МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДАЮ
Декан факультета
информационных технологий
/Д. Г. Демидов/
"28" апреля 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Методы и средства повышения осведомлённости персонала по вопросам информационной безопасности

Направление подготовки
10.04.01 Информационная безопасность

Профиль
Системы управления информационной безопасностью

Квалификация
Магистр

Формы обучения
Очная

Москва, 2022 г.

Разработчик:

Кандидат экономических наук, доцент  /К.Н. Темникова/

Согласовано:
И.о. заведующего кафедрой «Информационная безопасность»,  /А.Ю. Гневшев

Руководитель образовательной программы
Доцент. к.т.н.  /С.А. Кесель/

Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине

Цель дисциплины является подготовка обучающихся к решению задач профессиональной деятельности организационно-управленческого, проектного и научно-исследовательского типов в области защиты информации по направлению подготовки 10.04.01 Информационная безопасность (магистерская программа: Безопасность автоматизированных систем) посредством обеспечения этапов формирования компетенций, предусмотренных ФГОС и установленных программой магистратуры на основе профессиональных стандартов, в части представленных ниже знаний, умений и навыков.

К **основным целям** освоения дисциплины «Методы и средства повышения осведомлённости персонала по вопросам информационной безопасности» следует отнести:

- сформировать у студентов теоретические представления о целях, задачах и основных современных методах повышения осведомлённости персонала по вопросам информационной безопасности;
- выработать навыки целеполагания, бюджетирования затрат на повышение осведомленности персонала в области информационной безопасности в соответствии с требованиями международных (серии ISO 270XX) и национальных (ГОСТ Р ИСО 270XX) стандартов, практического применения методов; освоение стандартов оформления результатов повышения осведомлённости персонала по вопросам информационной безопасности.

К **основным задачам** освоения дисциплины «Методы и средства повышения осведомлённости персонала по вопросам информационной безопасности» следует отнести:

- ознакомить обучающихся с российскими нормативными правовыми документами, международными и национальными стандартами в области систем менеджмента информационной безопасности;
- дать представление об угрозах, рисках и уязвимостях информационной безопасности в части повышения осведомленности в области информационной безопасности;
- сформировать умение проводить анализ проблем информационной безопасности в части повышения осведомленности в области информационной безопасности;
- сформировать навыки разработки концепции, политики и целей управления информационной безопасностью и мер, направленных на повышение осведомленности в области информационной безопасности (прежде всего в отношении Политики и Целей в области информационной безопасности);
- сформировать умение разрабатывать стратегию построения и внедрения системы управления информационной безопасностью в части повышения осведомленности в области информационной безопасности;
- научить выполнять оценку эффективности и результативности системы менеджмента информационной безопасности предприятия в части повышения осведомленности в области информационной безопасности;
- выработать навыки и умения формировать программы повышения осведомлённости персонала по вопросам информационной безопасности, применять соответствующие методы и средства повышения осведомлённости персонала по вопросам информационной безопасности и результатов для принятия управленческих решений в информационной безопасности;
- сформировать умение сопоставлять процессы, модели, методы и средства повышения осведомлённости персонала по вопросам информационной безопасности с задачами конкретного исследования и правильно выбирать метод в соответствии с его целями, задачами, гипотезами и имеющимися данными; развитие умений оценки достоверности и значимости полученных результатов.

Планируемые результаты обучения

В результате освоения дисциплины «Методы и средства повышения осведомлённости персонала по вопросам информационной безопасности» у обучающихся формируются следующие компетенции и должны быть достигнуты результаты обучения как этап формирования соответствующих компетенций.

В результате освоения дисциплины «Методы и средства повышения осведомлённости персонала по вопросам информационной безопасности» у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Компетенции 10.04.01 ИБ Системы управления информационной безопасностью

Тип задач профессиональной деятельности: организационно-управленческий

ПК-11. Способен проводить занятия по предметной области данного направления и разрабатывать методические материалы	ИПК-11.1. **Знает:** структуру и состав методических материалов, используемые в образовательной деятельности. ИПК-11.2. **Умеет:** проводить занятия по избранным дисциплинам предметной области данного направления. ИПК-11.3. **Владеет:** навыками разработки методических материалы, используемых в образовательной деятельности.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к части, формируемой участниками образовательных отношений блока Б1 «Дисциплины (модули)».

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Построение и совершенствование систем управления информационной безопасностью», «Управление информационной безопасностью», «Защита информации в системах обработки данных».

