ФГБОУ ВО «Санкт-Петербургский университет ГПС МЧС России»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Специалитет по специальности
10.05.03 – Информационная безопасность автоматизированных систем

Специализация «Анализ безопасности информационных систем»

Санкт-Петербург

1. Цели и задачи дисциплины

Цель освоения дисциплины:

– формирование навыков организации и методологии обеспечения информационной безопасности в организациях; создание представления о функциях, структурах и штатах подразделения информационной безопасности; об организационных основах, принципах, методах и технологиях и управлении информационной безопасностью в организациях РФ; развитие способностей по использованию существующей системы управления информационной безопасности.

Перечень компетенций, формируемых в процессе изучения дисциплины

Компетенции	Содержание
ОПК - 13	Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем
ОПК – 15	Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем
ОПК – 7.2	Способен разрабатывать методики и тесты для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации

Задачи дисциплины:

- изучение основ культуры обеспечения информационной безопасности;
- изучение роли процессов управления в обеспечении информационной безопасности организаций, объектов и систем;
- изучение основных методов безопасности организаций, объектов и систем;
- изучение различных методов реализации процессов управления информационной безопасностью.

2. Перечень планируемых результатов дисциплины, соотнесенных с индикаторами достижения компетенций

Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
ОПК-13.1. Использует модели угроз и рисков информационной безопасности автоматизированных систем, методы оценки уязвимостей каналов передачи информации	**Знает** модели угроз и рисков информационной безопасности автоматизированных систем, методы оценки уязвимостей каналов передачи информации **Умеет** применять модели угроз и рисков информационной безопасности автоматизированных систем, методы оценки уязвимостей каналов передачи информации в профессиональной деятельности
ОПК-15.3. Применяет инструментальные средства мониторинга и анализа состояния системы информационной безопасности	**Знает** основные инструментальные средства мониторинга и анализа состояния системы информационной безопасности **Умеет** применять на практике инструментальные средства мониторинга и анализа состояния системы информационной безопасности
ОПК-7.2.3. Обладает навыками формирования требований по защите информации информационных систем; настройки систем передачи данных и тестирования информационных систем	**Знает** требования по защите информации информационных систем **Умеет** настраивать системы передачи данных и тестировать информационные системы на соответствие требований по защите информации

3. Место дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Управление информационной безопасностью» относится к обязательной части образовательной программы специалитета по специальности **10.05.03 – Информационная безопасность автоматизированных систем**, специализация - **Анализ безопасности информационных систем.**

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 6 зачётных единиц, 216 часов.

4.1 Распределение трудоемкости учебной дисциплины по видам работ по семестрам для очной формы обучения

Вид учебной работы	Трудоемкость			
	з.е.	час.	по семестрам	
			10	11
Общая трудоемкость дисциплины по учебному плану	**6**	**216**	**72**	**144**
Контактная работа		**92**	**36**	**56**
Лекции		32	14	18
Лабораторные		4		4
Практические занятия		54	22	32
Консультация		2		2
Самостоятельная работа		**88**	**36**	**52**
Зачет с оценкой			+	
Экзамен		**36**		+

4.2. Тематический план, структурированный по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий для очной формы обучения

Наименование разделов	**Всего часов**	**Количество часов по видам занятий**					**Самостоятельная работа**
		Лекции	**Практические занятия**	**Лабораторные работы**	**Консультации**	**Контроль**	
10семестр							
Раздел 1. Основы управления ИБ	24	6	6				12
Раздел 2. Политика безопасности организации	24	4	8				12
Раздел 3. Системы управления ИБ	24	4	8				12
Зачет с оценкой						+	
Итого за 10 семестр	**72**	**14**	**22**				**36**
11 семестр							
Раздел 4. Основы управления рисками ИБ	36	6	12				18
Раздел 5. Процессы управления ИБ	36	6	10				18
Раздел 6. Системы обнаружения и предотвращения компьютерных атак	34	6	10	4			16
Консультация	2				2		
Экзамен	36					+	
Итого за 11 семестр	**144**	**18**	**32**	**4**	**2**	**36**	**52**
Всего за 10, 11 семестр	**216**	**32**	**58**	**4**	**2**	**36**	**88**

4.3 Содержание дисциплины для очной формы обучения

Раздел 1. Основы управления ИБ

Лекции. Цели и задачи курса. Рекомендуемая литература. Основные понятия и определения. Содержание и задачи процесса управления информационной безопасностью автоматизированных систем и организации в целом.

