Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Локтионова Оксана Геннадьевна
Должность: проректор по учебной работе
Дата подписания: 12.03.2025 21:18:54
Уникальный программный ключ:
0b817ca911e6668abb13a5d426d39e5f1c11eabbf73e943df4a4851fda56d089

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
«_8_» _08_____ 2023 г.

Организация и управление службой защиты информации

Методические указания по организации самостоятельной работы по дисциплине «Организация и управление службой защиты информации» для студентов укрупненной группы направлений подготовки и специальностей 10.00.00

Курск 2023

УДК 004.773.5

Составители: Кулешова Е.А.

Рецензент

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

Организация и управление службой защиты информации: методические указания для самостоятельной работы / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 9с.: Библиогр.: с. 9.

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

Предназначены для студентов укрупненной группы направлений подготовки и специальностей 10.00.00.

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

Содержание самостоятельной работы

	Тема СРС	Задание
1	Кадровая политика в области информационной безопасности	Используя принципы кадровой политики, разработайте комплекс мер по укреплению информационной безопасности для организации, работающей с конфиденциальными данными. Шаги выполнения задания: 1. Определите основные требования и квалификационные характеристики персонала, занимающегося обработкой конфиденциальных данных. 2. Разработайте и внедрите процесс набора, аттестации и обучения сотрудников, чтобы гарантировать, что они обладают необходимыми знаниями и навыками в области информационной безопасности. 3. Создайте систему мотивации и стимулирования сотрудников, чтобы повысить их ответственность и заинтересованность в обеспечении информационной безопасности. 4. Установите процедуры проверки фоновых данных и проведения проверок на предмет наличия возможных угроз со стороны сотрудников. 5. Разработайте план противодействия внутренним угрозам информационной безопасности и определите роли и ответственность персонала при идентификации и предотвращении подобных случаев. 6. Определите процедуры реагирования на инциденты информационной безопасности и обучите сотрудников, как действовать в случае возникновения угрозы или нарушения безопасности. 7. Постоянно оценивайте эффективность кадровой политики в области информационной безопасности и внесите необходимые корректировки для ее улучшения. Представьте разработанный комплекс мер в виде презентации или письменного отчета, обоснуйте выбор каждого шага и предложите план действий по его реализации.
2	Методы планирования работ по обеспечению информационной безопасности	Разработайте план работы по обеспечению информационной безопасности для организации, включающий методы планирования работ. Шаги выполнения задания: 1. Изучите основные принципы и методы обеспечения информационной безопасности, такие как идентификация уязвимостей, риски и угрозы, анализ последствий нарушений безопасности и выбор соответствующих мер защиты. 2. Определите цели и задачи организации в области информационной безопасности. Учтите специфику организации, ее бизнес-процессы и требования к конфиденциальности данных. 3. Разработайте план действий по обеспечению

		информационной безопасности, включающий этапы и сроки реализации мероприятий. Определите ответственных лиц и ресурсы, необходимые для выполнения плана. 4. Примените методы оценки рисков и угроз для выявления наиболее критических областей, требующих особого внимания. Составьте список приоритетных мер по устранению уязвимостей и минимизации рисков. 5. Определите методы мониторинга и контроля за выполнением плана работы по обеспечению информационной безопасности. Разработайте процедуры проверки эффективности применяемых мер и системы предупреждения инцидентов. 6. Внедрите систему обучения и осведомленности персонала о методах обеспечения информационной безопасности. Обучите сотрудников правилам использования информационных ресурсов организации и способам предотвращения угроз безопасности. 7. Проведите аудит текущего состояния информационной безопасности и сравните его с заданными целями и планом работ. Проанализируйте полученные результаты и внесите необходимые корректировки в план работы. Представьте разработанный план работы в виде презентации или письменного отчета, обоснуйте выбор каждого шага и предложите план действий по его реализации.
3	Методы решения проблемных ситуаций в коллективе	Задание: Разработка плана действий для решения проблемной ситуации в коллективе Описание задания: 1. Выберите проблемную ситуацию, которая возникает или может возникнуть в вашем коллективе. Например: конфликт между сотрудниками, неэффективное общение, недостаточная мотивация или отсутствие сотрудничества. 2. Изучите и проанализируйте данную проблему, выявите ее корневые причины и последствия. 3. Разделите участников группы на команды (можно работать как индивидуально, так и в группах). 4. Каждая команда должна разработать план действий по решению выбранной проблемной ситуации. План должен включать следующие шаги: • Определение целей решения проблемы. • Анализ и выявление факторов, способствующих возникновению проблемы. • Выработка стратегии решения проблемы. • Определение конкретных шагов и ответственности для их реализации. • Оценка возможных рисков и разработка плана мероприятий по их минимизации. • Определение критериев успешного решения проблемы. 5. После разработки планов действий каждая команда

