

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Локтионова Оксана Геннадьевна  
Должность: проректор по учебной работе  
Дата подписания: 31.08.2023 22:34:11  
Уникальный программный ключ:  
0b817ca911e6668abb13a5d426d39e5f1c11eabbf73e943df4a4851fda56d089

## МИНОБРНАУКИ РОССИИ

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

Кафедра информационной безопасности

УТВЕРЖДАЮ

Проректор по учебной работе

О.Г. Локтионова  
2023 г.

« 8 » 08



### Организация работ по обеспечению безопасности в информационных системах

Методические указания по организации самостоятельной  
работы по дисциплине «Организация работ по обеспечению  
безопасности в информационных системах» для студентов  
направления подготовки 10.04.01 «Информационная  
безопасность»

Курск 2023

УДК 004.773.5

Составители: Кулешова Е.А.

Рецензент

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

**Организация работ по обеспечению безопасности в информационных системах:** 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 направления подготовки 10.04.01 «Информационная безопасность».

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 информационно й безопасности	<p>Используя принципы кадровой политики, разработайте комплекс мер по укреплению информационной безопасности для организации, работающей с конфиденциальными данными.</p> <p>Шаги выполнения задания:</p> <ol style="list-style-type: none"> <li>1. Определите основные требования и квалификационные характеристики персонала, занимающегося обработкой конфиденциальных данных.</li> <li>2. Разработайте и внедрите процесс набора, аттестации и обучения сотрудников, чтобы гарантировать, что они обладают необходимыми знаниями и навыками в области информационной безопасности.</li> <li>3. Создайте систему мотивации и стимулирования сотрудников, чтобы повысить их ответственность и заинтересованность в обеспечении информационной безопасности.</li> <li>4. Установите процедуры проверки фоновых данных и проведения проверок на предмет наличия возможных угроз со стороны сотрудников.</li> <li>5. Разработайте план противодействия внутренним угрозам информационной безопасности и определите роли и ответственность персонала при идентификации и предотвращении подобных случаев.</li> <li>6. Определите процедуры реагирования на инциденты информационной безопасности и обучите сотрудников, как действовать в случае возникновения угрозы или нарушения безопасности.</li> <li>7. Постоянно оценивайте эффективность кадровой политики в области информационной безопасности и внесите необходимые корректировки для ее улучшения.</li> </ol> <p>Представьте разработанный комплекс мер в виде презентации или письменного отчета, обоснуйте выбор каждого шага и предложите план действий по его реализации.</p>
2	Методы планирования работ по обеспечению информационно й безопасности	<p>Разработайте план работы по обеспечению информационной безопасности для организации, включающий методы планирования работ.</p> <p>Шаги выполнения задания:</p> <ol style="list-style-type: none"> <li>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.</li> <li>2. Определите цели и задачи организации в области информационной безопасности. Учтите специфику организации, ее бизнес-процессы и требования к конфиденциальности данных.</li> <li>3. Разработайте план действий по обеспечению</li> </ol>

		<p>информационной безопасности, включающий этапы и сроки реализации мероприятий. Определите ответственных лиц и ресурсы, необходимые для выполнения плана.</p> <ol style="list-style-type: none"> <li>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.</li> <li>5. Определите методы мониторинга и контроля за выполнением плана работы по обеспечению информационной безопасности. Разработайте процедуры проверки эффективности применяемых мер и системы предупреждения инцидентов.</li> <li>6. Внедрите систему обучения и осведомленности персонала о методах обеспечения информационной безопасности. Обучите сотрудников правилам использования информационных ресурсов организации и способам предотвращения угроз безопасности.</li> <li>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.</li> </ol> <p>Представьте разработанный план работы в виде презентации или письменного отчета, обоснуйте выбор каждого шага и предложите план действий по его реализации.</p>
3	<p>Методы решения проблемных ситуаций в коллективе</p>	<p>Задание: Разработка плана действий для решения проблемной ситуации в коллективе</p> <p>Описание задания:</p> <ol style="list-style-type: none"> <li>1. Выберите проблемную ситуацию, которая возникает или может возникнуть в вашем коллективе. Например: конфликт между сотрудниками, неэффективное общение, недостаточная мотивация или отсутствие сотрудничества.</li> <li>2. Изучите и проанализируйте данную проблему, выявите ее корневые причины и последствия.</li> <li>3. Разделите участников группы на команды (можно работать как индивидуально, так и в группах).</li> <li>4. Каждая команда должна разработать план действий по решению выбранной проблемной ситуации. План должен включать следующие шаги: <ul style="list-style-type: none"> <li>• Определение целей решения проблемы.</li> <li>• Анализ и выявление факторов, способствующих возникновению проблемы.</li> <li>• Выработка стратегии решения проблемы.</li> <li>• Определение конкретных шагов и ответственности для их реализации.</li> <li>• Оценка возможных рисков и разработка плана мероприятий по их минимизации.</li> <li>• Определение критериев успешного решения проблемы.</li> </ul> </li> <li>5. После разработки планов действий каждая команда</li> </ol>