Дисциплина обеспечивает изучение дисциплин «Стратегии управления информационной безопасностью», «Защита информации в автоматизированных системах управления технологическими процессами», «Защита информации от утечки по техническим каналам» и подготовку выпускной квалификационной работы.

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (108 часов)

4 Виды учебной работы и трудоемкость

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры
			3
1	**Аудиторные занятия**	**54**	3
	В том числе:		
1.1	Лекции		3
1.2	Семинарские/практические занятия		3
1.3	Лабораторные занятия	54	3
2	**Самостоятельная работа**	**54**	**3**
3	**Промежуточная аттестация**		**3**
	Экзамен		3

	Итого:	**108**	

Тематический план изучения дисциплины

3.2.1 Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	**Аудиторная работа**				**Самостоятельная работа**
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	
1	Тема 1. Концепция, политика и цели информационной безопасности при внедрении системы управления информационной безопасностью (СУИБ).				2		2
2	Тема 2. Задачи, методы и средства повышения осведомленности в области информационной безопасности в рамках СУИБ.				2		2
3	Тема 3. Стандартизация процессов повышения осведомленности в области информационной безопасности в рамках СУИБ.				2		2
4	Тема 4. Классификация угроз информационной безопасности в части, связанной с персоналом организации.				2		2
5	Тема 5. Модель нарушителя информационной безопасности и ее значение для выбора методов и средств повышения осведомленности в области информационной безопасности.				2		2
6.	Тема 6. Документальное обеспечение выбора методов и средств для процессов повышения осведомленности в области информационной безопасности в рамках СУИБ.				2		2
7.	Тема 7. Мероприятия по повышению осведомленности в области информационной безопасности в рамках СУИБ и их бюджетирование.				2		2

8.	Тема 8. Сервисы управления навыками кибербезопасности.				2		2
9.	Тема 9. Процессы и подпроцессы повышения осведомленности в области информационной безопасности, применимые методы и средства повышения осведомленности в области информационной безопасности				4		4
10.	Тема 10. Организационные вопросы повышения осведомленности в области информационной безопасности.				2		2
11.	Тема 11. Технические аспекты повышения осведомленности в области информационной безопасности.				2		2
12.	Тема 12. Программные средства повышения осведомленности в области информационной безопасности.				4		4
13.	Тема 13. Идентификация и анализ рисков и возможностей, связанных с повышением осведомленности в области информационной безопасности.				4		4
14.	Тема 14. Методы управления рисками и возможностями процессов, связанных с повышением осведомленности в области информационной безопасности. Снижение рисков, связанных с атаками на персонал.				4		4
15.	Тема 15. Мониторинг уровня осведомленности в области информационной безопасности. Аудит процессов, связанных с повышением осведомленности в области информационной безопасности.				4		4
16.	Тема 16. Измерение уровня повышения осведомленности в области информационной безопасности.				8		8

17	Тема 17. Проблемные вопросы повышения осведомленности в области информационной безопасности, закрепления знаний на практике, выработки навыков безопасного поведения, пути их решения.				6		6
Итого		**108**			**54**		**54**

5 Содержание дисциплины

Раздел 1.

Тема 1. Концепция, политика и цели информационной безопасности при внедрении системы управления информационной безопасностью (СУИБ).

Тема раскрывает основные вопросы, касающиеся концепции, политики и целей информационной безопасности при внедрении системы управления информационной безопасностью (СУИБ), информации о текущем уровне киберграмотности сотрудников организации, стратегии информационной безопасности в части работы с персоналом, применение цикла PDCA в вопросах повышения осведомленности.

Тема 2. Задачи, методы и средства повышения осведомленности в области информационной безопасности в рамках СУИБ.

Тема раскрывает основные моменты и нюансы в области учебных фишинговых рассылок с учетом актуальных векторов атак, специфики компании и новостной повестки, обучающих курсов и тестов, шаблонов имитированных атак.

Тема 3. Стандартизация процессов повышения осведомленности в области информационной безопасности в рамках СУИБ.

Тема раскрывает основные вопросы, касающиеся стандартизации процессов повышения осведомленности в области информационной безопасности в рамках СУИБ, выбора актуальных тем обучения по информационной безопасности, встраивания обучения в рабочий процесс.

Раздел 2.

Тема 4. Классификация угроз информационной безопасности в части, связанной с персоналом организации.

