МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ФГБОУ ВО «ИГУ»

Кафедра радиофизики и радиоэлектроники

УТВЕРЖДАЮ
Декан _____ Буднев Н.М.
«22» апреля 2020 г.

Рабочая программа дисциплины (модуля)

Наименование дисциплины (модуля**) Б1.В.01 Технико-экономическое обоснование и управление проектами**

Направление подготовки 10.03.01 Информационная безопасность

Тип образовательной программы - бакалавриат

Направленность (профиль) подготовки N 4 "Безопасность автоматизированных систем" (по отрасли или в сфере профессиональной деятельности)

Квалификация выпускника бакалавр

Форма обучения очная

Согласовано с УМК физического факультета
Протокол № 25 от «21» апреля 2020 г.
Председатель _____ Буднев Н.М.

Рекомендовано кафедрой радиофизики и радиоэлектроники:
Протокол № 8
От «20» марта 2020 г.
И.О.Зав. кафедрой _____ Колесник С.Н.

Иркутск 2020 г.

Содержание

стр.

1. Цели и задачи дисциплины (модуля)

Цели: Главной целью дисциплины является формирования у обучающихся универсальных, общепрофессиональных и профессиональных компетенций в соответствии с требованиями ФГОС ВО по направлению подготовки 10.03.01 **«Информационная безопасность»** направленность (профиль) **«Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности),** а также изучение теоретических, методологических и практических проблем формирования **т**ехнико-экономическое обоснование и управлением проектами, а также функционирования и развития систем управления информационной безопасностью и защитой информации

Задачи:

– направленность на многоуровневую систему образования и непрерывность профессионального развития;

– обеспечение обучающимися выбора индивидуальной образовательной траектории;

– практико-ориентированное обучение, позволяющее сочетать фундаментальные знания с практическими навыками по направлению подготовки 10.03.01 Информационная безопасности, учитывающие требования предъявляемых к выпускникам на рынке труда, обобщения отечественного и зарубежного опыта, проведения консультаций с ведущими работодателями и иных источников;

– формирование готовности выпускников Университета к активной профессиональной и социальной деятельности

- раскрытие места информационной безопасности и защиты информации в системе информационных отношений;

- раскрытие направлений и областей деятельности субъектов информационных отношений, составной частью которых является обеспечение информационной безопасности и защита информации;

- определение места защиты информации в обеспечении сохранности документальной базы, раскрывающей различные стороны социально-экономического и культурного развития страны.

2. Место дисциплины в структуре ОПОП

Учебная дисциплина **«Технико-экономическое обоснование и управлением проектами»** относится к обязательной части программы

Для изучения данной учебной дисциплины (модуля) необходимы знания, умения и навыки, формируемые предшествующими дисциплинами*:*

«Документоведение. Нормативные документы в сфере информационной безопасности». «Защита и обработка конфиденциальных документов», «Основы построения и функционирования технических средств защиты информации», «Компьютерная защита информации от несанкционированного доступа», «Управление проектами», «Защита информации от утечки по техническим каналам», «Организационное и правовое обеспечение информационной безопасности», «Программно-аппаратные средства защиты информации», «Основы управления информационной безопасностью»

Перечень последующих учебных дисциплин, для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной: «Комплексная система защиты информации», «Государственная итоговая аттестация».

)

3. Требования к результатам освоения дисциплины (модуля)

Процесс изучения дисциплины (модуля) направлен на формирование следующих компетенций:

ОПК-7. способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты

В результате изучения дисциплины студент должен:

Знать: нормативную документацию в сфере защиты информации при решении задач профессиональной деятельности

Уметь: использовать нормативную документацию в сфере защиты информации при решении задач профессиональной деятельности

Владеть: навыками по применению нормативной документации в сфере защиты информации при решении задач профессиональной деятельности**.**

ПК-7. способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений

Знать: рабочую техническую документацию с учетом действующих нормативных и методических документов

