МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«_16_» _05_ 2024 г.

Оценка рисков информационной безопасности

Методические указания по организации самостоятельной работы по дисциплинам «Оценка рисков информационной безопасности» и «Оценка рисков и угроз» для студентов направления подготовки 10.03.01 «Информационная безопасность»

Курск 2024

УДК 004

Составители: Кулешова Е.А.

Рецензент

Кандидат технических наук, доцент кафедры
Вычислительной техники А.В. Киселев

Оценка рисков информационной безопасности: Методические указания по организации самостоятельной работы по дисциплинам «Оценка рисков информационной безопасности» и «Оценка рисков и угроз» / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2024. – 14 с.: Библиогр.: с. 13.

Содержат сведения по вопросам самостоятельной работы на протяжении изучения дисциплины. Указывается порядок выполнения самостоятельных работ, содержание работы.

Предназначены для студентов укрупненной группы специальностей и направлений подготовки 10.00.00.

Текст печатается в авторской редакции
Подписано в печать 16.05.24 . Формат 60x84 1/16.
Усл. печ.л. 0,7. Уч. –изд.л. 0,6. Тираж 50 экз. Заказ 402
Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Содержание

1. Содержание самостоятельных работ

Самостоятельная работа №1

Тема: Основные понятия и содержание дисциплины «Оценка рисков информационной безопасности».

Задание:

1. **Изучение основных понятий:**
   - Проведите анализ и изучение основных понятий в области оценки рисков информационной безопасности, таких как угроза, уязвимость, риск, методы оценки рисков и т.д.
2. **Анализ методов оценки рисков:**
   - Изучите различные методы оценки рисков информационной безопасности, такие как анализ угроз, определение уязвимостей, матрица рисков, анализ воздействия и вероятности и другие.
   - Определите основные шаги и этапы процесса оценки рисков.
3. **Анализ сценариев:**
   - Разработайте несколько сценариев, иллюстрирующих ситуации, когда оценка рисков информационной безопасности становится критически важной для организации.

Пример сценария:

Представьте, что компания подверглась кибератаке, которая привела к утечке конфиденциальных данных клиентов. Какие риски могли возникнуть в данной ситуации и какие меры предотвращения стоило бы предпринять заранее?

4. **Практическое задание:**
   - Самостоятельно проведите оценку рисков информационной безопасности для выбранной ситуации или организации.
   - Определите потенциальные угрозы, уязвимости, вероятность и воздействие рисков, а также предложите меры по их уменьшению или устранению.
5. **Составление отчета:**
   - Напишите отчет, включающий результаты вашей оценки рисков информационной безопасности, анализ сценариев и

предложения по улучшению уровня информационной безопасности в организации.

Дополнительно:

- Обратите внимание на важность регулярного обновления оценки рисков и адаптации стратегии информационной безопасности в соответствии с изменяющейся угрозовой ситуацией.

Самостоятельная работа №2

Тема: Оценка информационных рисков.

Задание:

1. **Изучение основных понятий:**
   - Изучите основные понятия, связанные с оценкой информационных рисков, такие как активы, угрозы, уязвимости, вероятность событий, последствия инцидентов.
2. **Обзор методов оценки рисков:**
   - Ознакомьтесь с различными методами оценки информационных рисков, включая квантитативные (например, методика Annual Loss Expectancy) и качественные подходы (например, Методика OCTAVE).
3. **Выбор сценариев:**
   - Выберите 2-3 сценария, которые могли бы быть критичными для информационной безопасности организации (например, утечка конфиденциальных данных, кибератака на веб-сервер, внутренний физический доступ к серверам).
4. **Проведение оценки рисков:**
   - Для каждого выбранного сценария выполняйте следующие шаги:
     - Определите ценность активов, подверженных риску.
     - Идентифицируйте потенциальные угрозы и уязвимости.
     - Оцените вероятность реализации угроз и возможные последствия инцидентов.
     - Рассчитайте уровень риска для каждого сценария.
5. **Разработка мер по снижению рисков:**
   - На основе результатов оценки рисков, предложите конкретные меры по снижению выявленных рисков (например,

внедрение многоуровневой защиты, обучение сотрудников по информационной безопасности, регулярное аудитирование).

6. **Составление отчета:**
   - Напишите отчет, включающий описание выбранных сценариев, результаты оценки рисков, предложения по снижению рисков и обоснование важности принятых мер для обеспечения информационной безопасности.

Дополнительно:

- Подчеркните необходимость регулярного мониторинга и обновления оценки рисков в соответствии с изменяющейся угрозовой средой и структурой информационных активов.

Самостоятельная работа №3

Тема: Управление рисками. Основные понятия.