Тема раскрывает основные вопросы, касающиеся классификации угроз информационной безопасности в части, связанной с персоналом организации. В данной теме рассматриваются цифровые угрозы, стратегическая задача снижения киберриска человеческого фактора.

Тема 5. Модель нарушителя информационной безопасности и ее значение для выбора методов и средств повышения осведомленности в области информационной безопасности.

Тема раскрывает основные вопросы, касающиеся модели нарушителя информационной безопасности и ее значения для выбора методов и средств повышения осведомленности в области информационной безопасности.

Тема 6. Документальное обеспечение выбора методов и средств для процессов повышения осведомленности в области информационной безопасности в рамках СУИБ.

Тема раскрывает основные вопросы, касающиеся документального обеспечения выбора методов и средств для процессов повышения осведомленности в области информационной безопасности в рамках СУИБ, планирования обучения и тренировок навыков, формирования шаблона имитированных атак и графика проведения учебных рассылок, создание и согласование регламента обучения, управление группами обучаемого персонала с учетом приема и увольнения сотрудников, формирования отчетов с развернутой аналитикой по обучению и рекомендациями по улучшению политики ИБ в отношении персонала.

Тема 7. Мероприятия по повышению осведомленности в области информационной безопасности в рамках СУИБ и их бюджетирование.

Тема раскрывает основы системы управления информационной безопасностью, место и роль вопросов планирования, проведения, контроля и совершенствования мероприятий по повышению осведомленности в области информационной безопасности в рамках СУИБ и бюджетирование этих мероприятий.

Тема 8. Сервисы управления навыками кибербезопасности.

Тема раскрывает основы развития у сотрудников устойчивых навыков реагирования на фишинговые атаки.

Тема 9. Процессы и подпроцессы повышения осведомленности в области информационной безопасности, применимые методы и средства повышения осведомленности в области информационной безопасности.

Тема раскрывает основные процессы и подпроцессы повышения осведомленности в области информационной безопасности, применимые методы и средства повышения осведомленности в области информационной безопасности.

Раздел 3.

Тема 10. Организационные вопросы повышения осведомленности в области информационной безопасности.

Тема раскрывает организационные вопросы повышения осведомленности в области информационной безопасности.

Тема 11. Технические аспекты повышения осведомленности в области информационной безопасности.

Тема раскрывает главные технические аспекты повышения осведомленности в области информационной безопасности.

Тема 12. Программные средства повышения осведомленности в области информационной безопасности.

Тема раскрывает главные программные средства повышения осведомленности в области информационной безопасности.

Тема 13. Идентификация и анализ рисков и возможностей, связанных с повышением осведомленности в области информационной безопасности.

Тема раскрывает вопросы, связанные с идентификацией и анализом рисков и возможностей, связанных с повышением осведомленности в области информационной безопасности, снижением вероятности утечки конфиденциальной информации.

Раздел 4.

Тема 14. Методы управления рисками и возможностями процессов, связанных с повышением осведомленности в области информационной безопасности.

Тема раскрывает основные методы управления рисками и возможностями процессов, связанных с повышением осведомленности в области информационной безопасности. Снижение рисков, связанных с атаками на персонал.

Тема 15. Мониторинг уровня осведомленности в области информационной безопасности. Аудит процессов, связанных с повышением осведомленности в области информационной безопасности.

Тема раскрывается основные моменты и нюансы мониторинга и изменения уровня осведомленности в области информационной безопасности, аудита процессов, связанных с повышением осведомленности в области информационной безопасности.

Раздел 5.

Тема 16. Измерение уровня повышения осведомленности в области информационной безопасности.

Тема раскрывает измерение уровня повышения осведомленности в области информационной безопасности. Оценка зрелости процессов. Место и роль отчетов о повышении осведомленности в области информационной безопасности в анализе и планировании СМИБ со стороны высшего руководства.

Тема 17. Проблемные вопросы повышения осведомленности в области информационной безопасности, закрепления знаний на практике, выработки навыков безопасного поведения, пути их решения.

Тема раскрывает проблемные вопросы повышения осведомленности в области информационной безопасности, закрепления знаний на практике, выработки навыков безопасного поведения, пути их решения.