Уметь: использовать нормативную и техническую документацию с учетом действующих нормативных и методических документов

Владеть: навыками по применению рабочей технической документацией с учетом действующих нормативных и методических документов

ПК-14. способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности

Знать: рабочую техническую документацию с учетом действующих нормативных и методических документов

Уметь: использовать документацию по управлению проектной деятельностью

Владеть: навыками по применению рабочей технической документацией с учетом действующих нормативных и методических документов

4. Объем дисциплины (модуля) и виды учебной работы

Вид учебной работы	Всего часов / зачетных единиц	Семестры			
		8			
Аудиторные занятия (всего)	108/3	108/3			
В том числе:	-	-	-	-	-
Лекции	44/1,2	44/1,2			
Практические занятия (ПЗ)	44/1,2	44/1,2			
Семинары (С)					
Лабораторные работы (ЛР)					
КСР	4/0,11	4/0,11			
Самостоятельная работа (всего)	16/0,44	16/0,44			
В том числе:	-	-	-	-	-
Курсовой проект (работа)					
Расчетно-графические работы					
Реферат (при наличии)					
Другие виды самостоятельной работы	16/0,44	16/0,44			
Вид промежуточной аттестации (*зачет, экзамен*)	зачет	зачет			
Контактная работа (всего)					
Общая трудоемкость часы	108	108			
зачетные единицы	3	3			

5. Содержание дисциплины (модуля)

5.1. Содержание разделов и тем дисциплины (модуля). Все разделы и темы нумеруются

1.Раздел
Категории затрат на безопасность информационных активов
Затраты на предупредительные организационные мероприятия (формирование, поддержание системы управления информационной безопасностью, организационные мероприятия по предотвращению нарушений политики безопасности предприятия)
Затраты на предупредительные технические мероприятия (техническое обслуживание системы защиты информации и мероприятия по предотвращению нарушений политики безопасности предприятия)
Затраты на ликвидацию последствий нарушения политики информационной безопасности (компенсация потерь при на-рушениях политики безопасности в случаях, связанных с утечкой информации, потерей имиджа компании, утратой доверия партнеров и потребителей и т.п.).

2. Раздел

Общие ежегодные затраты на информационную безопасность

3.Раздел

Необходимые затраты на информационную безопасность

Формирование политики безопасности
Обслуживание технических средств защиты
Установка антивирусного программного обеспечения
Функционирование и аудит системы безопасности
Конфиденциальное делопроизводство
Обучение персонала методам информационной безопасности.

4.Раздел

Методика уменьшения затрат при соблюдении политики безопасности и проведении профилактики нарушений

Затраты на восстановление системы безопасности до соответствия требованиям политики безопасности
Затраты на восстановление информационных активов предприятия
Затраты на переделки внутри системы безопасности
Затраты на восстановление удовлетворенности государственных организаций и партнеров
Затраты на юридические споры и выплаты компенсаций;
Затраты на выявление причин нарушения политики безопасности

5.Раздел

Обстоятельства отличия стоимости защитных мероприятий

Величины и характер деятельности
Нормативно-правовая база
Уровень зависимости от информационно-телекоммуникационных технологий
Вовлеченность в электронный бизнес, профессиональные и личностные качества персонала

6.Раздел

Распределение бюджета на информационные технологии и информационную безопасность

5.2. Разделы дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) дисциплин	№№ разделов (тем) данной дисциплины, необходимых для изучения обеспечиваемых (последующих) дисциплин
1	Техническая защита информации	1-16
2	Радиотехнические цепи и сигналы	1-16
3	Защита информации от несанкционированного доступа	1-16
4	Электроника и схемотехника	1-16
5	Операционные системы	1-16
6	Базы данных	1-16
7	Электротехника	1-16
8	Основы построения и функционирования специальных технических средств	1-16
9	Безопасность компьютерных сетей	1-16
10	Практика по получению первичных профессиональных умений и навыков	1-16
11	Эксплуатационная практика	1-16
12	Проектно-технологическая практика	1-16