Задание:

1. **Определение основных понятий:**
   - Изучите основные понятия в области управления рисками, такие как риск, угроза, уязвимость, вероятность, воздействие, стратегии управления рисками и др.
2. **Анализ риск-процесса:**
   - Разберитесь в этапах процесса управления рисками: идентификация рисков, анализ рисков, оценка рисков, управление рисками и мониторинг рисков.
3. **Идентификация рисков:**
   - Выберите предметную область (например, информационная безопасность, финансовые риски) и проведите идентификацию потенциальных рисков, присущих данной области.
4. **Анализ и оценка рисков:**
   - Для каждого идентифицированного риска проведите анализ его возможных последствий, определите вероятность наступления и оцените величину ущерба.
5. **Управление рисками:**
   - На основе проведенного анализа разработайте план управления рисками, включающий методы предотвращения, смягчения и переноса рисков.
6. **Проведение мониторинга:**

- Определите показатели и критерии, по которым будет вестись мониторинг рисков, и разработайте систему отслеживания изменений в рисках.

7. **Составление отчета:**
   - Напишите отчет, включающий результаты исследования и анализа рисков, предложения по управлению рисками и рекомендации по совершенствованию стратегии управления рисками.

Дополнительно:

- Подчеркните важность вовлечения всех заинтересованных сторон в процесс управления рисками и постоянную адаптацию стратегии управления в соответствии с изменяющейся средой.

Самостоятельная работа №4

Тема: Методики и технологии управления рисками.

Задание:

1. **Обзор методик управления рисками:**
   - Изучите основные методики управления рисками, такие как ISO 31000, COSO ERM, PMI Risk Management Framework и другие. Сравните их основные принципы и подходы.
2. **Выбор методики для анализа:**
   - Выберите одну методику управления рисками для более подробного изучения и применения в рамках задания.
3. **Применение выбранной методики:**
   - В рамках выбранной методики:
     - Идентифицируйте ключевые шаги процесса управления рисками.
     - Проанализируйте примеры технологий и инструментов, поддерживающих реализацию данной методики.
4. **Разработка плана управления рисками:**
   - На основе выбранной методики разработайте план управления рисками для определенной организации или предметной области.
5. **Применение технологий управления рисками:**

- Выберите одну или несколько технологий управления рисками (например, GRC-системы, инструменты для анализа рисков) и изучите их функциональность и возможности.

6. **Практическое задание:**
   - Примените выбранную методику и технологии управления рисками на практике, используя конкретный кейс или ситуацию, связанную с предпринимательской деятельностью или информационной безопасностью.
7. **Составление отчета:**
   - Напишите отчет, описывающий процесс выбора и применения методики управления рисками, использованные технологии, результаты и рекомендации по улучшению стратегии управления рисками.

Дополнительно:

- Оцените эффективность выбранной методики и технологий управления рисками в контексте современных требований к безопасности и управлению рисками.

Самостоятельная работа №5

Тема: Разработка корпоративной методики анализа рисков.

Задание:

1. **Изучение существующих методик:**
   - Проведите обзор существующих методик анализа рисков (например, ISO 31000, OCTAVE, NIST SP 800-30) и выделите основные принципы и этапы каждой из них.
2. **Анализ потребностей организации:**
   - Проведите анализ потребностей вашей организации (или вымышленной компании), определите особенности ее деятельности, основные уязвимости и риски.
3. **Разработка корпоративной методики:**
   - На основе собранных данных разработайте корпоративную методику анализа рисков, учитывающую специфику вашей организации.
     - Включите этапы и процедуры для идентификации, анализа, оценки и управления рисками.
     - Опишите критерии оценки рисков, меры по снижению рисков и механизмы мониторинга и своевременного реагирования на риски.

4. **Тестирование методики:**
   - Примените разработанную корпоративную методику к конкретному кейсу или сценарию в вашей организации, чтобы проверить ее эффективность и применимость.
5. **Оценка результатов:**
   - Оцените результаты тестирования методики, выявите ее преимущества и недостатки, предложите возможные улучшения.
6. **Составление отчета:**
   - Напишите отчет, описывающий процесс разработки корпоративной методики анализа рисков, результаты тестирования, рекомендации по ее дальнейшему совершенствованию и внедрению.

Дополнительно:

- Обратите внимание на важность обучения сотрудников по использованию новой корпоративной методики и настройку процессов управления рисками в организации в соответствии с ней.

Самостоятельная работа №6

Тема: Современные методы и средства анализа и управление рисками информационных систем компаний.

Задание:

1. **Изучение современных методов анализа и управления рисками ИС:**
   - Изучите современные методики и подходы к анализу и управлению рисками информационных систем, такие как FAIR (Factor Analysis of Information Risk), Cybersecurity Framework (CSF), Threat Modeling и др.
2. **Выбор нескольких методов для изучения:**
   - Выберите несколько современных методов и средств анализа и управления рисками информационных систем для более детального изучения.
3. **Исследование выбранных методов:**
   - Разберитесь в принципах и шагах каждого выбранного метода:
     - Как проводится идентификация рисков ИС?

- Как оцениваются вероятность и воздействие рисков?
- Какие меры по управлению рисками рекомендуются?