6 Тематика семинарских/практических и лабораторных занятий

3.4.1 Семинарские/практические занятия

1. Концепция, политика и цели информационной безопасности при внедрении системы управления информационной безопасностью (СУИБ).
2. Задачи, методы и средства повышения осведомленности в области информационной безопасности в рамках СУИБ.
3. Стандартизация процессов повышения осведомленности в области информационной безопасности в рамках СУИБ.
4. Классификация угроз информационной безопасности в части, связанной с персоналом организации.
5. Модель нарушителя информационной безопасности и ее значение для выбора методов и средств повышения осведомленности в области информационной безопасности.
6. Документальное обеспечение выбора методов и средств для процессов повышения осведомленности в области информационной безопасности в рамках СУИБ.
7. Мероприятия по повышению осведомленности в области информационной безопасности в рамках СУИБ и их бюджетирование.
8. Сервисы управления навыками кибербезопасности.
9. Процессы и подпроцессы повышения осведомленности в области информационной безопасности, применимые методы и средства повышения осведомленности в области информационной безопасности.
10. Организационные вопросы повышения осведомленности в области информационной безопасности.
11. Технические аспекты повышения осведомленности в области информационной безопасности.
12. Программные средства повышения осведомленности в области информационной безопасности.
13. Идентификация и анализ рисков и возможностей, связанных с повышением осведомленности в области информационной безопасности.
14. Методы управления рисками и возможностями процессов, связанных с повышением осведомленности в области информационной безопасности.
15. Мониторинг уровня осведомленности в области информационной безопасности. Аудит процессов, связанных с повышением осведомленности в области информационной безопасности.
16. Измерение уровня повышения осведомленности в области информационной безопасности.
17. Проблемные вопросы повышения осведомленности в области информационной безопасности, закрепления знаний на практике, выработки навыков безопасного поведения, пути их решения.

7 Учебно-методическое и информационное обеспечение

8 Нормативные документы и ГОСТы

1. ГОСТ Р ИСО 27001-2021. Системы менеджмента информационной безопасности. Требования.

2. Федеральный государственный образовательный стандарт высшего образования (уровень магистратуры) по направлению подготовки 10.04.01 Информационная безопасность,

утвержденный приказом Министерства образования и науки Российской Федерации от 26.11.2020 № 1455.

3. Профессиональные стандарты:

– 06.032 Специалист по безопасности компьютерных систем и сетей. Утвержден приказом Министерства труда и социальной защиты РФ от 14.09.2022 № 533н;
– 06.033 Специалист по защите информации в автоматизированных системах. Утвержден приказом Министерства труда и социальной защиты РФ от 14.09.2022 г. № 525н).

9 Основная литература

1. Гультяева Т.А. Основы информационной безопасности [Электронный ресурс]: учебное пособие / Т.А. Гультяева; Новосибирский государственный технический университет. – Новосибирск: Новосибирский государственный технический университет, 2018. – 79 с. Режим доступа: https://biblioclub.ru/index.php?page=book&id=574729

2. Парфёнов, Ю. П. Средства управления и защиты информационных ресурсов автоматизированных систем : учебное пособие / Ю. П. Парфёнов. — 2-е изд. — Москва : ФЛИНТА, 2022. — 120 с. — ISBN 978-5-9765-5016-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/231707. — Режим доступа: для авториз. пользователей.

3. Шилов А.К. Управление информационной безопасностью [Электронный ресурс]: учебное пособие / А.К. Шилов; Министерство науки и высшего образования РФ, Южный федеральный университет, Институт компьютерных технологий и информационной безопасности. – Ростов-на-Дону; Таганрог: Южный федеральный университет, 2018. – 121 с. Режим доступа: https://biblioclub.ru/index.php?page=book&id=500065

10 Дополнительная литература

1 Аверченков В.И. Аудит информационной безопасности [Электронный ресурс]: учебное пособие для вузов / В.И. Аверченков. – М.: ФЛИНТА, 2016. – 269 с. Режим доступа: https://biblioclub.ru/index.php?page=book&id=93245

2 Бекетнова Ю.М. Международные основы и стандарты информационной безопасности финансово-экономических систем [Электронный ресурс]: учебное пособие / Ю.М. Бекетнова, Г.О. Крылов, С.Л. Ларионова; Финансовый университет при Правительстве Российской Федерации. – Москва: Прометей, 2018. – 173 с. Режим доступа: http://biblioclub.ru/index.php?page=book&id=494850

3 Веселов Г.Е. Менеджмент риска информационной безопасности [Электронный ресурс]: учебное пособие / Г.Е. Веселов, Е.С. Абрамов, А.К. Шилов; Министерство образования и науки РФ, Южный федеральный университет, Инженерно- технологическая академия. – Таганрог: Издательство Южного федерального университета, 2016. – 109 с. Режим доступа: http://biblioclub.ru/index.php?page=book&id=493331

