ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Высшая школа электроники и компьютерных наук

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Голлай А. В.
Пользователь: gollaiav
Дата подписания: 16.09.2021

А. В. Голлай

РАБОЧАЯ ПРОГРАММА

дисциплины В.1.09 Обеспечение информационной безопасности на критически важных объектах
для специальности 10.05.03 Информационная безопасность автоматизированных систем
уровень специалист **тип программы** Специалитет
специализация Информационная безопасность автоматизированных систем критически важных объектов
форма обучения очная
кафедра-разработчик Защита информации

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 01.12.2016 № 1509

Зав.кафедрой разработчика,
к.техн.н., доц.

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Соколов А. Н.
Пользователь: sokolovan
Дата подписания: 16.09.2021

А. Н. Соколов

Разработчик программы,
старший преподаватель

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Антясов И. С.
Пользователь: antiasovis
Дата подписания: 16.09.2021

И. С. Антясов

Челябинск

1. Цели и задачи дисциплины

Целью преподавания дисциплины является знакомство студентов с принципами, особенностями и способами обеспечения информационной безопасности всего жизненного цикла на критически важных объектах. Задачами дисциплины являются: - изучение системы государственного контроля в области обеспечения информационной безопасности на критически важных объектах и системы признаков критически важных объектов; - обучение принципам анализа с целью выявления потенциальных уязвимостей информационной безопасности на критически важных объектах; - выработка умений классифицировать и оценивать угрозы информационной безопасности для критически важных объектов, эффективно использовать различные методы и средства защиты информации; - изучение основных средств и способов обеспечения информационной безопасности на критически важных объектах, принципов построения систем защиты информации.

Краткое содержание дисциплины

Дисциплина «Обеспечение информационной безопасности на критически важных объектах» является неотъемлемой составной частью профессиональной подготовки специалистов по специальности 090303 «Информационная безопасность автоматизированных систем», специализации «Информационная безопасность автоматизированных систем критически важных объектов». Вместе с другими дисциплинами специального цикла изучение данной дисциплины призвано формировать специалиста и, в частности, вырабатывать у него такие качества, как способностью к логическому мышлению, обобщению, анализу, критическому осмыслению и систематизации информации, а также способность самостоятельно применять методы и средства познания, обучения и самоконтроля для приобретения новых знаний и умений.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине (ЗУНы)
ПК-11 способностью разрабатывать политику информационной безопасности автоматизированной системы	Знать:существующие принципы, политики и процедуры безопасности в области защиты информации;
	Уметь:
	Владеть:навыками формирования политик безопасности для критически важных объектов и автоматизированных систем критически важных объектов;
ПСК-3.4 способностью разрабатывать технические регламенты для различных видов деятельности по обеспечению информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов	Знать:подходы к построению систем защиты информации на критически важных объектах;
	Уметь:разрабатывать предложения по совершенствованию и повышению эффективности применения мер информационной безопасности на критически важных объектах;

	Владеть:терминологией и системным подходом обеспечения информационной безопасности на критически важных объектах;
ПСК-3.2 способностью участвовать в разработке, осуществлять внедрение и эксплуатацию средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов	Знать:средства защиты информации, используемые на критически важных объектах;
	Уметь:формулировать основные требования к методам и средствам защиты информации на критически важных объектах;
	Владеть:
ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	Знать:способы выявления угроз информационной безопасности на критически важных объектах;
	Уметь:применять принципы конфиденциальности, целостности и доступности информации;
	Владеть:навыками анализа угроз и уязвимостей информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов;
ПСК-3.3 способностью применять современную нормативную базу, регламентирующую деятельность критически важных объектов и обеспечение информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов	Знать:классы и характеристики критически важных объектов; понятия и определения, на которых базируются решения проблем информационной безопасности; нормативно-методические и руководящие документы, регламентирующие обеспечение информационной безопасности критически важных объектов;
	Уметь:реализовывать с учетом особенностей функционирования критически важных объектов требования нормативно-методической и руководящей документации, а также действующего законодательства по вопросам защиты информации ограниченного доступа;
	Владеть:навыками работы с нормативными правовыми актами в области технической защиты информации ограниченного доступа на предприятии (в организации, учреждении);

