты повторяемости риска. Частота зависит от вероятности возникновения угрозы и степени легкости, с которой может быть использована уязвимость (уровень уязвимости). В результате получается таблица, аналогичная таблице 3.

Уровень угрозы (вероятность ее осуществления)								
Низкий			**Средний**			**Высокий**		
Уровень уязвимости			**Уровень уязвимости**			**Уровень уязвимости**		
H	**C**	**B**	**H**	**C**	**B**	**H**	**C**	**B**
0	1	2	1	2	3	2	3	4

Таблица 3. Показатель частоты повторяемости риска.

Затем определяется показатель пары ресурс/угроза. На каждую пару ресурс/угроза составляется таблица, аналогичная таблице 4, в которой суммируются показатель ценности ресурса и показатель угрозы. Фактически таблица представляет собой матрицу, элементы которой равны сумме номеров строки и столбца конкретного элемента. Эту таблицу можно использовать в дальнейшем, для обоснования критичности того или иного ресурса – чем больше показатель пары ре-

сурс/угроза, тем более критичен ресурс и на его защиту следует обратить больше внимания, на этапе управления рисками.

Показатель ценности ресурса	**Показатель частоты повторяемости риска**				
	0	**1**	**2**	**3**	**4**
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3=2+1	4	5	6
3	3	4	5=3+2	6	7
4	4	5	6	7	8

Таблица 4. Показатели пары ресурс/угроза.

На заключительном этапе суммируются все итоговые баллы по всем ресурсам ИС и формируется ее общий балл. Его можно использовать для выявления тех элементов системы, защита которых должна быть приоритетной.

Практическая работа № 17
Качественная оценка рисков

Задание

Проведите качественную оценку рисков информационной безопасности компании. Реализуйте алгоритм оценки либо вручную, либо используя средства программирования.

Входные данные алгоритма:

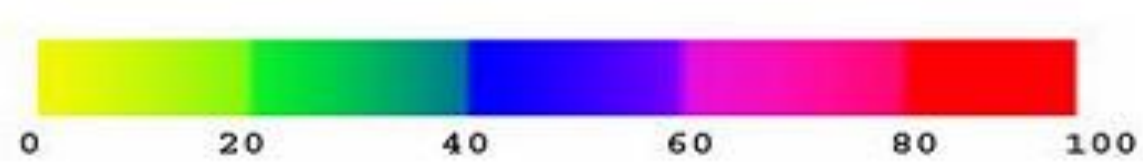
- информационные ресурсы;
- критичность ресурсов;
- угрозы, действующие на ресурсы;
- уязвимости, через которые реализуются угрозы;
- вероятность реализации угрозы через данную уязвимость;
- критичность реализации угрозы через данную уязвимость.

С точки зрения базовых угроз ИБ существует два режима работы алгоритма:

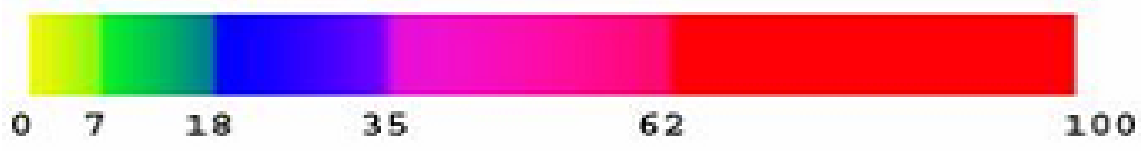
1. Одна базовая угроза (суммарная).
2. Три базовые угрозы.

Выбор шкалы для оценки риска и разбиение ее на уровни

При работе с алгоритмом используется числовая шкала от 0 до 100%. Шкалу разбивают максимум на 100 уровней. При разбиении шкалы на меньшее число уровней, каждый уровень занимает определенный интервал на шкале. Причем, возможно два варианта разделения:



– равномерное;



– логарифмическое.

Расчет рисков информационной безопасности

1. На первом этапе рассчитывается **уровень угрозы по уязвимости** (Th) на основе критичности и вероятности реализации угрозы через данную уязвимость. Уровень угрозы показывает, насколько критичным является воздействие данной угрозы на ресурс с учетом вероятности ее реализации.

$$Th = \frac{ER}{100} \times \frac{P(V)}{100},$$

$$Th_{c,i,a} = \frac{ER_{c,i,a}}{100} \times \frac{P(V)_{c,i,a}}{100},$$

где $ER_{c,i,a}$ – критичность реализации угрозы (указывается в %), $P(V)_{c,i,a}$ – вероятность реализации угрозы через данную уязвимость по конфиденциальности, целостности и доступности (указывается в %).

Здесь вычисляется одно (Th) или три значения (Th_c, Th_i, Th_a) в зависимости от количества базовых угроз. Значение уровня угрозы по уязвимости лежит в отрезке [0, 1].

2. Чтобы рассчитать **уровень угрозы по всем уязвимостям** (CTh), через которые возможна реализация данной угрозы на ресурс, просуммируем полученные уровни угроз через конкретные уязвимости по следующим формулам.