4. Полное руководство по обучению в области ИБ. Режим доступа: https://www.kaspersky.ru/resource-center/preemptive-safety/cybersecurity-training?ysclid=ln7p7p538f967632524

5. Повышение осведомленности пользователей по вопросам ИБ. Режим доступа: https://lib.itsec.ru/articles2/control/povyshenie-osvedomlennosti-polzovateley-po-voprosam-ib

11 Электронные образовательные ресурсы

1. ЭОР разрабатывается.
2. Московский Политех подключен к ЭБС: Юрайт, АйПиАр и Лань https://mospolytech.ru/obuchauschimsya/biblioteka/

12 Лицензионное и свободно распространяемое программное обеспечение

1. OpenOffice: режим доступа: свободный.
2. Яндекс.Телемост: режим доступа: свободный.
3. Специальное программное обеспечение не предусмотрено.

13 Современные профессиональные базы данных и информационные справочные материалы

1. Официальный Интернет-сайт Федеральной службы государственной статистики. 2007-2017. – Режим доступа: http://www.gks.ru/, свободный

2. Справочная правовая система Консультант плюс [электронный ресурс] — Режим доступа: http://www.consultant.ru/online/

3. Официальный сайт Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минкомсвязь России) [электронный ресурс] — Режим доступа: http://government.ru/department/387/events/

4. Официальный сайт Росстата [электронный ресурс] — Режим доступа: www.gks.ru/

5. 20 интернет-ресурсов для специалистов по информационной безопасности // официальный сайт компании «ГЕОЛАЙН Технологии» [электронный ресурс] — Режим доступа: http://geoline-tech.com/top-20-sites-about-information-security/

6. Полезные сайты и инструменты// Информационная безопасность. Практика информационной безопасности [электронный ресурс] — Режим доступа: http://dorlov.blogspot.com/p/blog-page_3151.html

7. Информационная безопасность [электронный ресурс] — Режим доступа: http://www.securrity.ru/

8. 30 ресурсов по безопасности, которые точно пригодятся [электронный ресурс] — Режим доступа: https://proglib.io/p/information-security-guide/

9. Информационная безопасность. Защита данных // habr - веб-сайт в формате коллективного блога с элементами новостного сайта [электронный ресурс] — Режим доступа: https://habr.com/ru/hub/infosecurity/

10. База Знаний Клуба Информационной безопасности [электронный ресурс] — Режим доступа: http://wiki.informationsecurity.club/doku.php/main

14 Материально-техническое обеспечение

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, экран) – 1 комплект.

Для проведения лабораторных занятий необходимо наличие компьютерных классов оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

С целью повышения качества ведения образовательной деятельности в университете создана электронная информационно-образовательная среда. Она подразумевает организацию взаимодействия между обучающимися и преподавателями через систему личных кабинетов студентов, расположенных на официальном сайте университета в информационно телекоммуникационной сети «Интернет». Созданная информационно-образовательная среда позволяет осуществлять взаимодействие между участниками образовательного процесса посредством организации дистанционного консультирования по вопросам выполнения практических заданий. В процессе самостоятельной работы студентов предусмотрена возможность получения индивидуальных консультаций преподавателя с использованием электронной почты в сети Интернет.

При работе в аудитории и самостоятельной работе обучающихся для проведения расчётов и оформления отчётов о выполнении лабораторных работ и контрольной работы используются следующие программные продукты:

-веб-браузер «Яндекс» или аналогичные.

-Яндекс.Метрика

Для проведения лабораторных работ и самостоятельной работы студентов подходят аудитории, оснащенные компьютерами с программным обеспечением в соответствии со списком в пункте 4.5 и подключенные к интернету.

Число рабочих мест в аудитории должно быть достаточным для обеспечения индивидуальной работы студентов.

Рабочее место преподавателя должно быть оснащено компьютером с подключенным к нему проектором или иным аналогичным по функциональному назначению оборудованием.

15 Методические рекомендации

16 Методические рекомендации для преподавателя по организации обучения

1. При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.

2. При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

3. При организации и проведения экзаменов в практико-ориентированной форме следует использовать утвержденные кафедрой Методические рекомендации.

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки **10.04.01 «Информационная безопасность»**

17 Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются лекции и лабораторные занятия.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

Самостоятельная работа включает:

- изучение теоретических и практических разделов дисциплины;
- подготовку и оформление расчётно-графической работы.