5.3. Разделы и темы дисциплин (модулей) и виды занятий

№ п/п	Наименование раздела	Наименование темы	Виды занятий в часах					
			Лекц.	Практ. зан.	Семин	Лаб. зан.	СРС	Всего
1.	***Раздел 1***	Тема 1	2	2			1	5
2.	***Раздел 2***	Тема 2	3	3			2	8
3.	***Раздел 3***	Тема 3	3	3			1	7
4.	***Раздел 3***	Тема 4	3	3			1	7
5.	***Раздел 3***	Тема 6	3	3			1	7
6.	***Раздел 4***	Тема 7	3	3			1	7
7.	***Раздел 4***	Тема 8	3	3			1	7
8.	***Раздел 4***	Тема 9	3	3			1	7
9.	***Раздел 4***	Тема 10	3	3			1	7
10.	***Раздел 4***	Тема 11	3	3			1	7
11	***Раздел 4***	Тема 12	3	3			1	7
12	***Раздел 4***	Тема 13	3	3			1	7
13	***Раздел 4***	Тема 14	3	3			1	7
14	***Раздел 5***	Тема 15	3	3			1	7
15	***Раздел 6***	Тема 16	3	3			1	7

6. Перечень семинарских, практических занятий и лабораторных работ

№ п/п	№ раздела и темы дисциплины (модуля)	Наименование семинаров, практических и лабораторных работ	Трудоемкость (час.)	Оценочные средства	Формируемые компетенции
1	**2**	**3**	**4**	**5**	**6**
1.	***Раздел 3***	Практич. Занятие№1	7	Тестовый контроль по теме	ОПК-7
2.	***Раздел 4***	Практич. Занятие№2	7	Тестовый контроль по теме	ОПК-7
3.	***Раздел 4***	Практич. Занятие№3	7	Тестовый контроль по теме	ПК-7
4.	***Раздел 4***	Практич. Занятие№4	7	Тестовый контроль по теме	ПК-14
5.	***Раздел 5***	Практич. Занятие№5	7	Тестовый контроль по теме	ПК-7

6.	***Раздел 6***	Лабораторная №6	9	Тестовый контроль по теме	ПК-7

6.1. План самостоятельной работы студентов

№ нед.	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
1-7	**1-6**	Подготовка к практич. работе №1	№1	Учебный сайт	8
8		Практическая работа №1.		Учебный сайт	
9		Подведение итогов по практич. работе №1. Работа над ошибками по контрольной работе №1.		Учебный сайт	
10-16	**7-16**	Подготовка итоговой экзаменационной работы	№2	Учебный сайт	8
17		Подготовка доклада с презентацией		Учебный сайт	
18		Подведение итогов		Учебный сайт	

6.2. Методические указания по организации самостоятельной работы студентов

Текущая самостоятельная работа по дисциплине «Технико-экономическое обоснование и управление проектами», направленная на углубление и закрепление знаний студента, на развитие практических умений, включает в себя следующие виды работ:

- работа с лекционным материалом;
- подготовка к практическим занятиям;
- выполнение индивидуальных проектов;
- подготовка к контрольным работам;
- подготовка к зачету.

Творческая проблемно-ориентированная самостоятельная работа по дисциплине «Технико-экономическое обоснование и управление проектами»,» направленная на развитие интеллектуальных умений, общекультурных и профессиональных компетенций, развитие творческого мышления у студентов, включает в себя следующие виды работ по основным проблемам курса:

- поиск, анализ, структурирование информации;
- выполнение графических работ, обработка и анализ данных;
- участие в конференциях, олимпиадах и конкурсах.

Оценка результатов самостоятельной работы организуется как единство двух форм: самоконтроль и контроль со стороны преподавателя.

