МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Забайкальский государственный университет»
(ФГБОУ ВО «ЗабГУ»)

Энергетический факультет

Кафедра Физики и техники связи

УТВЕРЖДАЮ:

Декан факультета

Мирошников С.Ф.

«____»_____20____г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.Б.35.06.Программно-аппаратные средства обеспечения информационной безопасности (в исполнительных органах государственной власти)

на 144 часа(ов), 4 зачетных(ые) единиц(ы)

для направления подготовки (специальности) 10.05.02 – Информационная безопасность телекоммуникационных систем

составлена в соответствии с ФГОС ВО, утвержденным приказом Министерства образования и науки Российской Федерации от «___» _____ 20____ г. №_____

Специализация – Защита информации в системах связи и управления (для набора 2020)

Форма обучения очная

1. Организационно-методический раздел

1.1 Цель и задачи дисциплины (модуля)

Цель изучения дисциплины:

Целями освоения дисциплины «Программно-аппаратные средства обеспечения информационной безопасности (в исполнительных органах государственной власти)» являются обучение студентов системному подходу к обеспечению защиты информации в комплексных системах связи и телекоммуникации.

Задачи изучения дисциплины:

В результате изучения дисциплины студент должен освоить следующие компетенции:
владеть культурой мышления, способностью к восприятию информации, постановке цели и выбору путей ее достижения (ОК-1);
уметь аргументированно и ясно строить устную и письменную речь (ОК-2);
способностью находить решения в нестандартных ситуациях и готовностью нести за них ответственность (ОК-4);
использовать основные законы естественнонаучных дисциплин в профессиональной деятельности, применять методы математического анализа и моделирования, теоретического и экспериментального исследования (ОК-9);
способностью понимать значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны; владеть основными методами, способами и средствами получения, хранения, переработки информации (ПК-1);
иметь навыки самостоятельной работы на компьютере и в компьютерных сетях;
осуществлять компьютерное моделирование устройств, систем и процессов с использованием универсальных пакетов прикладных компьютерных программ (ПК-2);
уметь составлять нормативную документацию (инструкции) по эксплуатационно-техническому обслуживанию сооружений, сетей и оборудования связи, по программам испытаний (ПК-9);
готовностью изучать научно-техническую информацию, отечественный и зарубежный опыт по тематике исследования (ПК-16);

1.2. Место дисциплины (модуля) в структуре ОП

Учебная дисциплина "Программно-аппаратные средства обеспечения информационной безопасности (в исполнительных органах государственной власти)" является обязательной дисциплиной

1.3. Объем дисциплины (модуля) с указанием трудоемкости всех видов учебной работы

Общая трудоемкость дисциплины (модуля) составляет 4 зачетных(ые) единиц(ы), 144 часов.

Очная форма

Виды занятий	Распределение по семестрам	Всего часов
	10 семестр	
Общая трудоемкость		144
Аудиторные занятия, в т.ч.	64	64
лекционные (ЛК)	32	32

практические (семинарские) (ПЗ, СЗ)	16	16
лабораторные (ЛР)	16	16
Самостоятельная работа студентов (СРС)	44	44
Форма промежуточной аттестации в семестре	Зачет	0
Курсовая работа (курсовой проект) (КР, КП)	КП	

2. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Индекс компетенции	Содержание компетенции
ПК-1	Способность осуществлять анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем
ПК-6	Способность применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду
ПСК-10.3	Способность оценивать возможности средств технических разведок в отношении к системам связи, управления и объектами информатизации
ПСК-10.4	Способность применять наиболее эффективные методы и средства для закрытия возможных каналов перехвата акустической речевой информации

Планируемые результаты обучения по дисциплине для последовательного достижения уровней сформированности компетенций

Результат обучения

Знать	Пороговый: : общие проблемы безопасности, роль и место информационной безопасности на современном этапе развития общества; основные методы инженерно-технической, программно-аппаратной и криптографической защиты информации; способы несанкционированного доступа к информации и средства инженерной защиты и технической охраны объектов
	Стандартный: применять системный подход к обеспечению информационной безопасности систем связи и инфокоммуникационных систем; разрабатывать модели информационной безопасности телекоммуникационных систем, использовать стандартные методы инженерно-технической, программно-аппаратной и криптографической защиты информации; практически решать задачи защиты инженерно-технической, программно-аппаратной и криптографической защиты программ и данных
	Эталонный: анализа механизмов реализации методов защиты конкретных объектов и процессов для решения профессиональных задач; применения штатные средств защиты и специализированных продукты для решения типовых задач; квалифицированно оценивать область применения конкретных механизмов защиты; грамотно использовать аппаратные средства защиты при решении практических задач.
	Пороговый: общие проблемы безопасности, роль и место информационной безопасности на современном этапе развития общества; основные методы инженерно-технической, программно-аппаратной и криптографической защиты информации; способы несанкционированного доступа к информации и средства инженерной защиты и технической охраны объектов