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
В.1.07 Инженерно-техническая защита информации и технические средства охраны на критически важных объектах, В.1.08 Основы аттестации объектов информатизации критически важных объектов	Не предусмотрены

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования

В.1.07 Инженерно-техническая защита информации и технические средства охраны на критически важных объектах	Знать технические каналы утечки информации. Уметь определять разведопасные направления. Обладать навыками применения технических средств защиты информации.
В.1.08 Основы аттестации объектов информатизации критически важных объектов	Знать основные положения по аттестации объектов информатизации. Уметь анализировать достаточность принятых мер по защите информации. Обладать навыками подготовки заключения по эффективности принятых мер по защите информации

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 4 з.е., 144 ч.

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		10
Общая трудоёмкость дисциплины	144	144
Аудиторные занятия:	72	72
Лекции (Л)	36	36
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	36	36
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	72	72
Проработка лекционного материала	36	36
Выполнение заданий поисково – исследовательского характера	36	36
Вид итогового контроля (зачет, диф.зачет, экзамен)	-	экзамен

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Объекты критической информационной инфраструктуры РФ	6	6	0	0
2	Порядок категорирования объектов критической информационной инфраструктуры	22	8	14	0
3	Особенности обеспечения информационной безопасности для всего жизненного цикла объектов критической информационной инфраструктуры.	20	8	12	0
4	Организационно-технические и режимные меры информационной безопасности на объектах критической информационной инфраструктуры.	16	8	8	0
5	Средства защиты информации, использующиеся на значимых объектах и оценка их эффективности.	6	4	2	0
6	Государственный контроль и надзор в области обеспечения информационной безопасности на значимых объектах.	2	2	0	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Основные направления государственной политики в области обеспечения безопасности критически важных объектов инфраструктуры Российской Федерации	4
2	1	Организационные основы обеспечения информационной безопасности критической информационной инфраструктуры.	2
3	2	Общий порядок категорирования. Виды категорий значимости	2
4	2	Перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значения	2
5	2	Права и обязанности субъектов критической информационной инфраструктуры	2
6	2	Порядок взаимодействия с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры	2
7	3	Стадии жизненного цикла безопасности объектов критической информационной инфраструктуры в целом	2
8	3	Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры и обеспечению их функционирования .	2
9	3	Анализ угроз безопасности информации и разработка модели угроз безопасности информации	4
10	4	Планирование и разработка мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры	2
11	4	Силы обеспечения безопасности значимых объектов	1
12	4	Установление требований к обеспечению безопасности значимого объекта	3
13	4	Политики информационной безопасности критически важных объектов	2
14	5	Средства защиты информации, использующиеся на значимых объектах и оценка их эффективности.	2
15	5	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации	2
16	6	Контроль мер обеспечения информационной безопасности на значимых объектах.	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	2	Определение принадлежности организации к субъектам критической информационной инфраструктуры	2
2	2	Определение критических процессов, нарушение и/или прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка	2
3	2	Формирование сводного перечня объектов критической информационной инфраструктуры в организации	2
4	2	Формирование исходных данных на каждый объект критической информационной инфраструктуры	4
5	2	Категорирование объектов критической информационной инфраструктуры в	4

		соответствии с перечнем показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений	
6	3	Рассмотрение возможных действий нарушителей, иных источников угроз безопасности. Анализ угроз и уязвимостей. Подготовка модели угроз.	6
7	3	Подготовка формы направления сведений о результатах присвоения объекту одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий	4
8	3	Разработка требований к оформлению концепции для всего жизненного цикла обеспечения информационной безопасности объекта.	2
9	4	Составление плана мероприятий по обеспечению безопасности на значимом объекте	2
10	4	Разработка организационно-распорядительных документов по безопасности значимых объектов критической информационной инфраструктуры	4
11	4	Обеспечение безопасности значимого объекта в ходе его эксплуатации	2
12	5	Выбор средств защиты информации	2