Самоконтроль зависит от определенных качеств личности, ответственности за результаты своего обучения, заинтересованности в положительной оценке своего труда, материальных и моральных стимулов, от того насколько обучаемый мотивирован в достижении наилучших результатов. Задача преподавателя состоит в том, чтобы создать условия для выполнения самостоятельной работы (учебно-методическое обеспечение), правильно использовать различные стимулы для реализации этой работы (рейтинговая система), повышать её значимость, и грамотно осуществлять контроль самостоятельной деятельности студента (фонд оценочных средств).

7. Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) учебным планом не предусмотрены.

8. Учебно-методическое и информационное обеспечение дисциплины (модуля):

а) основная литература

1.Глухов Н.И., Крячко Е.Ю Документоведение: курс лекций. Иркутск: РИО ГУ НЦ РВХ ВСНЦ СО РАМН, 2005. – 156 с.

2.Яшин В.Н. Информатика. Аппаратные средства персонального компьютера. – М.: ИНФРА – М, 2008. – 254 с.

3.Бройдо, В. Л. Вычислительные системы, сети и телекоммуникации [Текст] : учеб. пособие / В. Л. Бройдо, О. П. Ильина. - 3-е изд. - СПб.: Питер, 2008. - 766 с..

в) программное обеспечение

Система тестирования и анализа аппаратной платформы ЭВМ.

г) базы данных, информационно-справочные и поисковые системы

1. Учебный сайт Лаборатории ТЗИ Физического факультета ИГУ - – Режим доступа: https://sites.google.com/view/ltzi/, свободный.

9. Материально-техническое обеспечение дисциплины (модуля)

Компьютерная лаборатория 323б (14 серверов) и лекционная аудитория 225, оснащенные мультимедийными средствами, электронной базой знаний, системой тестирования, выходом в глобальную сеть Интернет. Технические характеристики серверов обеспечивают возможность моделирования необходимого аппаратного обеспечения для работы с современными компьютерными системами хранения и обработки информации.

10. Образовательные технологии

Для достижения планируемых результатов обучения, в дисциплине ««Документоведение. Нормативные документы безопасности автоматизированных систем» используются различные образовательные технологии:

Информационно-развивающие технологии, направленные на формирование системы знаний, запоминание и свободное оперирование ими.

Используется лекционно-семинарский метод, самостоятельное изучение литературы, применение новых информационных технологий для самостоятельного пополнения знаний, включая использование технических и электронных средств информации.

Деятельностные практико-ориентированные технологии, направленные на формирование системы профессиональных практических умений при проведении экспериментальных исследований, обеспечивающих возможность качественно выполнять профессиональную деятельность.

Используется анализ, сравнение методов проведения химических исследований, выбор метода, в зависимости от объекта исследования в конкретной производственной ситуации и его практическая реализация.

Развивающие проблемно-ориентированные технологии, направленные на формирование и развитие проблемного мышления, мыслительной активности, способности видеть и формулировать проблемы, выбирать способы и средства для их решения. Используются виды проблемного обучения: освещение основных проблем общей и неорганической химии на лекциях, учебные дискуссии, коллективная деятельность в группах при выполнении лабораторных работ, решение задач повышенной сложности. При этом используются первые три уровня (из четырех) сложности и самостоятельности: проблемное изложение учебного материала преподавателем; создание преподавателем проблемных ситуаций, а обучаемые вместе с ним включаются в их разрешение;

преподаватель создает проблемную ситуацию, а разрешают её обучаемые в ходе самостоятельной деятельности.

Личностно-ориентированные технологии обучения, обеспечивающие в ходе учебного процесса учет различных способностей обучаемых, создание необходимых условий для развития их индивидуальных способностей, развитие активности личности в учебном процессе. Личностно-ориентированные технологии обучения реализуются в результате индивидуального общения преподавателя и студента при защите лабораторных работ, при выполнении домашних индивидуальных заданий, решении задач повышенной сложности, на еженедельных консультациях.