Уметь	Стандартный: применять системный подход к обеспечению информационной безопасности систем связи и инфокоммуникационных систем; разрабатывать модели информационной безопасности телекоммуникационных систем, использовать стандартные методы инженерно-технической, программно-аппаратной и криптографической защиты информации; практически решать задачи защиты инженерно-технической, программно-аппаратной и криптографической защиты программ и данных
	Эталонный: анализа механизмов реализации методов защиты конкретных объектов и процессов для решения профессиональных задач; применения штатные средств защиты и специализированных продукты для решения типовых задач; квалифицированно оценивать область применения конкретных механизмов защиты; грамотно использовать аппаратные средства защиты при решении практических задач.
Владеть	Пороговый: общие проблемы безопасности, роль и место информационной безопасности на современном этапе развития общества; основные методы инженерно-технической, программно-аппаратной и криптографической защиты информации; способы несанкционированного доступа к информации и средства инженерной защиты и технической охраны объектов
	Стандартный: применять системный подход к обеспечению информационной безопасности систем связи и инфокоммуникационных систем; разрабатывать модели информационной безопасности телекоммуникационных систем, использовать стандартные методы инженерно-технической, программно-аппаратной и криптографической защиты информации; практически решать задачи защиты инженерно-технической, программно-аппаратной и криптографической защиты программ и данных

	Эталонный: анализа механизмов реализации методов защиты конкретных объектов и процессов для решения профессиональных задач; применения штатные средств защиты и специализированных продукты для решения типовых задач; квалифицированно оценивать область применения конкретных механизмов защиты; грамотно использовать аппаратные средства защиты при решении практических задач.

3. Содержание дисциплины

3.1. Разделы дисциплины и виды занятий

Очная форма

Модуль	Номер раздела	Наименование раздела	Всего часов	Аудиторные занятия			СРС
				ЛК	ПЗ(СЗ)	ЛР	
1	1	Разграничение доступа к ресурсам	11	3	4	0	4
	2	Разграничение доступа к ресурсам	8	3	0	0	5
	3	Разграничение доступа к ресурсам	13	4	0	4	5
2	1	Регистрация событий	13	4	4	0	5
	2	Регистрация событий	13	4	0	4	5
	3	Регистрация событий	12	3	4	0	5
3	1	Организация защищённого документооборота	12	3	0	4	5
	2	Организация защищённого документооборота	13	4	4	0	5
	3	Организация защищённого документооборота	13	4	0	4	5
Итого			108	32	16	16	44

3.2. Лекционные занятия

Очная форма

Модуль	Номер раздела	Содержание лекционных занятий

1	1	Разграничение доступа на основе атрибутов (англ. Attribute-Based Access Control, ABAC) — модель контроля доступа к объектам, основанная на анализе правил для атрибутов объектов или субъектов, возможных операций с ними и окружения, соответствующего запросу[1]. Системы управления доступом на основе атрибутов обеспечивают мандатное и избирательное управление доступом. Рассматриваемый вид разграничения доступа даёт возможность создать огромное количество комбинаций условий для выражения различных политик[
	2	Для упрощения администрирования учетных записей пользователя назначить привилегии следует в первую очередь учетным записям группы, а не отдельным учетным записям пользователя. При назначении привилегий учетной записи групп пользователи автоматически получают эти привилегии, когда становятся членами этой группы.
	3	Делегирование объектов Active Directory
2	1	При использовании Windows Server 2003 аудит, можно отслеживать действия пользователя и действия Windows Server 2003, которые называются событиями на компьютере. При использовании аудита, можно указать, какие события записываются в журнал безопасности. Например в журнал безопасности можно вести запись допустимы и неверных попыток входа и события, связанные с создание, открытие или удаление файлов и других объектов
	2	Audit Collection Services (ACS) предоставляет средства для сбора записей, созданных с помощью политики аудита и их хранения в централизованной базе данных. Используя ACS, организации могут консолидировать отдельные журналы безопасности в централизованно управляемой базе данных и могут фильтровать и анализировать события с помощью инструментов, предоставляемых Microsoft SQL Server
	3	При использовании Wndows Server 2003 аудит, можно отслеживать действия пользователя и действия Windows Server 2003, которые называются событиями на компьютере. При использовании аудита, можно указать, какие события записываются в журнал безопасности. Например в журнал безопасности можно вести запись допустимы и неверных попыток входа и события, связанные с создание, открытие или удаление файлов и других объектов