Практические занятия. Политика государства в области информационной безопасности. Базовые вопросы управления ИБ. Стандартизация в области управления ИБ

Самостоятельная работа. Задачи процесса управления информационной безопасностью автоматизированных систем и организации в целом

Рекомендуемая литература:

Основная литература: [1];

Дополнительная литература: [1,2].

Раздел 2. Политика безопасности организации

Лекции. Содержание политики безопасности. Управление активами. Безопасность, связанная с управлением персоналом. Жизненный цикл политики безопасности

Практические занятия. Аудит информационной безопасности. Назначение, цели и виды аудита ИБ. Требования к аудитору ИБ, особенности взаимодействия в процессе аудита. Оценка работы аудитора.

Самостоятельная работа. Стандартизация в сфере аудита информационной безопасности. Содержание и организация процесса аудита информационной безопасности. Оценка рисков информационной безопасности. Отчетные документы по результатам аудита. Выполнение рекомендаций по итогам проведения аудита информационной безопасности.

Рекомендуемая литература:

Основная литература: [1];

Дополнительная литература: [1,2].

Раздел 3. Системы управления ИБ

Лекции. Системный подход к управлению информационной безопасностью. Стандартизация в сфере управления информационной безопасностью.

Практические занятия. Процессный подход к управлению ИБ. Область деятельности СУИБ. Ролевая структура СУИБ. Политика СУИБ

Самостоятельная работа. Системный подход к управлению информационной безопасностью. Стандартизация в сфере управления информационной безопасностью.

Рекомендуемая литература:

Основная литература: [1];

Дополнительная литература: [1,2].

Раздел 4. Основы управления рисками ИБ

Лекции. Угрозы и нарушители безопасности информации. Рискология ИБ. Методы анализа рисков ИБ

Практические занятия. Практическое применение методов анализа рисков ИБ.

Самостоятельная работа. Операционные процедуры и обязанности. Процедуры реагирования на события. Разделение обязанностей. Сетевое администрирование. Средства управления безопасностью сетей. Групповые политики безопасности.

Рекомендуемая литература:

Основная литература: [2];

Дополнительная литература: [1,3].

Раздел 5. Процессы управления ИБ

Лекции. Основные процессы СУИБ. Внедрение разработанных процессов. Внедрение мер (контрольных процедур) по обеспечению ИБ. Процесс «Управление инцидентами ИБ». Эксплуатация и независимый аудит СУИБ

Практические занятия. Средства управления информационной безопасностью.

Самостоятельная работа. Программные средства автоматизации процедур информационной безопасности и анализа политики информационной безопасности. Программные средства поддержки процессов управления информационной безопасности

Рекомендуемая литература:

Основная литература: [2];

Дополнительная литература: [1,3].

Раздел 6. Системы обнаружения и предотвращения компьютерных атак

Лекции. Требования к системам обнаружения и предотвращения компьютерных атак. Системы анализа защищенности. Системы обнаружения атак.

Практические занятия. Системы контроля целостности. Системы анализа журналов регистрации. Критерии выбора систем обнаружения и предотвращения компьютерных атак

Лабораторная работа. Формирование заданий по безопасности и SIEM-экосистемы

Самостоятельная работа. Основные положения стандартов в области управления инцидентами информационной безопасности. Регламентация действий сотрудников при возникновении нештатных ситуаций.

Рекомендуемая литература:

Основная литература: [2];
Дополнительная литература: [1,3].

5. Методические рекомендации по организации изучения дисциплины

При реализации программы учебной дисциплины используется традиционная образовательная технология, основой которой является системный принцип построения разделов и тем, используются лекционные, практические занятия и лабораторная работа.

Общими целями занятий являются:

– обобщение, систематизация, углубление, закрепление теоретических знаний по конкретным темам дисциплины;

– формирование умений применять полученные знания на практике, реализация единства интеллектуальной и практической деятельности;

– выработка при решении поставленных задач профессионально значимых качеств: самостоятельности, ответственности, точности, творческой инициативы.

Целями лекции являются:

- дать систематизированные научные знания по дисциплине, акцентировав внимание на наиболее сложных вопросах;

стимулировать активную познавательную деятельность обучающихся, способствовать формированию их творческого мышления.

В ходе практического занятия обеспечивается процесс активного взаимодействия обучающихся с преподавателем; приобретаются практические навыки и умения. Цель практического занятия: углубить и закрепить знания, полученные на лекции, формирование навыков использования знаний для решения практических задач; выполнение тестовых заданий по проверке полученных знаний и умений.

Целями лабораторной работы являются: формирование исследовательских умений и навыков; развитие аналитических, проектировочных и конструктивных умений. выработка самостоятельности, ответственности и творческой инициативы.