11. Оценочные средства (ОС):

11.1. Оценочные средства для входного контроля

Входной контроль (25 вариантов, 3-й семестр), представляет собой перечень из 10-15 вопросов и заданий. Входной контроль проводится в письменном виде на первом практическом занятии в течение 15 минут. Проверяется уровень входных знаний.

11.2. Оценочные средства текущего контроля

Вопросы к практическим занятиям (10 тем). Представляют собой перечень вопросов, проверяющих знание теоретического лекционного материала и тем, вынесенных на самостоятельную проработку.

11.3. Оценочные средства для промежуточной аттестации

(в форме зачета).

Тестовые работы (10 комплектов по 3-5 вариантов). Проверяется степень усвоения теоретических и практических знаний, приобретенных умений на репродуктивном и продуктивном уровне.

Контроль качества освоения студентами дисциплины осуществляется непрерывно в течение всего периода обучения с использованием балльно-рейтинговой системы (БРС). Индикатором сформированности компетенции является начисление студенту баллов за выполнение задания семинаров, контрольных работ в виде теста, получения премиальных баллов и /или выполнения итогового теста.

Тест

1. Выберите правильное определение термина «информация»:

а) совокупность содержащихся в базах данных сведений;

б) совокупность содержащихся в базах данных сведений, зафиксированных на машинных носителях;

в) сведения (сообщения, данные) воспроизводимые различными системами;

г) сведения (сообщения, данные) независимо от формы их представления.

2. Выберите правильное определение термина «обладатель информации»:

а) лицо, самостоятельно создавшее информацию;

б) лицо, получившее на основании закона или договора право разрешать или ограничивать доступ к информации;

в) лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

г) лицо, самостоятельно создавшее информацию либо получившее право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

3. Выберите правильное определение термина «предоставление информации»:

а) действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

б) действия, направленные на распространение сведений в средствах массовой информации;

в) действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

г) действия, направленные на получение информации как определённым, так и неопределённым кругом лиц или передачу информации как определенному, так и неопределённому кругу лиц.

4. Выберите правильное определение термина «защищаемые помещения»:

а) помещения, специально предназначенные для хранения носителей конфиденциальной информации;

б) помещения, специально предназначенные для размещения технических средств информационной системы;

в) помещения, специально предназначенные для хранения носителей конфиденциальной информации и размещения технических средств информационной системы;

г) помещения, специально предназначенные для проведения конфиденциальных мероприятий;

5. Выберите правильное определение термина «контролируемая зона»:

а) пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств;

б) часть здания, в котором исключено неконтролируемое пребывание посторонних лиц, транспортных, технических и иных материальных средств;

в) пространство (территория, здание, часть здания, помещение), в котором действует особый режим наблюдения за всеми сотрудниками организации;

г) помещение, в котором постоянно, независимо от окружающих факторов ведётся систематический контроль и надзор за действиями пользователей.

6. К рекомендуемым методам и способам защиты информации в информационных системах относятся (выберите все верные варианты ответов):

а) методы и способы защиты информации от несанкционированного доступа;

б) методы и способы сокрытия информации от внутренних нарушителей;

в) методы и способы устранения конкурентов;

г) методы и способы защиты информации от утечки по техническим каналам;

7. Средствами защиты информации, подлежащими сертификации, являются (выберите все верные варианты ответов):

а) строительные материалы, используемые для отделки помещений, в которых размещаются отдельные элементы АС;

б) детали интерьера, используемые для размещения АИС;

в) средства контроля эффективности применения средств защиты информации;

г) средства контроля эффективности прочности ограждений;

д) средства защиты информации (технические, программные, программно-аппаратные) от НСД, блокировки доступа и нарушения целостности.

8. Технические способы защиты информации в зависимости от используемых средств классифицируются как (выберите все верные варианты ответов):

а) полуактивные;

б) пассивные;

в) разноплановые;

г) удостоверяющие;

д) активные.