Общие рекомендации по организации самостоятельной работы:

Время, которым располагает студент для выполнения учебного плана, складывается из двух составляющих: одна из них – это аудиторная работа в вузе по расписанию занятий, другая –внеаудиторная самостоятельная работа. Задания и материалы для самостоятельной работы выдаются во время учебных занятий по расписанию, на этих же занятиях преподаватель осуществляет контроль за самостоятельной работой, а также оказывает помощь студентам по правильной организации работы.

Чтобы выполнить весь объем самостоятельной работы, необходимо заниматься по 1 – 4 часа ежедневно. Начинать самостоятельные внеаудиторные занятия следует с первых же дней семестра. Первые дни семестра очень важны для того, чтобы включиться в работу, установить определенный порядок, равномерный ритм на весь семестр. Ритм в работе –это ежедневные самостоятельные занятия, желательно в одни и те же часы, при целесообразном чередовании занятий с перерывами для отдыха.

Начиная работу, не нужно стремиться делать вначале самую тяжелую ее часть, надо выбрать что-нибудь среднее по трудности, затем перейти к более трудной работе. И напоследок оставить легкую часть, требующую не столько больших интеллектуальных усилий, сколько определенных моторных действий (черчение, построение графиков и т.п.).

Следует правильно организовать свои занятия по времени: 50 минут – работа, 5-10 минут – перерыв; после 3 часов работы перерыв – 20-25 минут. Иначе нарастающее утомление повлечет неустойчивость внимания. Очень существенным фактором, влияющим на повышение умственной работоспособности, являются систематические занятия физической культурой. Организация активного отдыха предусматривает чередование умственной и физической деятельности, что полностью восстанавливает работоспособность.

Методические указания к отдельным видам деятельности:

Лекция: Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, формулировки, выводы. Помечать важные мысли. Выделять ключевые слова, термины. Делать пометки на вопросах, терминах, блоках в тексте, которые вызвали затруднения, после чего постараться найти ответ в рекомендуемой литературе. Если ответ не найден, то на консультации обратиться к преподавателю.

Лабораторная работа: Работа с конспектом лекций и методическими указаниями по выполнению лабораторной работы, просмотр рекомендуемой литературы, конспектирование основных мыслей и выводов, разработка плана выполнения лабораторной работы, предварительная формулировка возможных выводов по работе. Подготовка к практическим занятиям, проработка материала по вопросам, выносимым на практические занятия. Для более углублённого изучения темы задания для самостоятельной работы рекомендуется выполнять параллельно с изучением данной темой.

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются лекции и самостоятельная работа.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, готовятся к промежуточной аттестации, а также самостоятельно изучают отдельные темы учебной программы.

На занятиях студентов, в том числе предполагающих практическую деятельность, осуществляется закрепление полученных, в том числе и в процессе самостоятельной работы, знаний. Особое внимание обращается на развитие умений и навыков установления связи положений теории с профессиональной деятельностью будущего специалиста.

Самостоятельная работа осуществляется индивидуально. Контроль самостоятельной работы организуется в двух формах:

- самоконтроль и самооценка студента;
- контроль со стороны преподавателей (текущий и промежуточный).

Текущий контроль осуществляется на аудиторных занятиях.

Критериями оценки результатов самостоятельной работы студента являются:

- уровень освоения студентом учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- сформированность компетенций;
- оформление материала в соответствии с требованиями.

Приветствуется обсуждение самих заданий с другими студентами: можно как давать, так и получать советы по общей стратегии выполнения и изучения материала, давать и получать помощь.

18 Фонд оценочных средств

19 Методы контроля и оценивания результатов обучения

Приведенные ниже правила выставления оценок и опозданий могут быть изменены, если преподаватель сочтет это необходимым. Важно, чтобы студенты регулярно просматривали план курса, выложенный в СДО, на предмет его обновления или изменения.

Достижение компетенций оценивается с помощью лабораторных работ и рубежных контролей.

Каждый студент имеет право на 6 дней опоздания, которые могут быть потрачены на любые задания в течение семестра. Опоздания предназначены для решения особых ситуаций, таких как болезнь или чрезвычайные семейные обстоятельства.

Когда использованы все дни опоздания за каждый день просрочки начисляется штраф в размере 25% от максимального результата за задание. Задания, присланные позже, чем 4 дня, не будут оцениваться. В связи с зависимостью между работами студентам может потребоваться все равно выполнить предыдущие работы, даже если они не оцениваются.