3	1	Организация работы с документами: организация документооборота, хранения и использования документов в текущей деятельности учреждения 1. Из определения видно, что одной из составляющих организации работы с документами является документооборот
	2	ISO3 — Ряды номиналов радио деталей. ISO4 — система сокращения названий периодических изданий (журналов). ISO5 — Фотографии и графические технологии — измерения плотности. ISO6 — Светочувствительность фотоматериалов. ISO7 — Трубная резьба
	3	ЭЦП и юридическая значимость электронного документа

3.3. Практические (семинарские) занятия

Очная форма

Модуль	Номер раздела	Содержание практических(семинарских) занятий
1	1	Разграничение доступа на основе атрибутов (англ. Attribute-Based Access Control, ABAC) — модель контроля доступа к объектам, основанная на анализе правил для атрибутов объектов или субъектов, возможных операций с ними и окружения, соответствующего запросу[1]. Системы управления доступом на основе атрибутов обеспечивают мандатное и избирательное управление доступом. Рассматриваемый вид разграничения доступа даёт возможность создать огромное количество комбинаций условий для выражения различных политик[
2	1	При использовании Windows Server 2003 аудит, можно отслеживать действия пользователя и действия Windows Server 2003, которые называются событиями на компьютере. При использовании аудита, можно указать, какие события записываются в журнал безопасности. Например в журнал безопасности можно вести запись допустимы и неверных попыток входа и события, связанные с создание, открытие или удаление файлов и других объектов
	3	При использовании Windows Server 2003 аудит, можно отслеживать действия пользователя и действия Windows Server 2003, которые называются событиями на компьютере. При использовании аудита, можно указать, какие события записываются в журнал безопасности. Например в журнал безопасности можно вести запись допустимы и неверных попыток входа и события, связанные с создание, открытие или удаление файлов и других объектов

3	2	ISO 3 — Ряды номиналов радиодеталей. ISO 4 — система сокращения названий периодических изданий (журналов). ISO 5 — Фотографии и графические технологии — измерения плотности. ISO 6 — Светочувствительность фотоматериалов. ISO 7 — Трубная резьба.

3.4. Лабораторные занятия

Очная форма

Модуль	Номер раздела	Содержание лабораторных занятий
1	3	Делегирование объектов Active Directory
2	2	Audit Collection Services (ACS) предоставляет средства для сбора записей, созданных с помощью политики аудита и их хранения в централизованной базе данных. Используя ACS, организации могут консолидировать отдельные журналы безопасности в централизованно управляемой базе данных и могут фильтровать и анализировать события с помощью инструментов, предоставляемых Microsoft SQL Serve
3	1	Организация работы с документами: организация документооборота, хранения и использования документов в текущей деятельности учреждения1. Из определения видно, что одной из составляющих организации работы с документами является документооборот.
	3	ЭЦП и юридическая значимость электронного документа

3.5. Организация самостоятельной работы

Очная форма

Модуль	Номер раздела	Содержание материала выносимого на самостоятельное изучение	Виды самостоятельной работы
1	1	Разграничение доступа	
1	2	Права и превелегии пользователей	
1	3	Разграничение доступа в Active Directory	
2	1	Системы аудита Windows Server 2003	

2	2	Службы ACS	
2	3	Система аудита Windows Server 2003	
3	1	Работа с документами в организации	
3	2	Стандарты ISO	
3	3	Правовые вопросы применения ЭЦП и СКЗИ в России	

4. Интерактивные формы образовательных технологий

Модуль	Номер раздела	Вид учебных занятий	Образовательные технологии	Количество часов
1	1	ЛК	Физическая демонстрация с использованием презентации	3
2	5	ЛК, ПЗ	Работа с электронными образовательными ресурсами	4
3	9	ЛК	Физическая демонстрация с использованием презентации	4

5. Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

Фонд оценочных средств

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Основная литература

6.1.1. Печатные издания

1. Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : учеб. пособие. - Москва : Академия, 2006. - 240с. - (Высшее профессиональное образование). - ISBN 5-7695-2706-4 : 291-40.
2. Расторгуев С.П. Основы информационной безопасности : учеб. пособие для студентов вузов. - Москва : Академия, 2007. - 186 с. - (Высш. проф. образование). - ISBN 978-5-7695-3098-2 : 225-00.