Для режима с одной базовой угрозой:

$$CTh = 1 - \prod_{i=1}^{n} (1 - Th).$$

Для режима с тремя базовыми угрозами:

$$CTh_c = 1 - \prod_{i=1}^{n} (1 - Th_c),$$

$$CTh_i = 1 - \prod_{i=1}^{n} (1 - Th_i),$$

$$CTh_a = 1 - \prod_{i=1}^{n} (1 - Th_a).$$

Значение уровня угрозы по всем уязвимостям лежит в отрезке [0, 1].

3. Далее рассчитывается **общий уровень угроз по ресурсу** (CThR) с учетом всех угроз, действующих на ресурс.

Для режима с одной базовой угрозой:

$$CThR = 1 - \prod_{i=1}^{n}(1 - CTh) .$$

Для режима с тремя базовыми угрозами:

$$CThR_c = 1 - \prod_{i=1}^{n}(1 - CTh_c) ,$$

$$CThR_i = 1 - \prod_{i=1}^{n}(1 - CTh_i) ,$$

$$CThR_a = 1 - \prod_{i=1}^{n}(1 - CTh_a) .$$

Значение общего уровня угрозы лежит в отрезке [0, 1].

4. Итоговый **риск по ресурсу** (R), характеризующий возможные потери собственника ИС, связанные с реализацией некоторой угрозы через любую уязвимость, рассчитывается следующим образом.

Для режима с одной базовой угрозой:

$$R = CThR \times D ,$$

где D – критичность ресурса. Для угроз нарушения целостности или доступности определяется заранее (в деньгах или уровнях в год), а в случае угрозы нарушения доступности ресурса (DoS – отказ в обслуживании) критичность ресурса в год рассчитывается по формуле:

$$D_{a/год} = D_{a/час} \times T ,$$

где $D_{a/час}$ – критичность простоя ресурса в час, T – общее время простоя.

Для режима с тремя базовыми угрозами:

$$R_{c,i,a} = CThR_{c,i,a} \times D_{c,i,a} ,$$

$$R = (1 - (1 - \frac{R_c}{100})(1 - \frac{R_i}{100})(1 - \frac{R_a}{100})) \times 100 ,$$

где $D_{c,i,a}$ – критичность ресурса по каждой из трех угроз заданная в деньгах или уровнях в год.

5. Общий **риск по информационной системе** (CR) рассчитывается по следующим формулам.

Для режима с одной базовой угрозой:

$$CR = \sum_{i=1}^{n} R_i$$

– для случая оценки в деньгах;

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

– для случая оценки в уровнях.

Для режима с тремя базовыми угрозами:

$$CR_{c,i,a} = \sum_{i=1}^{n} R_i ,$$

$$CR = CR_c + CR_i + CR_a$$

– для случая оценки в деньгах;

$$CR_{a,c,i} = (1 - \prod_{i=1}^{n} (1 - \frac{R_i}{100})) \times 100 ,$$

$$CR = (1 - (1 - \frac{R_c}{100})(1 - \frac{R_i}{100})(1 - \frac{R_a}{100})) \times 100$$

– для случая оценки в уровнях. В обоих режимах подразумевается R_i – риск i-го ресурса, $CR_{c,i,a}$ – риск по ИС для каждого вида угроз.

6. Для расчета **эффективности введенной контрмеры** (E) необходимо заново пройти шаги 1-5 с учетом заданной контрмеры и определить значение двух рисков – риска без учета контрмеры (R_{old}) и риск с учетом заданной контрмеры (R_{new}) или с учетом того, что уязвимость закрыта.

Эффективность введения контрмеры рассчитывается по формуле:

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

В результате работы алгоритма пользователь получает следующие данные:

1. Риск реализации по трем базовым угрозам (или по одной суммарной угрозе) для ресурса.
2. Риск реализации суммарно по всем угрозам для ресурса.
3. Риск реализации по трем базовым угрозам (или по одной суммарной угрозе) для ИС.
4. Риск реализации по всем угрозам для ИС.
5. Риск реализации по всем угрозам для ИС после задания контрмер.
6. Эффективность контрмеры.

Практическая работа № 18
Минимизация рисков ИБ

Задание

На основании проведенной оценки рисков ИБ подготовьте проект документа о минимизации рисков.

Документ должен включать в себя все направления деятельности, которые предусматривают снижение уровня обнаруженных рисков до минимума.

Практическая работа № 19
Разработка контрольных процедур

Задание

На основании разработанных политик, регламентов и инструкций, а также данных аудита подготовьте проект документа о контрольных процедурах системы защиты данных в организации, который должен отражать все направления безопасности информации организации. По каждому направлению документ должен быть отдельным.

Практическая работа № 20
Построение комплексной системы защиты ИБ организации

Задание

На основании разработанных политик, регламентов и инструкций, а также данных аудита подготовьте проект комплексной системы защиты данных в организации, который должен отражать все направления безопасности информации организации.

Оформите проект в виде итогового документа.