После сдачи лабораторной работы студент должен ее защитить. Во время защиты лабораторной работы преподаватель проверяет выполнение критериев и требований задания, а студент отвечает на вопросы преподавателя по его лабораторной работе, а также теоретических вопросов, приведенных после текста задания лабораторной работы. Если студент отказывается отвечать на вопросы, или дает полностью неверные ответы, или ответы не по теме, то работа может считаться сданной, но при этом она не оценивается.

Студенты должны заранее сообщать о том, что у них могут возникнуть трудности со своевременной сдачей задания или проекта. При наличии реальных причин задержки студентам следует как можно скорее связаться с преподавателем и обсудить возможные условия.

20 Шкала и критерии оценивания результатов обучения

Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации: экзамен

Промежуточная аттестация обучающихся в форме дифференцированного зачёта проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	Описание
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации. Присутствовал более чем на ¾ занятий
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки. Присутствовал более чем на ¾ занятий
Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность. Присутствовал более чем на ½ занятий

Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации. Присутствовал менее чем на ½ занятий

Лабораторная работа оценивается в процентах степени выполнения следующих критериев и для выставления оценки суммируются проценты за каждый из четырех критериев:

1. Полнота выполнения практического задания (30%): соответствует ли функциональность заданным требованиям и целям, насколько точно и без ошибок лабораторная работа выполняет поставленные задачи, насколько эффективно задание отвечает требованиям целевой аудитории и обеспечивает приятное восприятие.

2. Качество и структура предлагаемых решений (10%): качество, читаемость и организация таблиц, текстов лабораторной работы, проектов документов, рациональность выполнения задания, последовательность именования и соблюдение лучших практик, наличие пояснений и комментариев.

3. Творчество и инновации (10%): творческий подход студентов к выполнению заданий, насколько студенты вышли за рамки основных требований и реализовали дополнительные возможности или использовали уникальные решения.

4. Ответы на вопросы по лабораторной работе студента и теории (50%):

Дает краткий ответ, содержащий ошибки или неточности. На наводящие вопросы отвечает неправильно (10% из 50%)

Дает развернутый ответ, содержащий ошибки или неточности. На наводящие вопросы отвечает неверно (20% из 50%)

Дает развернутый ответ, содержащий ошибки или неточности. На наводящие вопросы отвечает правильно (30% из 50%)

Дает правильные и развернутые ответы на вопросы (50% из 50%).

R лабораторные рассчитывается как среднее результатов за все лабораторные работы. За полное и безошибочное выполнение всех лабораторных работ в срок и их защиту можно получить максимум 100 баллов (R лабораторные).

Рубежный контроль оценивается по следующим критериям:

1. Полнота выполнения практического задания (30%): соответствует ли функциональность заданным требованиям и целям, насколько точно и без ошибок лабораторная работа выполняет поставленные задачи, насколько эффективно задание отвечает требованиям целевой аудитории и обеспечивает приятное восприятие.

2. Качество и структура предлагаемых решений (10%): качество, читаемость и организация таблиц, текстов лабораторной работы, проектов документов, рациональность выполнения задания, последовательность именования и соблюдение лучших практик, наличие пояснений и комментариев.

3. Творчество и инновации (10%): творческий подход студентов к выполнению заданий, насколько студенты вышли за рамки основных требований и реализовали дополнительные возможности или использовали уникальные решения.

4. Ответы на вопросы по лабораторной работе студента и теории (50%):

Подробное описание критериев дается в тексте задания рубежного контроля.

За полностью выполненные рубежные контроли также можно получить 100 баллов (R контроль).

Также имеется коэффициент сданных работ K сданные, который равен 1 если все работы сданы и 0 если хотя бы одна работа не сдана.

Итоговый балл рассчитывается по формуле: R сем = (0,5 x R лабораторные + 0,5 x R контроль) * K сданные.

Итоговый балл пересчитывается по шкале ниже и на основании полученной оценки фиксируется результат промежуточной аттестации.