9. “Технический канал утечки информации” - это:

а) совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;

б) совокупность средств доступа к информации, нарушающих правила разграничения доступа с использованием штатных средств;

в) совокупность физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;

г) совокупность объекта технической разведки и средств, которыми добывается защищаемая информация.

10. Техническими каналами утечки информации являются (выберите все верные варианты ответов):

а) кражи технических средств информационной системы;

б) утечки акустической (речевой) информации;

в) утечки информации, реализуемые через общедоступные информационные сети;

г) утечки видовой информации;

д) утечки информации по каналам побочных электромагнитных излучений;

е) утечки информации, реализуемые через интернет;

11. «Несанкционированный доступ к информации» - это:

а) доступ, реализующий возможности совокупности физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;

б) доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств;

в) доступ с использованием совокупности средств технической разведки и прочих средств, которыми добывается защищаемая информация;

г) доступ к информации, реализуемый путём уничтожения технических средств информационной системы.

12. «Персональный идентификатор» — это

а) устройство для хранения зашифрованной информации пользователя;

б) устройство для хранения информации, необходимой при идентификации и аутентификации пользователя;

в) устройство для хранения журнала аудита.

13. Механизм контроля целостности СЗИ Secret Net предназначен для

а) формирония цифровых отпечатков данных;

б) контроля информационных потоков;

в) слежения за неизменностью содержимого ресурсов компьютера.

14. Механизм замкнутой программной среды СЗИ Secret Net и Dallas Lock предназначен для

а) ограничения использования программного обеспечения на компьютере;

б) установки ограниченного количества программ;

в) сбора сведений об используемых приложениях.

15. В СЗИ Secret Net пользователю с уровнем допуска "конфиденциально" разрешается выполнять чтение файлов с категориями

а) «конфиденциально»;

б) «секретно»;

в) «строго конфиденциально»,

г) «неконфиденциально».

16. Длина ключа шифрования алгоритма ГОСТ 28147-89 равна

а) 56 бит;

б) 256 бит;

в) 1024 бит;

г) 128 бит.

17. К какому типу криптосистем относится алгоритм AES?

а) несимметричные;

б) асиммеричные;

в) симметричные;

г) полусимметричные.

18. Пассивными способами защиты информации являются:

а) создание маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях технических средств;

б) ослабление наводок ПЭМИ в посторонних проводниках и соединительных линиях технических средств, выходящих за пределы контролируемой зоны;

в) создание маскирующих электромагнитных помех в цепях заземления;

г) выставление постов охраны у помещений, в которых размещаются технические средства обработки информации.

19. Межсетевой экран служит для:

а) разграничения доступа в помещения АИС;

б) фильтрации трафика при передачи данных;

в) защиты от утечек информации путем экранирования стен;

г) контроля целостности программного обеспечения.

20. Максимально возможное количество категорий конфиденциальности в СЗИ Secret Net 7.x равно _____ (16).

21. В СЗИ Secret Net категорию конфиденциальности можно назначить для следующих ресурсов: каталоги и файлы на дисках с файловой системой _____ (NTFS).

22. Практическая стойкость алгоритма RSA основана на сложности решения задачи _____ (факторизации).

23. Практическая стойкость алгоритма Диффи-Хеллмана основана на сложности решения задачи нахождения дискретного_____ (логарифма).

24. Эффективным средством защиты от утечки информации из АИС показали себя _____ (DLP) – системы.

25. Хэш-функции предназначены, главным образом, для контроля _____(целостности) данных.

26. Технология электронной подписи разработана с целью подтверждения _____ (авторства) и _____ (подлинности) сообщений.

27. Длина хэш-кода алгоритма MD5 составляет _____ (128) бит.

28. Как в СЗИ Secret Net происходит включение режима хранения пароля в идентифика торе?