5.3. Лабораторные работы

Не предусмотрены

5.4. Самостоятельная работа студента

Выполнение СРС		
Вид работы и содержание задания	Список литературы (с указанием разделов, глав, страниц)	Кол-во часов
Проработка лекционного материала	приложенный конспект лекций	36
Выполнение заданий поисково – исследовательского характера	Изучение современных нормативных правовых актов в области обеспечения безопасности критической информационной инфраструктуры. Справочно-поисковая система "Гарант"	36

6. Инновационные образовательные технологии, используемые в учебном процессе

Инновационные формы учебных занятий	Вид работы (Л, ПЗ, ЛР)	Краткое описание	Кол-во ауд. часов
Использование проблемно-ориентированного междисциплинарного подхода к изучению наук	Лекции	Тема «Рассмотрение возможных действий нарушителей, иных источников угроз безопасности. Анализ угроз и уязвимостей. Подготовка модели угроз.» в разделе 3	6
Компьютерная симуляция	Практические занятия и семинары	Средства защиты информации, использующиеся на значимых объектах и оценка их эффективности.	4
Использование методов, основанных на изучении практики	Лекции	Тема лекции в разделе 3 «Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры и обеспечению их функционирования»	2

Собственные инновационные способы и методы, используемые в образовательном процессе

Не предусмотрены

Использование результатов научных исследований, проводимых университетом, в рамках данной дисциплины: нет

7. Фонд оценочных средств (ФОС) для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

7.1. Паспорт фонда оценочных средств

Наименование разделов дисциплины	Контролируемая компетенция ЗУНы	Вид контроля (включая текущий)	№№ заданий
Все разделы	ПК-11 способностью разрабатывать политику информационной безопасности автоматизированной системы	экзамен	11-14
Все разделы	ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	экзамен	9-10
Все разделы	ПСК-3.3 способностью применять современную нормативную базу, регламентирующую деятельность критически важных объектов и обеспечение информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов	практическое задание	1-20
Все разделы	ПСК-3.2 способностью участвовать в разработке, осуществлять внедрение и эксплуатацию средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов	бонусное задание	6-8
Средства защиты информации, использующиеся на значимых объектах и оценка их эффективности.	ПСК-3.4 способностью разрабатывать технические регламенты для различных видов деятельности по обеспечению информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов	экзамен	15-18
Все разделы	ПСК-3.3 способностью применять современную нормативную базу, регламентирующую деятельность критически важных объектов и обеспечение информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов	экзамен	1-5
Все разделы	ПСК-3.3 способностью применять современную нормативную базу, регламентирующую деятельность критически важных объектов и обеспечение информационной безопасности критически важных объектов и автоматизированных	посещаемость	1-18

	систем критически важных объектов		

7.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
экзамен	На экзамене происходит оценивание учебной деятельности обучающихся по дисциплине с учетом полученных оценок за посещаемость и выполнение практического задания. При оценивании результатов учебной деятельности обучающегося по дисциплине используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Показателями при проведении экзамена являются следующие: 1. Студенты в аудитории письменно отвечают на вопросы экзаменационного билета, который включает 2 теоретических вопроса по пройденным разделам, преподаватель проверяет, беседует и оценивает. Показатели оценивания ответов по каждому из вопросов: 5-6 баллов – студент обладает твёрдым и полным знанием материала дисциплины, владеет дополнительными знаниями даны полные, развёрнутые ответы; логически, грамотно и точно излагает материал дисциплины, интерпретируя его самостоятельно, способен самостоятельно его анализировать и делать выводы; 3-4 балла – студент знает материал дисциплины в запланированном объёме, некоторые моменты в ответе не отражены или в ответе имеются несущественные неточности; грамотно и по существу излагает материал. 1-2 балла – студент знает только основной материал дисциплины, не усвоил его деталей, дана только часть ответа на вопросы; в ответе имеются существенные ошибки; допускает неточности в изложении и интерпретации знаний; имеются нарушения логической последовательности 0 баллов – студент не знает значительной части материала дисциплины; ответ не дан или допускает грубые ошибки при изложении ответа на вопрос; неверно излагает и интерпретирует знания; изложение материала логически не выстроено. Максимальное число баллов - 12. 2. Максимальное число баллов за выполнение практического задания - 9.	Отлично: величина рейтинга обучающегося по дисциплине 85…100 % Хорошо: величина рейтинга обучающегося по дисциплине 75…84 % Удовлетворительно: величина рейтинга обучающегося по дисциплине 60…74 % Неудовлетворительно: величина рейтинга обучающегося по дисциплине 0…59 %. Если рейтинг обучающегося по дисциплине ниже 60%, то он сдает экзамен с целью возможного повышения рейтинга. По результатам сдачи экзамена выставляется оценка, которая учитывается при определении рейтинга.