Соответствие баллов в 100 балльной рейтинговой системе оценке по 4-бальной шкале:
0-54 - неудовлетворительно
55-69 - удовлетворительно
70-84 - хорошо
85-100 – отлично

21 Оценочные средства

7.3.1 Текущий контроль

Примерный список вопросов:

1. Концепция, политика и цели информационной безопасности при внедрении системы управления информационной безопасностью (СУИБ).
2. Информация о текущем уровне киберграмотности сотрудников организации.
3. Стратегии информационной безопасности в части работы с персоналом.
4. Применение цикла PDCA в вопросах повышения осведомленности в области информационной безопасности.
5. Задачи, методы и средства повышения осведомленности в области информационной безопасности в рамках системы управления информационной безопасностью (СУИБ).
6. Учебные фишинговые рассылки с учетом актуальных векторов атак, специфики компании и новостной повестки.
7. Обучающие курсы и тесты.
8. Шаблоны имитированных атак.
9. Стандартизация процессов повышения осведомленности в области информационной безопасности в рамках системы менеджмента информационной безопасности (СМИБ).
10. Выбор актуальных тем обучения по информационной безопасности, встраивания обучения в рабочий процесс.
11. Классификация угроз информационной безопасности в части, связанной с персоналом организации.
12. Цифровые угрозы.
13. Стратегическая задача снижения киберриска человеческого фактора.
14. Модель нарушителя информационной безопасности и ее значение для выбора методов и средств повышения осведомленности в области информационной безопасности.
15. Модель нарушителя информационной безопасности и ее значение для выбора методов и средств повышения осведомленности в области информационной безопасности.
16. Документальное обеспечение выбора методов и средств для процессов повышения осведомленности в области информационной безопасности в рамках системы управления информационной безопасностью (СУИБ).
17. Планирование обучения и тренировок навыков.
18. Формирование шаблона имитированных атак и графика проведения учебных рассылок.
19. Создание и согласование регламента обучения.
20. Управление группами обучаемого персонала с учетом приема и увольнения сотрудников.
21. Формирование отчетов с развернутой аналитикой по обучению и рекомендациями по улучшению политики информационной безопасности в отношении персонала.
22. Мероприятия по повышению осведомленности в области информационной безопасности и их бюджетирование.
23. Тема раскрывает основы системы управления информационной безопасностью, место и роль вопросов планирования, проведения, контроля и совершенствования мероприятий по повышению осведомленности в области информационной безопасности в рамках СУИБ и бюджетирование этих мероприятий.
24. Сервисы управления навыками кибербезопасности.
25. Развитие у сотрудников устойчивых навыков реагирования на фишинговые атаки.

26. Процессы и подпроцессы повышения осведомленности в области информационной безопасности, применимые методы и средства повышения осведомленности в области информационной безопасности.
27. Организационные вопросы повышения осведомленности в области информационной безопасности.
28. Технические аспекты повышения осведомленности в области информационной безопасности.
29. Программные средства повышения осведомленности в области информационной безопасности.
30. Идентификация и анализ рисков и возможностей, связанных с повышением осведомленности в области информационной безопасности.
31. Снижение вероятности утечки конфиденциальной информации.
32. Методы управления рисками и возможностями процессов, связанных с повышением осведомленности в области информационной безопасности.
33. Снижение рисков, связанных с атаками на персонал.
34. Мониторинг уровня осведомленности в области информационной безопасности.
35. Аудит процессов, связанных с повышением осведомленности в области информационной безопасности.
36. Измерение уровня повышения осведомленности в области информационной безопасности.
37. Оценка зрелости процессов повышения осведомленности в области информационной безопасности.
38. Место и роль отчетов о повышении осведомленности в области информационной безопасности в анализе и планировании системы управления информационной безопасностью (СУИБ) со стороны высшего руководства.
39. Проблемные вопросы повышения осведомленности в области информационной безопасности, закрепления знаний на практике, выработки навыков безопасного поведения, пути их решения.
40. Практические примеры выбора эффективных методов и средств повышения осведомленности в области информационной безопасности.

Пример билета.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №1
по дисциплине

«МЕТОДЫ И СРЕДСТВА ПОВЫШЕНИЯ ОСВЕДОМЛЕННОСТИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки
10.04.01 Информационная безопасность

ВОПРОСЫ:

1. Концепция, политика и цели информационной безопасности при внедрении системы управления информационной безопасностью (СУИБ).
2. Процессы и подпроцессы повышения осведомленности в области информационной безопасности, применимые методы и средства повышения осведомленности в области информационной безопасности.

Утверждено: _____ / _____ / «__» _____ 20__г.

7.3.2 Промежуточная аттестация

Оценочные средства для промежуточной аттестации не требуется, так как оценка за промежуточную аттестацию выставляется по балльно-рейтинговой системе, описанной в пункте 7.2.