		должна представить свое решение перед остальными участниками и обсудить его совместно. 6. В процессе обсуждения участники могут задавать вопросы, выражать свои мысли и предлагать дополнительные идеи для улучшения планов действий. 7. По окончании обсуждения каждая команда может внести коррективы в свой план действий, основываясь на обратной связи и обсуждении с группой. 8. Наконец, каждая команда должна представить окончательную версию плана действий и объяснить, почему они считают его эффективным для решения выбранной проблемы в коллективе. Цель задания: Применить знания о методах решения проблемных ситуаций в коллективе и развить навыки коллективной работы, анализа причин и разработки эффективных стратегий решения проблем.
4	Применение нормативно-правовых актов при организации работ по защите информации	Задание: Опишите процесс применения нормативно-правовых актов при организации работ по защите информации в организации, с учетом следующих шагов: 1. Выберите одну организацию (можете использовать реальную или выдуманную) и определите ее тип (государственная, коммерческая, некоммерческая и т. д.). 2. Исследуйте и анализируйте нормативно-правовые акты, связанные с защитой информации, которые применимы к данной организации. Включите в анализ как общие законы (например, закон о защите персональных данных), так и специализированные нормативные акты, относящиеся к конкретным отраслям или видам информации. 3. Составьте план мероприятий по применению этих нормативно-правовых актов в организации. Укажите необходимые этапы и ресурсы для успешной организации работ по защите информации. 4. Опишите механизм контроля и проверки соблюдения нормативно-правовых актов организацией. Рассмотрите возможные способы проверки, включая внутренний аудит, независимую экспертизу или контрольные органы. 5. Проведите анализ эффективности применения нормативно-правовых актов в организации. Оцените результаты и предложите рекомендации по оптимизации процесса организации работ по защите информации на основе этого анализа. 6. Подготовьте заключительный отчет, в котором представите результаты выполненной работы, включая все составленные планы, анализы и рекомендации. Примечание: В данном задании участникам предлагается провести теоретическое исследование и разработать практический план действий, основанный на применении нормативно-правовых актов при организации работ по защите

		информации.
5	Управление разработкой информационных систем	Название задания: "Использование гибких методологий управления разработкой информационных систем: преимущества и ограничения" Описание задания: Ваша задача состоит в написании обзорной статьи на тему "Управление разработкой информационных систем" с акцентом на использование гибких методологий. В статье необходимо рассмотреть следующие аспекты: 1. Обзор традиционных и гибких методологий управления разработкой информационных систем. 2. Оценка преимуществ и ограничений гибкого подхода при управлении разработкой информационных систем. 3. Исследование успешных случаев применения гибких методологий управления разработкой информационных систем. 4. Анализ факторов, которые могут оказывать влияние на выбор методологии управления разработкой информационных систем. 5. Рекомендации по эффективному использованию гибких методологий при управлении разработкой информационных систем. В статье необходимо проанализировать актуальные исследования, используя надежные источники информации (академические статьи, конференции, профессиональные журналы и т.д.). Важно представить собственное мнение на основе анализа литературы и привести конкретные примеры для поддержки аргументов. Требования к статье: Объем: 3000-5000 слов. Структура: введение, литературный обзор, методология исследования, результаты и обсуждение, выводы, список литературы. Срок выполнения задания: 2 недели.
6	Формирование комплекса мер по обеспечению информационной безопасности	Задание: Напишите научную статью о формировании комплекса мер, направленных на обеспечение информационной безопасности в современном информационном пространстве. Ваша статья должна содержать следующие разделы: 1. Введение • Краткое введение в проблематику информационной безопасности и ее актуальность. • Формулировка цели и задач статьи. 2. Теоретический обзор • Обзор основных понятий и терминов, связанных с информационной безопасностью. • Изложение основных угроз и уязвимостей информационной безопасности в современном мире.