Самостоятельная работа обучающихся направлена на углубление и закрепление знаний, полученных на лекциях и других занятиях, выработку навыков самостоятельного активного приобретения новых, дополнительных знаний, подготовку к предстоящим занятиям.

6. Оценочные материалы по дисциплине

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины, проводится в соответствии с содержанием дисциплины по видам занятий в форме типовых контрольных заданий.

Промежуточная аттестация обеспечивает оценивание промежуточных и окончательных результатов освоения дисциплины, проводится в форме зачета с оценкой (10 семестр) и экзамена (11 семестр).

6.1. Примерные оценочные материалы:

6.1.1. Текущего контроля

Примерные вопросы для теста:

1. К какой разновидности моделей управления доступом относится модель Белла-Ла Падулы? а) модель дискреционного доступа; б) модель мандатного доступа; в) ролевая модель.
2. Как называются угрозы, вызванные ошибками в проектировании АИС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.?
3. К каким мерам защиты относится политика безопасности? а) к административным; б) к законодательным; в) к программно-техническим; г) к процедурным.
4. В каком из представлений матрицы доступа наиболее просто определить пользователей, имеющих доступ к определенному файлу? а) ACL; б) списки полномочий субъектов; в) атрибутные схемы.
5. Как называется свойство информации, означающее отсутствие неправомочных, и не предусмотренных ее владельцем изменений? а) целостность; б) апеллируемость; в) доступность; г) конфиденциальность; д) аутентичность
6. К основным принципам построения системы защиты АИС относятся: а) открытость; б) взаимозаменяемость подсистем защиты; в) минимизация привилегий; г) комплексность; д) простота
7. Какие из следующих высказываний о модели управления доступом RBAC справедливы? а) с каждым субъектом (пользователем) может быть ассоциировано несколько ролей; б) роли упорядочены в иерархию; в) с каждым объектом доступа ассоциировано несколько ролей ; г) для каждой пары «субъект-объект» назначен набор возможных разрешений
8. Диспетчер доступа... а) ... использует базу данных защиты, в которой хранятся правила разграничения доступа; б) ... использует атрибутные схемы для представления матрицы доступа; в) ... выступает посредником при всех обращениях субъектов к объектам; г) ... фиксирует информацию о попытках доступа в системном журнале;
9. Какие предположения включает неформальная модель нарушителя? а) о возможностях нарушителя; б) о категориях лиц, к которым

может принадлежать нарушитель; в) о привычках нарушителя; г) о предыдущих атаках, осуществленных нарушителем; д) об уровне знаний нарушителя

10. Что представляет собой доктрина информационной безопасности РФ? а) нормативно-правовой акт, устанавливающий ответственность за правонарушения в сфере информационной безопасности; б) федеральный закон, регулирующий правоотношения в области информационной безопасности; в) целевая программа развития системы информационной безопасности РФ, представляющая собой последовательность стадий и этапов; г) совокупность официальных взглядов на цели, задачи, принципы и основные на- правления обеспечения информационной безопасности Российской Федерации

11. К какому виду мер защиты информации относится утвержденная программа работ в области безопасности? а) политика безопасности верхнего уровня; б) политика безопасности среднего уровня; в) политика безопасности нижнего уровня; г) принцип минимизации привилегий; д) защита поддерживающей инфраструктуры.

12. Какие из перечисленных ниже угроз относятся к классу преднамеренных? а) заражение компьютера вирусами; б) физическое разрушение системы в результате пожара; в) отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.); г) проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации; д) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств; е) вскрытие шифров криптозащиты информации

6.1.2. Промежуточной аттестации

Примерный перечень вопросов, выносимых на зачет с оценкой

1. Приведите убедительные доводы того, что информационная безопасность - одна из важнейших проблем современной жизни..
2. Для каких целей служит сервис анализа защищенности? В чем заключается специфика управления, как сервиса безопасности?
3. Охарактеризуйте шифрование (криптографию) в качестве основного сервиса безопасности ИС.
4. Дайте определение персональных данных. Какие сведения могут быть отнесены к персональным данным? Кто является держателем персональных данных?
5. Охарактеризуйте экранирование в качестве основного сервиса безопасности ИС. Что такое firewall и как он функционирует?

6. Перечислите и охарактеризуйте защитные действия от НСД к конфиденциальной информации.

7. Каким требованиям должна удовлетворять информация, чтобы ее можно было бы отнести к служебной тайне? Приведите перечень сведений, которые не могут быть отнесены к служебной информации ограниченного распространения.