(Основной тезис: происходит добавление в базу данных Secret Net сведений о включении для пользователя режима хранения пароля в идентификаторе. Одновременно с этой операцией выполняется запись пароля в идентификатор. После включения режима

пароль пользователя при входе в систему не вводится с клавиатуры, а считывается из идентификатора).

29. Каким образом в СЗИ Secret Net происходит присвоение пользователю персонального идентификатора?

(Основной тезис: происходит добавление в базу данных Secret Net сведений о том, что пользователю принадлежит персональный идентификатор данного типа с уникальным серийным номером).

30. Каким образом в СЗИ Secret Net реализуется затирание файлов?

(Основной тезис: при действии механизма затирания в область диска, где физически было расположено содержимое удаленного файла, записывается последовательность случайных чисел).

31. Что происходит при выборе способа очистки журнала СЗИ Secret Net при его переполнении «Затирать события по мере необходимости»?

(Основной тезис: при переполнении журнала система защиты автоматически удаляет из журнала необходимое количество самых старых записей).

32. Каким образом в СЗИ Secret Net реализуется настройка дискреционного разграничения доступа к файлам и папкам?

(Основной тезис: настройка дискреционного разграничения доступа к файлам и папкам производится штатными средствами операционной системы).

33. Кратко описать назначение и функции Удостоверяющего Центра в системе PCI.

Назначение оценочных средств текущего контроля – выявить сформированность компетенций (ОПК-5). Ниже приведен перечень оценочных средств текущего контроля:

1. Семинарские задания. Назначение оценочного средства – мониторинг эффективности подготовки студентов в ходе обучения. Показателем эффективности подготовки студента является получение им балла, превышающего пороговое значение в 3 балла за выполнение и усвоение одного семинарского задания. В семестре предполагается выполнение 14 семинаров. Суммарно для допуска к зачету студент должен получить за уяснение вопросов семинаров не менее 42 бала.

Параметры оценочного средства

Критерии оценки	Оценка		
	Отлично	Хорошо	Удовлетв.
Выполнение заданий	Полностью и корректно выполнены все задания **(9-10 баллов)**	Полностью выполнены все задания, допущены одна – две ошибки **(7 -8 баллов)**	Не полностью выполнены задания, допущены одна – две ошибки **(5 -6 балла)**

Промежуточная аттестация проводится в форме защиты реферата. Студент допускается к итоговой аттестации - экзамену в том случае, если он защитит реферат, выполнит все семинарские задания и получит более 42 баллов, а также сдаст на положительную оценку контрольные работы в виде тестов. Если студент набрал необходимое количество баллов, предлагается итоговый тест – экзамен.

В случае если студент не набрал пороговое значение баллов, ему предлагается пройти итоговое тестирование по тем разделам, которые остались не изучены (пропущены, не сданы на положительную оценку). Характеристики итогового теста сходны с характеристиками тестов для контрольны аттесх работ.

Объем теста –33 вопроса.

Параметры оценочного средства

Предел длительности контроля	45 мин
Последовательность выборки вопросов из разделов (по всему курсу дисциплины)	случайная
Критерии оценки:	
«5», если	45 – 50 правильных ответов (добавляется 17 - 20 баллов в рейтинг студента)
«4», если	39 - 44 правильный ответ (добавляется 13 - 16 баллов в рейтинг студента)
«3», если	33 - 38 правильных ответов (добавляется 10 - 12 баллов в рейтинг студента)

Итоговый рейтинг студента формируется следующим образом:

№ п/п	Вид учебной деятельности	баллы	Максимально за 1 семестр
1.	Ведение конспекта лекций (за лекцию)	0.5	9
2	Выполнение семинарских заданий (см. перечень заданий в прил. 1)	2	28
3	Премиальные баллы за интерес к изучению курса (за семестр):	10	10
	Экзамен в сессию	8	8

доцент Н.И.Глухов

Программа рассмотрена на заседании кафедры радиофизики и радиоэлектроники «20» марта 2020 г.

Протокол № 8 И.О.Зав. кафедрой Колесник С.Н.