6.1.2. Издания из ЭБС

1.Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : Рекомендовано Государственным образовательным учреждением высшего профессионального образования "Академия Федеральной службы безопасности Российской Федерации" в качестве учебного пособия для студентов высших учебных заведений, обучающихся по специальностям направления подготовки 090300 - "Информационная безопасность вычислительных, автоматизированных и телекоммуникационных систем" и направлению подготовки 090900 - "Информационная безопасность". Регистрационный номер рецензии № 742 от 25 февраля 2010 г. (ГОУВПО

"Московский государственный университет печати") / Девянин П.Н. - Moscow : Горячая линия - Телеком, 2012. - . - Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс] : Учебное пособие для вузов / Девянин П.Н. - М. : Горячая линия - Телеком, 2012. - http://www.studentlibrary.ru/book/ISBN9785991201476.html. - ISBN 978-5-9912-0147-6

6.2. Дополнительная литература

6.2.1. Печатные издания

1.Столлингс Вильям. Основы защиты сетей : приложения и стандарты / пер. с англ. и ред. А.Г. Сивака. - Москва : Вильямс, 2002. - 432с. : ил. - ISBN 5-8459-0298-3. - ISBN 0-1301-6093-8 : 145-20.
2. Мартин Майкл Дж. Введение в сетевые технологии : практич. руководство по организации сетей. - Москва : ЛОРИ, 2002. - 659с. - ISBN 0-7357-0977-7 : 130-00.
3. Клейменов Сергей Анатольевич. Администрирование в информационных системах : учеб. пособие / под ред. В.П. Мельникова. - Москва : Академия, 2008. - 272с. - (Высшее профессиональное образование). - ISBN 978-5-7695-4708-9 : 196-46.

6.2.2. Издания из ЭБС

1. Милославская Н.Г. Проверка и оценка деятельности по управлению информационной безопасностью : Допущено Учебно-методическим объединением высших учебных заведений России по образованию в области информационной безопасности в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению подготовки 090900 - "Информационная безопасность" (уровень - магистр) / Милославская Н.Г.; Сенаторов М.Ю.; Толстой А.И. - Moscow : Горячая линия - Телеком, 2013. - . - Проверка и оценка деятельности по управлению информационной безопасностью [Электронный ресурс] : Учебное пособие для вузов / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - Вып. 5. - М. : Горячая линия - Телеком, 2013. - (Серия "Вопросы управления информационной безопасностью"). - http://www.studentlibrary.ru/book/ISBN9785991202756.html. - ISBN 978-5-9912-0275-6

6.3. Базы данных, информационно-справочные и поисковые системы

1 . Информационная система «Единое окно доступа к образовательным ресурсам» (http://window.edu.ru/).
2. Научная Электронная Библиотека http://www.e-library.ru.
3 . Электронные версии учебников, пособий, методических разработок, указаний и рекомендаций по всем видам учебной работы, предусмотренных вузовской рабочей программой, находящиеся в свободном доступе для студентов, обучающихся в вузе

7. Перечень программного обеспечения

Программное обеспечение общего назначения: ОС Microsoft Windows, Microsoft Office, ABBYY FineReader, ESET NOD32 Smart Security Business Edition, Foxit Reader, АИБС "МегаПро".
Программное обеспечение специального назначения:

8. Материально-техническое обеспечение дисциплины

672000, г. Чита, ул. Кастринская, д.1, корп. 1, ауд. 08-206
Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации
Комплект специализированной учебной мебели. Доска маркерная.
Наборы демонстрационного оборудования и учебно-наглядных пособий по дисциплинам,

переносной мультимедийный к-т в составе: экран на треноге, мультимедиапроектор, ноутбук.
MS Office Standart 2013 (договор № 223-798 от 30.12.2014 г., срок действия - бессрочно; договор № 223-799 от 30.12.2014г., срок действия - бессрочно) Mozilla Firefox Право использования программного обеспечения предоставляется по MPL лицензии (https://www.mozilla.org/ru/firefox/) (срок действия - право использования программного обеспечения действует до изменения политики правообладателя) АИБС «МегаПро» (договор № 13215/223П/15-569 от 18.12.2015 г.)