8. В чем заключается основная задача аудита, как сервиса безопасности?

9. Перечислите и прокомментируйте защитные действия от утечки конфиденциальной информации.

10. Перечислите и охарактеризуйте основные объекты профессиональной тайны. Каким требованиям должна удовлетворять информация, чтобы ее можно было бы отнести к профессиональной тайне?

11. Что такое протоколирование? Прокомментируйте особенности применения данного сервиса безопасности.

12. Каким требованиям должна отвечать коммерческая тайна? Охарактеризуйте о сановные субъекты права на коммерческую тайну. Какая информация не может быть отнесена к коммерческой тайне?

13. В чем заключается основная задача логического управления доступом? Что такое матрица доступа? Какая информация анализируется при принятии решения о предоставлении доступа?

14. Дайте определение способа защиты информации. Охарактеризуйте основные способы защиты. Перечислите основные защитные действия при реализации способов ЗИ.

15. Перечислите основные виды конфиденциальной информации, нуждающейся в защите.

16. Прокомментируйте возможности биометрической идентификации (аутентификации).

17. Перечислите основные угрозы конфиденциальности информации.

18. Что такое государственная тайна? Перечислите сведения, которые могут быть отнесены к государственной тайне. Приведите классификацию сведений, составляющих государственную тайну, по степеням секретности.

19. Прокомментируйте парольную идентификацию. Какие меры позволяют повысить надежность парольной защиты?

20. Охарактеризуйте основные угрозы целостности конфиденциальной информации.

21. Дайте определение защищаемой информации и охарактеризуйте ее основные признаки

Примерный перечень вопросов, выносимых на экзамен

1. Что такое идентификация? Дайте толкование понятия «аутентификация». Из-за каких причин затруднена надежная идентификация?

2. Что такое вредоносное программное обеспечение? Дайте определение «бомбы», «червя», «вируса». Какие негативные последствия в функционировании ИС вызывает вредоносное ПО?

3. Раскройте содержание политических, Экономических и организационно-технических факторов, влияющих на состояние информационной безопасности РФ

4. Какие аспекты современных ИС с точки зрения безопасности наиболее существенны?

5. Прокомментируйте наиболее распространенные угрозы доступности. Охарактеризуйте программные атаки на доступность

6. Перечислите основные причины важности программно-технического уровня ИБ. Назовите основные сервисы ИБ программно-технического уровня.

7. Что такое источник угроз безопасности информации? Назовите основные источники преднамеренных угроз.

8. Перечислите направления повседневной деятельности системного администратора, обеспечивающие поддержание работоспособности ИС.

9. Что такое канал утечки информации? Что такое технический канал утечки информации? Охарактеризуйте случайный и организованный канал утечки информации

10. В чем заключается основная специфика процедурного уровня ИБ? Перечислите основные классы мер процедурного уровня ИБ. Почему вопросы поддержания работоспособности ИС являются принципиальными на процедурном уровне ИБ?

11. Что такое управление рисками? Почему управление рисками рассматривается на административном уровне ИБ? В чем заключается суть мероприятий по управлению рисками?

12. Перечислите важнейшие задачи обеспечения информационной безопасности РФ.

13. Назовите главную цель мер административного уровня ИБ. Что понимается под политикой безопасности? Приведите примерный список решений верхнего уровня политики безопасности.

14. Что такое атака? Что такое окно опасности? Какие события происходят во время существования окна опасности?

15. Дайте определение угроз конфиденциальной информации. Какие действия определяют угрозы конфиденциальной информации?

16. Дайте определение лицензирования. Кто такие лицензиат и лицензирующие органы? Почему лицензирование и сертификация выступают в качестве средства защиты информации? Перечислите перечень видов деятельности, касающихся ИБ, на осуществление которых требуются лицензии.

17. Что такое «источник конфиденциальной информации»? Перечислите основные источники конфиденциальной информации.

18. Какие статьи Уголовного кодекса напрямую касаются информационной безопасности?

19. Что такое объекты угроз ИБ? В чем выражаются угрозы информации? Каковы основные источники угроз защищаемой информации? Каковы цели угроз информации со стороны злоумышленников?

20. Какая информация является предметом защиты? Перечислите основные свойства информации как предмета защиты. Охарактеризуйте секретную и конфиденциальную информацию.

21. Перечислите основные компоненты концептуальной модели ИБ. Изобразите графически схему концептуальной модели системы ИБ.

22. Дайте определение информационной системы. Перечислите структурные компоненты информационных систем. Что понимают под информационными ресурсами и процессами?

23. Что понимается под системой управления безопасностью?