	3.Максимально число баллов за посещаемость - 9. Максимальная оценка, которую может получить студент при выполнении всех заданий, составляет 30 баллов.	
бонусное задание	Студент представляет копии документов, подтверждающие победу или участие в конференции. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Максимально возможная величина бонус-рейтинга +15 %.	Зачтено: 15 % за победу в конференции международного уровня +10 % за победу в конференции российского уровня +5 % за победу в конференции университетского уровня +1 % за участие в конференции. Не зачтено: Не предусматривается
практическое задание	Защита практической работы осуществляется в форме доклада на практическом занятии с презентацией и сдачей подготовленного отчета. На защите студент коротко (5-7 мин.) докладывает об основных результатах выполнения практического задания и отвечает на вопросы. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Показатели оценивания: Соответствие заданию: 3 балла – полное соответствие заданию; 2 балла – в целом соответствие заданию, за исключением отдельных не принципиальных аспектов; 1 балл – не полное соответствие заданию; 0 баллов – не соответствие заданию; Качество оформления практической работы: 3 балла – работа имеет логичное, последовательное изложение материала с соответствующими выводами и обоснованными положениями; 2 балла – работа имеет грамотно изложенную теоретическую главу, в ней представлены достаточно подробный анализ и критический разбор практической деятельности, последовательное изложение материала с соответствующими выводами, однако с не вполне обоснованными положениями; 1 балл – работа имеет теоретическую главу, базируется на практическом материале, но имеет поверхностный анализ, в ней просматривается непоследовательность изложения материала, представлены необоснованные положения; 0 балл – пояснительная записка не содержит анализа, в работе нет выводов либо они	Зачтено: Рейтинг обучающегося за мероприятие больше или равен 60 %. Не зачтено: Величина рейтинга обучающегося по дисциплине 0…59 %

	носят декларативный характер. Защита практической работы: 3 балла – при защите студент показывает глубокое знание вопросов темы, свободно оперирует данными исследования, вносит обоснованные предложения, легко отвечает на поставленные вопросы; 2 балла – при защите студент показывает знание вопросов темы, оперирует данными исследования, вносит предложения по теме исследования, без особых затруднений отвечает на поставленные вопросы; 1 балл – при защите студент проявляет неуверенность, показывает слабое знание вопросов темы, не всегда дает исчерпывающие аргументированные ответы на заданные вопросы; 0 баллов – при защите студент затрудняется отвечать на поставленные вопросы по теме, не знает теории вопроса, при ответе допускает существенные ошибки. Максимальное количество баллов – 9.	
посещаемость	Отмечается присутствие студента на занятиях. За каждое посещение прибавляется 0,25 балла. Максимальное количество баллов за семестр равно 9	Зачтено: рейтинг обучающегося за мероприятие больше или равен 60 %. Не зачтено: рейтинг обучающегося за мероприятие менее 60 %

7.3. Типовые контрольные задания

Вид контроля	Типовые контрольные задания
экзамен	БИЛЕТЫ КИИ 2020.docx
бонусное задание	
практическое задание	методические указания к практическим работам.docx
посещаемость	

8. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

Не предусмотрена

б) дополнительная литература:

Не предусмотрена

в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:

1. Открытые системы. СУБД: информ.-аналит. журн. / учредитель ЗАО "Изд-во "Открытые системы". – 1996- .-М.: Издательство "Открытые системы", 1996- .-Ежемес.