9. Методические рекомендации по организации изучения дисциплины

Лекции являются основным источником теоретического материала по дисциплине. Посещение и конспектирование лекций является обязательной составляющей успешного освоения дисциплины обучающимися.
Для эффективного освоения материала дисциплины необходимо выполнение следующих требований:
- обязательное посещение всех лекционных и практических занятий, способствующее системному овладению материалом курса;
- все вопросы соответствующих разделов и тем по дисциплине необходимо фиксировать (на любых носителях информации);
- обязательное выполнение домашних заданий является важнейшим требованием и условием формирования целостного и системного знания по дисциплине;
- обязательность личной активности каждого студента на всех занятиях по дисциплине;
- в случаях неясности каких-либо вопросов, обсуждаемых на занятиях, необходимо задать соответствующие вопросы преподавателю, а не оставлять их непонятыми;
- в случаях пропусков занятий по уважительным причинам студентам предоставляется право подготовки и представления заданий и ответов на вопросы изученного материала, с расчетом на помощь преподавателя в его усвоении;
- в случаях пропусков без уважительной причины студент обязан самостоятельно изучить соответствующий материал;
- необходимым условием является самостоятельность и инициативность студентов при контроле набора баллов по дисциплине для успешного прохождения промежуточной аттестации.
Порядок организации лабораторной работы студентов
Лабораторная работа студентов предполагает сознательной активной работы не только в лаборатории при сборке установки и проведении измерений, но и дома при подготовке к измерениям, обработке результатов и составления отчета.
Выполнение лабораторной работы есть определенная последовательность действий:
— подготовка к эксперименту;
— проведение измерений;
— обработка полученных результатов;
— формулировка выводов и написание отчета.
Для грамотного и быстрого их выполнения должна сложиться определенная система знаний и умений (ориентировочная основа действия), которая обеспечит правильное и рациональное исполнение действия.
Поэтому выполнение каждой лабораторной работы необходимо начинать с изучения ее описания и приведения знаний в систему, а именно:
— ясно представить себе общую цель данной конкретной лабораторной работы и последовательность задач, решение которых приведет к достижению окончательной цели;
— знать основные особенности объекта исследования
— изучить и уметь объяснить физические основы используемых в работе методов измерения искомых величин;
— уметь нарисовать принципиальную схему используемой установки и знать назначение каждого из ее узлов;
— знать последовательность выполнения этапов лабораторной работы;
— иметь общее представление об ожидаемых результатах проводимого эксперимента и уметь выбрать метод, нужный для их математической обработки
Отчет студента по работе должен быть индивидуальным, составленным по

установленной форме, и содержать следующие разделы: наименование работы; цель работы; индивидуальное задание; применяемая аппаратура; ее описание (система, класс, цена давления и т.д.); краткое изложение методики, схемы опытов; таблицы данных измерений; итог обработки результатов и расчетные формулы; графики; анализ результатов и погрешностей; фрагмент конструкции соединения. Анализ результатов
является важной частью отчета.
Порядок организации студентов на практическом занятии
Перед практическими занятиями студент должен повторить лекционный материал, ответив на вопросы для самоконтроля по необходимой теме, а также просмотреть рекомендации по решению типичных задач этой темы.
На практических занятиях обобщаются и систематизируются знания, полученные на лекционных занятиях и формируются умения решать типовые задачи. При решении студент должен уметь:
- выделять описываемое явление (объект), анализировать условие задачи;
- выполнять построение модели явления;
- формулировать выводы из модели;
- выявлять применения полученных знаний в профессиональной деятельности.
На практических занятиях студент приобретает учится собирать и анализировать информацию для формирования исходных данных для проектирования средств и сетей связи.
Порядок организации самостоятельной работы студентов
Самостоятельная работа – индивидуальная учебная деятельность, осуществляемая без непосредственного руководства преподавателя, в ходе которой бакалавр активно воспринимает, осмысливает информацию, решает теоретические и практические задачи. В процессе проведенной самостоятельной работы формируются компетенции.
Самостоятельная работа студентов предполагает:
- самостоятельный поиск, обработку (анализ, синтез, обобщение и систематизацию), адаптацию необходимой по дисциплине информации;
- выполнение заданий для самостоятельной работы;
- изучение и усвоение теоретического материала, представленного на лекционных занятиях и в соответствующих литературных источниках (рекомендуемая основная и дополнительная литература);
- самостоятельное изучение отдельных вопросов курса;
- подготовка к практическим и лабораторным занятиям, в соответствии с рекомендациями преподавателя (выполнение конкретных заданий, соответствующие организационные действия и т.д.).
Самостоятельное выполнение контрольных и лабораторных работ является основным средством освоения теоретического материала курса и приобретения умений и навыков его практического применения, поскольку только применение знаний обеспечивает их глубокое понимание. Контроль за самостоятельной работой производится на практических занятиях.

Разработчик/группа разработчиков: Свешников Игорь Вадимович

Рассмотрена на заседании кафедры
(протокол от 24.05.2019 г. № 14)