6.2. Шкала оценивания результатов промежуточной аттестации и критерии выставления оценок

Форма контроля	**Показатели оценивания**	**Критерии выставления оценок**	**Шкала оценивания**
зачёт с оценкой (экзамен)	правильность и полнота ответа; выполнение контрольных нормативов	дан правильный, полный ответ на поставленный вопрос, показана совокупность осознанных знаний по дисциплине, доказательно раскрыты основные положения вопросов; могут быть допущены недочеты, исправленные самостоятельно в процессе ответа; выполнение контрольных нормативов более половины на оценку «отлично», остальные не ниже «хорошо».	Отлично
		дан правильный, недостаточно полный ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи; могут быть допущены недочеты, исправленные с помощью преподавателя; выполнение контрольных нормативов более половины на оценку «хорошо», остальные не ниже «удовлетворительно».	Хорошо
		дан недостаточно правильный и полный ответ, логика и последовательность изложения имеют нарушения, в ответе	Удовлетворительно

		отсутствуют выводы; выполнение контрольных нормативов более половины на оценку «удовлетворительно», остальные не ниже «отлично» и «хорошо» или все «удовлетворительно».	
		ответ представляет собой разрозненные знания с существенными ошибками по вопросу, присутствуют фрагментарность, нелогичность изложения, дополнительные и уточняющие вопросы не приводят к коррекции ответа на вопрос; выполнение одного и более контрольного норматива на оценку «неудовлетворительно».	Неудовлетворительно

7. Ресурсное обеспечение дисциплины.

7.1. Лицензионное и свободно распространяемое программное обеспечение

Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:

1. Astra Linux Common Edition релиз Орел - операционная систем общего назначения. Лицензия №217800111-ore-2.12-client-6196.
2. Astra Linux Special Edition - операционная система общего назначения. Лицензия №217800111-alse-1.7-client-medium-x86_64-0-14545.
3. Astra Linux Special Edition - операционная система общего назначения. Лицензия №217800111-alse-1.7-client-medium-x86_64-0-14544.

7.2. Профессиональные базы данных и информационные справочные системы

1. Портал открытых данных Российской Федерации https://data.gov.ru/ (свободный доступ).
2. Федеральный портал «Российское образование» http://www.edu.ru (свободный доступ).
3. Система официального опубликования правовых актов в электронном виде http://publication.pravo.gov.ru (свободный доступ).
4. Электронная библиотека университета http://elib.igps.ru (авторизованный доступ).
5. Электронно-библиотечная система «ЭБС» IPR BOOKS» http://www.iprbookshop.ru (авторизованный доступ).

6. Электроно-библиотечная система «Лань» https://e.lanbook.com (авторизованный доступ).

7.3. Литература

Основная литература:

1. Овчинникова Е.А. Основы управления информационной безопасностью : учебное пособие / Е. А. Овчинникова ; под редакцией С. Н. Новикова. — Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2023. — 167 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/138782.html

2. Метельков А.Н., Уткин О.В. Организационно-правовые и технические основы защиты конфиденциальной информации в МЧС России: учебное пособие. - СПб.: СПбУ ГПС МЧС России, 2022. - 216 с. - http://elib.igps.ru/?10&type=card&cid=ALSFR-5db13d78-75cf-449f-8f61-04f06a5e0dd7&remote=false

Дополнительная литература:

1. Шилов А.К. Управление информационной безопасностью : учебное пособие / Шилов А.К.. — Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2018. — 120 с. — ISBN 978-5-9275-2742-7. — Текст : электронный // IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/87643.html.

2. Поздняк, И. С. Управление информационной безопасностью : методические указания / И. С. Поздняк, И. С. Макаров. — Самара : ПГУТИ, 2019. — 43 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223313 .

3. Поздняк, И. С. Планирование и управление информационной безопасностью : учебное пособие / И. С. Поздняк, И. С. Макаров, Л. Р. Чупахина. — Самара : ПГУТИ, 2020. — 69 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/255569 .

7.4. Материально-техническое обеспечение

Для проведения и обеспечения занятий используются помещения, которые представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой специалитета, оснащенные оборудованием и техническими средствами обучения: автоматизированное рабочее место преподавателя, маркерная доска, мультимедийный проектор, документ-камера, посадочные места обучающихся.

Лабораторное занятие на 6 курсе обучения (11 семестр) проводится в лаборатории автоматизированных систем в защищенном исполнении.

Помещения для практических занятий и самостоятельной работы обучающихся оснащены компьютерной техникой, с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде университета.

Автор: кандидат технических наук, доцент Матвеев Александр Владимирович.