		<p>должна представить свое решение перед остальными участниками и обсудить его совместно.</p> <ol style="list-style-type: none"> <li>6. В процессе обсуждения участники могут задавать вопросы, выражать свои мысли и предлагать дополнительные идеи для улучшения планов действий.</li> <li>7. По окончании обсуждения каждая команда может внести коррективы в свой план действий, основываясь на обратной связи и обсуждении с группой.</li> <li>8. Наконец, каждая команда должна представить окончательную версию плана действий и объяснить, почему они считают его эффективным для решения выбранной проблемы в коллективе.</li> </ol> <p>Цель задания: Применить знания о методах решения проблемных ситуаций в коллективе и развить навыки коллективной работы, анализа причин и разработки эффективных стратегий решения проблем.</p>
4	<p>Применение нормативно-правовых актов при организации работ по защите информации</p>	<p>Задание:</p> <p>Опишите процесс применения нормативно-правовых актов при организации работ по защите информации в организации, с учетом следующих шагов:</p> <ol style="list-style-type: none"> <li>1. Выберите одну организацию (можете использовать реальную или выдуманную) и определите ее тип (государственная, коммерческая, некоммерческая и т. д.).</li> <li>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.</li> <li>3. Составьте план мероприятий по применению этих нормативно-правовых актов в организации. Укажите необходимые этапы и ресурсы для успешной организации работ по защите информации.</li> <li>4. Опишите механизм контроля и проверки соблюдения нормативно-правовых актов организацией. Рассмотрите возможные способы проверки, включая внутренний аудит, независимую экспертизу или контрольные органы.</li> <li>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.</li> <li>6. Подготовьте заключительный отчет, в котором представите результаты выполненной работы, включая все составленные планы, анализы и рекомендации.</li> </ol> <p>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</p>

		информации.
5	Управление разработкой информационных систем	<p>Название задания: "Использование гибких методологий управления разработкой информационных систем: преимущества и ограничения"</p> <p>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:</p> <ol style="list-style-type: none"> <li>1. Обзор традиционных и гибких методологий управления разработкой информационных систем.</li> <li>2. Оценка преимуществ и ограничений гибкого подхода при управлении разработкой информационных систем.</li> <li>3. Исследование успешных случаев применения гибких методологий управления разработкой информационных систем.</li> <li>4. Анализ факторов, которые могут оказывать влияние на выбор методологии управления разработкой информационных систем.</li> <li>5. Рекомендации по эффективному использованию гибких методологий при управлении разработкой информационных систем.</li> </ol> <p>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.</p> <p>Требования к статье: Объем: 3000-5000 слов. Структура: введение, литературный обзор, методология исследования, результаты и обсуждение, выводы, список литературы. Срок выполнения задания: 2 недели.</p>
6	Формирование комплекса мер по обеспечению информационной безопасности	<p>Задание: Напишите научную статью о формировании комплекса мер, направленных на обеспечение информационной безопасности в современном информационном пространстве. Ваша статья должна содержать следующие разделы:</p> <ol style="list-style-type: none"> <li>1. Введение <ul style="list-style-type: none"> <li>• Краткое введение в проблематику информационной безопасности и ее актуальность.</li> <li>• Формулировка цели и задач статьи.</li> </ul> </li> <li>2. Теоретический обзор <ul style="list-style-type: none"> <li>• Обзор основных понятий и терминов, связанных с информационной безопасностью.</li> <li>• Изложение основных угроз и уязвимостей информационной безопасности в современном мире.</li> </ul> </li> </ol>

		<ol style="list-style-type: none"> <li>3. Анализ существующих подходов к обеспечению информационной безопасности <ul style="list-style-type: none"> <li>• Описание и анализ существующих методов и подходов к защите информации.</li> <li>• Оценка эффективности и недостатков существующих решений.</li> </ul> </li> <li>4. Формирование комплекса мер по обеспечению информационной безопасности <ul style="list-style-type: none"> <li>• Разработка концепции и методологии формирования комплекса мер.</li> <li>• Описание основных шагов и этапов процесса формирования комплекса мер.</li> </ul> </li> <li>5. Примеры практического применения комплекса мер <ul style="list-style-type: none"> <li>• Представление конкретных примеров успешного внедрения комплекса мер по обеспечению информационной безопасности.</li> <li>• Анализ результатов и полученного опыта.</li> </ul> </li> <li>6. Выводы. Подведение итогов и формулировка основных выводов, сделанных в ходе исследования.</li> <li>7. Рекомендации и направления дальнейших исследований <ul style="list-style-type: none"> <li>• Формулировка рекомендаций по улучшению существующих подходов к обеспечению информационной безопасности.</li> <li>• Определение перспективных направлений для будущих исследований в данной области.</li> </ul> </li> </ol> <p>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.</p> <p>Срок выполнения задания: 2 недели.</p>
7	Порядок разработки модели угроз при построении информационных систем	<p>Задание: Создание презентации на тему "Порядок разработки модели угроз при построении информационных систем"</p> <p>Описание задания: Ваша задача - разработать презентацию, которая будет описывать порядок разработки модели угроз при построении информационных систем. Презентация должна включать следующие разделы:</p> <ol style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>3. Этапы разработки модели угроз:</li> </ol>

		<p>a. Анализ бизнес-процессов: Объясните необходимость изучения бизнес-процессов, которые будут поддерживаться информационной системой. Укажите, что это поможет определить основные активы и уязвимости.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>e. Разработка мер безопасности: Представьте набор мер безопасности, которые должны быть внедрены для защиты информационной системы. Включите технические, организационные и физические меры безопасности.</p> <p>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.</p> <p>4. Заключение: В этом разделе подведите итоги и сделайте акцент на значимости создания модели угроз для обеспечения безопасности информационных систем.</p> <p>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.</p>
--	--	---



## 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.