4. **Применение методов на практике:**
   - Возьмите в качестве примера информационную систему компании (реальной или вымышленной) и проведите анализ рисков этой системы с использованием выбранных методов.
5. **Оценка эффективности методов:**
   - Проанализируйте результаты применения выбранных методов анализа и управления рисками ИС. Оцените их эффективность, плюсы и минусы.
6. **Интеграция современных средств в компанию:**
   - Разработайте план по внедрению выбранных методов и средств в управление рисками информационных систем компании. Опишите, как обучить сотрудников и обеспечить поддержку процесса.
7. **Подготовка отчета:**
   - Напишите отчет, описывающий выбранные методы, процесс анализа рисков ИС, рекомендации по улучшению управления рисками и план их внедрения.

Дополнительно:

- Выделите в отчете ключевые преимущества современных методов и средств анализа и управления рисками информационных систем по сравнению с традиционными подходами.

2. Контрольные вопросы

3.

1. Что такое риск в контексте информационной безопасности?
2. Какие компоненты включает в себя процесс оценки рисков информационной безопасности?
3. Какие методы оценки рисков информационной безопасности вы знаете?
4. Какие основные шаги следует выполнить при проведении оценки рисков информационной безопасности?
5. Как определить активы в рамках оценки рисков информационной безопасности?
6. Какие факторы влияют на вероятность возникновения рисков в информационной безопасности?
7. Что такое уязвимости в контексте оценки рисков информационной безопасности?
8. Какие последствия могут возникнуть при реализации рисков информационной безопасности?
9. Как измеряется уровень риска в информационной безопасности?
10. Какие инструменты и методики могут помочь в проведении качественной оценки рисков информационной безопасности?
11. Какие меры безопасности можно принять для снижения рисков информационной безопасности?
12. Как влияет уровень защиты информационных систем на уровень рисков информационной безопасности?
13. Какие риски могут быть связаны с человеческим фактором в информационной безопасности?
14. Что такое матрица рисков и как она используется при оценке рисков информационной безопасности?
15. Какие приоритеты следует учитывать при управлении рисками информационной безопасности?
16. Как влияют внешние угрозы на оценку рисков информационной безопасности?
17. Как оценить потенциальные угрозы безопасности при анализе рисков информационной безопасности?

18. Что такое анализ воздействия и вероятности при проведении оценки рисков информационной безопасности?

19. Какие типы угроз могут возникать при использовании облачных технологий и как их можно учесть при оценке рисков?

20. Как обеспечить постоянное обновление оценки рисков информационной безопасности в условиях быстро меняющейся угрозовой среды?

3. Библиографический список

1) Милославская, Н. Г. Управление рисками информационной безопасности : учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. – Москва : Горячая линия – Телеком, 2013. – 130 с. : ил. – (Вопросы управления информационной безопасностью ; выпуск 2). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=253576 (дата обращения: 15.05.2024). – Библиогр. в кн. – ISBN 978-5-9912-0272-5. – Текст : электронный.

2) Веселов, Г. Е. Менеджмент риска информационной безопасности : учебное пособие / Г. Е. Веселов, Е. С. Абрамов, А. К. Шилов ; Южный федеральный университет, Инженерно-технологическая академия. – Таганрог : Южный федеральный университет, 2016. – 109 с. : схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=493331 (дата обращения: 15.05.2024). – Библиогр.: с. 85-86. – ISBN 978-5-9275-2327-5. – Текст : электронный.

3) Деревяшкин, С. А. Оценка рисков : [16+] / С. А. Деревяшкин ; Поволжский государственный технологический университет. – Йошкар-Ола : Поволжский государственный технологический университет, 2019. – 74 с. : табл., граф., схем., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=570617 (дата обращения: 15.05.2024). – Библиогр. в кн. – ISBN 978-5-8158-2097-5. – Текст : электронный.

4) Шапкин, А. С. Теория риска и моделирование рисковых ситуаций : учебник / А. С. Шапкин, В. А. Шапкин. – 10-е изд., перераб. – Москва : Дашков и К°, 2023. – 874 с. : табл., схем. – (Учебные издания для бакалавров). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=710894 (дата обращения: 15.05.2024). – Библиогр.: с. 859-865. – ISBN 978-5-394-05397-9. – Текст : электронный.

5) Аверченков, В. И. Аудит информационной безопасности : учебное пособие : [16+] / В. И. Аверченков. – 4-е изд., стер. – Москва : ФЛИНТА, 2021. – 269 с. : ил., схем., табл. – Режим доступа: по подписке. – URL:

https://biblioclub.ru/index.php?page=book&id=93245 (дата обращения: 15.05.2024). – Библиогр. в кн. – ISBN 978-5-9765-1256-6. – Текст : электронный.

6) Черняков, М. К. Управление рисками : конспект лекций : учебное пособие : [16+] / М. К. Черняков, М. М. Чернякова ; под ред. М. К. Чернякова ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2018. – 144 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=574663 (дата обращения: 15.05.2024). – Библиогр. в кн. – ISBN 978-5-7782-3746-9. – Текст : электронный.