г) методические указания для студентов по освоению дисциплины:

1. методические указания к практическим работам
2. Прохоров, А. В.Основы защиты информации [Текст] : метод. указания к практ. занятиям / А. В. Прохоров, С. В. Денисов ; Юж.-Урал. гос. ун-т, Озерск. фил., Каф. Информатика ; ЮУрГУ. – Челябинск : Издательский Центр ЮУрГУ, 2012. – 38 с.:ил.
3. Конспект лекций

из них: учебно-методическое обеспечение самостоятельной работы студента:

Электронная учебно-методическая документация

№	Вид литературы	Наименование разработки	Наименование ресурса в электронной форме	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
1	Основная литература	Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс] — Электрон. дан. — М. : Горячая линия-Телеком, 2017. — 338 с. — Режим доступа: http://e.lanbook.com/book/111049 — Загл. с экрана.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
2	Дополнительная литература	Технические средства и методы защиты информации. [Электронный ресурс] : учеб. пособие / А.П. Зайцев [и др.]. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 616 с. — Режим доступа: http://e.lanbook.com/book/5154 — Загл. с экрана.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
3	Дополнительная литература	Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам. [Электронный ресурс] — Электрон. дан. — М. : Горячая линия-Телеком, 2015. — 586 с. — Режим доступа: http://e.lanbook.com/book/94555 — Загл. с экрана.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
4	Основная литература	Нормативные правовые акты в области обеспечения безопасности критической информационной инфраструктуры	Гарант	Интернет / Авторизованный
5	Основная литература	Криулин, А. А. Основы безопасности прикладных информационных технологий и систем : учебное пособие / А. А. Криулин, В. С. Нефедов, С. И. Смирнов. — Москва : РТУ МИРЭА, 2020. — 136 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167606 (дата обращения: 16.09.2021). — Режим доступа: для авториз. пользователей.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
6	Основная	Алѐшкин, А. С. Аппаратные и программные	Электронно-	Интернет /

	литература	средства поиска уязвимостей при моделировании и эксплуатации информационных систем (обеспечение информационной безопасности) : учебное пособие / А. С. Алѐшкин, С. А. Лесько, Д. О. Жуков. — Москва : РТУ МИРЭА, 2020. — 152 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167600 (дата обращения: 16.09.2021). — Режим доступа: для авториз. пользователей.	библиотечная система издательства Лань	Авторизованный

9. Информационные технологии, используемые при осуществлении образовательного процесса

Перечень используемого программного обеспечения:

Нет

Перечень используемых информационных справочных систем:

Нет

10. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Лекции	912 (3б)	Комплект компьютерного оборудования, LCD Проектор, Экран проекционный, настенные стенды по защите информации (5 шт.), программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+.
Практические занятия и семинары	910 (3б)	Комплект компьютерного оборудования, Стенд по методам и средствам защиты телефонных аппаратов и телефонных линий, Стенд по биометрическим способам индикации, Стенд по противопожарной защите, Стенд по системам аналогового видеонаблюдения, Стенд по системам цифрового видеонаблюдения, Стенд по техническим средствам охраны на базе приборов «Сигнал 20» и «Сигнал 20 П», Стенд по техническим средствам охраны на базе контроллера «С200-КФЛ», Переносной комплекс для измерений «Навигатор П3Г», Комплекс контроля эффективности защиты речевой информации «Спрут-мини-А», Лабораторный стенд для исследования линий связи, Селективный микровольтметр, Осциллограф С1-65, Генератор импульсов Г5-54, Аппаратный шифратор, Поисковый комплекс «Пиранья», Нелинейный локатор «Родник-2К», Детектор поля, Устройство комбинированной защиты, настенные информационные стенды (3 шт.), программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Орион, VidioNET.