		3. Анализ существующих подходов к обеспечению информационной безопасности • Описание и анализ существующих методов и подходов к защите информации. • Оценка эффективности и недостатков существующих решений. 4. Формирование комплекса мер по обеспечению информационной безопасности • Разработка концепции и методологии формирования комплекса мер. • Описание основных шагов и этапов процесса формирования комплекса мер. 5. Примеры практического применения комплекса мер • Представление конкретных примеров успешного внедрения комплекса мер по обеспечению информационной безопасности. • Анализ результатов и полученного опыта. 6. Выводы. Подведение итогов и формулировка основных выводов, сделанных в ходе исследования. 7. Рекомендации и направления дальнейших исследований • Формулировка рекомендаций по улучшению существующих подходов к обеспечению информационной безопасности. • Определение перспективных направлений для будущих исследований в данной области. Примечание: Ваша статья должна быть основана на актуальных и достоверных источниках информации. При написании статьи рекомендуется использовать методы аналитического исследования, сравнительный анализ, а также приводить примеры из практического опыта. Срок выполнения задания: 2 недели.
7	Порядок разработки модели угроз при построении информационных систем	Задание: Создание презентации на тему "Порядок разработки модели угроз при построении информационных систем" Описание задания: Ваша задача - разработать презентацию, которая будет описывать порядок разработки модели угроз при построении информационных систем. Презентация должна включать следующие разделы: 1. Введение: В этом разделе вы должны представить общую информацию о важности создания модели угроз для информационных систем. Расскажите о растущей угрозе кибератак и необходимости защиты конфиденциальной информации. 2. Определение целей и задач: В этом разделе опишите основные цели и задачи создания модели угроз. Объясните, что модель угроз позволяет идентифицировать потенциальные угрозы и принимать меры по их предотвращению. 3. Этапы разработки модели угроз:

		a. Анализ бизнес-процессов: Объясните необходимость изучения бизнес-процессов, которые будут поддерживаться информационной системой. Укажите, что это поможет определить основные активы и уязвимости. b. Идентификация активов: Расскажите о важности определения всех активов, с которыми будет работать информационная система. Укажите на конфиденциальность данных, финансовые ресурсы и другие активы, требующие защиты. c. Определение потенциальных угроз: Приведите примеры возможных угроз, таких как хакерские атаки, физические повреждения и несанкционированный доступ к данным. Объясните, что этот шаг помогает выявить риски и уязвимые места. d. Оценка уровня риска: Объясните процесс оценки вероятности возникновения угроз и их потенциальных последствий. Укажите, что это позволяет определить приоритетные угрозы и разработать соответствующие меры безопасности. e. Разработка мер безопасности: Представьте набор мер безопасности, которые должны быть внедрены для защиты информационной системы. Включите технические, организационные и физические меры безопасности. f. Разработка плана реагирования на инциденты: Объясните необходимость разработки плана действий в случае возникновения угрозы или инцидента. Укажите на важность быстрой реакции, ликвидации угрозы и восстановления после инцидента. 4. Заключение: В этом разделе подведите итоги и сделайте акцент на значимости создания модели угроз для обеспечения безопасности информационных систем. Результаты задания: В результате выполнения задания вы должны предоставить готовую презентацию на тему "Порядок разработки модели угроз при построении информационных систем". Презентация должна содержать все перечисленные разделы и быть структурированной, наглядной и информативной.

Перечень литературы

1. Аверченков, В. И. Служба защиты информации : организация и управление : учебное пособие / В. И. Аверченков, М. Ю. Рытов. – 4-е изд., стер. – Москва : ФЛИНТА, 2021. – 186 с. – URL: https://biblioclub.ru/index.php?page=book&id=93356 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.
2. Аверченков, В. И. Аудит информационной безопасности : учебное пособие / В. И. Аверченков. – 4-е изд., стер. – Москва : ФЛИНТА, 2021. – 269 с. – URL: https://biblioclub.ru/index.php?page=book&id=93245 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.
3. Абрамов, Г. В. Проектирование информационных систем : учебное пособие / Г. В. Абрамов, И. Е. Медведкова, Л. А. Коробова. – Воронеж : Воронежский государственный университет инженерных технологий, 2012. – 172 с. – URL: https://biblioclub.ru/index.php?page=book&id=141626 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.
4. Петренко, В. И. Теоретические основы защиты информации : учебное пособие / В. И. Петренко ; Северо-Кавказский федеральный университет. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2015. – 222 с. – URL: https://biblioclub.ru/index.php?page=book&id=458204 (дата обращения: 22.05.2023). - Режим доступа: по подписке. – Текст : электронный.
5. Технологии обеспечения безопасности информационных систем : учебное пособие / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. – URL: https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.