МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
"Казанский (Приволжский) федеральный университет"
Институт вычислительной математики и информационных технологий

УТВЕРЖДАЮ
Проректор по образовательной деятельности КФУ
проф. Таюрский Д.А.
"___"_____20___ г.

Программа дисциплины

Программно-аппаратные средства защиты информации

Направление подготовки: 10.03.01 - Информационная безопасность
Профиль подготовки: Безопасность компьютерных систем
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2020

Содержание

Программу дисциплины разработал(а)(и) заведующий кафедрой, к.н. (доцент) Акчурин А.Д. (Кафедра радиоастрономии, Высшая школа киберфизических систем и прикладной электроники), Adel.Akchurin@kpfu.ru ; Иванов Константин Васильевич

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОПОП ВО

Обучающийся, освоивший дисциплину (модуль), должен обладать следующими компетенциями:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОПК-7	способность 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
ПК-1	способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
ПК-7	способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений

Обучающийся, освоивший дисциплину (модуль):

Должен знать:

принципы работы и организацию современных средств защиты информации;

основные подходы к созданию программно-аппаратных средств защиты информации ;

функции и задачи, стоящие перед администраторами безопасности.

Должен уметь:

- Администрировать средства защиты информации, встроенные в современные операционные системы, обеспечивающие дополнительный функционал для средств защиты СВТ, а также сетевые средства защиты информации;

- осуществлять поиск уязвимостей механизмов защиты, реализованных в программном и аппаратном обеспечении;

- выбирать и устанавливать аппаратные средства защиты информации и соответствующее программное обеспечение

Должен владеть:

-Навыками аргументированного выбора механизмов защиты информации, используемых при построении системы защиты информации Автоматизированных систем;

-навыками внедрения и эксплуатации современных средств программно-аппаратной защиты информации;

- навыками во внедрении, адаптации и настройке механизмов защиты прикладных ИС.

Должен демонстрировать способность и готовность:

Применять программно-технические способы и средства для обеспечения информационной безопасности объекта;

осуществлять аргументированный выбор средств защиты информации;

использовать встроенные в программное и аппаратное обеспечение механизмы защиты информации.

2. Место дисциплины (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в раздел "Б1.Б.08 Дисциплины (модули)" основной профессиональной образовательной программы 10.03.01 "Информационная безопасность (Безопасность компьютерных систем)" и относится к базовой (общепрофессиональной) части.
Осваивается на 4 курсе в 7 семестре.

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 5 зачетных(ые) единиц(ы) на 180 часа(ов).

Контактная работа - 90 часа(ов), в том числе лекции - 54 часа(ов), практические занятия - 0 часа(ов), лабораторные работы - 36 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 54 часа(ов).

Контроль (зачёт / экзамен) - 36 часа(ов).

Форма промежуточного контроля дисциплины: экзамен в 7 семестре.

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Структура и тематический план контактной и самостоятельной работы по дисциплине (модулю)

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. введение в предметную область.	7	2	0	0	2
2.	Тема 2. Техническое проектирование и реализация комплексов средств защиты информации. Обзор подходов к созданию средств защиты информации. Проблемы проектирования и реализации механизмов защиты	7	4	0	0	4
3.	Тема 3. Теоретические основы реализации механизмов защиты информации	7	10	0	0	6
4.	Тема 4. Организационные основы реализации механизмов защиты информации/ Нормативно-правовые документы, регламентирующие применение программно-аппаратных методов и средств ЗИ.	7	8	0	10	12
5.	Тема 5. Механизмы защиты, реализуемые на основе программных продуктов фирмы Microsoft	7	4	0	6	5
6.	Тема 6. Механизмы защиты, реализуемые на базе ОС семейства Linux	7	2	0	6	5
7.	Тема 7. Средства защиты информации, реализованные в активном сетевом оборудовании	7	6	0	6	5
8.	Тема 8. Средства защиты информации, реализованные в прикладном программном обеспечении	7	4	0	0	5
9.	Тема 9. Разработка средств защиты, реализуемых на программно-аппаратном уровне на примере выполнения опытно-конструкторской работы(ОКР).	7	10	0	6	8
10.	Тема 10. Сертификация средств защиты информации.	7	4	0	2	2

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
	Итого		54	0	36	54

4.2 Содержание дисциплины (модуля)

Тема 1. введение в предметную область.

Место программно-аппаратных методов и средств в комплексных системах защиты информации.Основные термины и определения. Структура и состав систем защиты информации и комплексов средств защиты. Законы РФ "О государствен-ной тайне", "Об информации, информатизации и защите информации". Структура государственных органов, осуществляющих контроль за выполнением требований по защите информации. Органи-зационная поддержка мер за-щиты. Отраслевые стандар-ты. Пакет руководящих до-кументов Гостехкомиссии России. ISO 15408. Единые критерии. Особенности ISO 15408 по сравнению с другими стандартами в области безопасности. Документы ФСТЭК России, разработан-ные на базе ISO 15408.

Тема 2. Техническое проектирование и реализация комплексов средств защиты информации. Обзор подходов к созданию средств защиты информации. Проблемы проектирования и реализации механизмов защиты

Техническое проектирование и реализация комплексов средств защиты. Жизненный цикл корпоративный системы. Обзор подходов к созданию комплексов средств защиты. Проблемы проектирования и реализации защищенных АС. Синтез КСЗ и его этапы.

Основные термины и определения. Техническое проектирование и реализация систем защиты. Жизненный цикл системы. Обзор подходов к созданию защищённых автоматизированных систем (АС). Проблемы проектирования и реализации защищенных АС. Синтез АС и его этапы.

Организационно-правовые аспекты защиты информации в АС.

Тема 3. Теоретические основы реализации механизмов защиты информации

Основные теоретические положения защиты информации. Подсистема управления доступом.Идентификация и аутентификация. Формальные модели и политики управления доступом. Подсистема обеспечения целостности. Контроль целостности. Антивирусная защиты. Резервное копирование. Подсистема регистрации и учёта событий. Криптографическая подсистема.

Тема 4. Организационные основы реализации механизмов защиты информации/ Нормативно-правовые документы, регламентирующие применение программно-аппаратных методов и средств ЗИ.

Законы РФ ?О государственной тайне?, ?Об информации, информатизации и защите информации?. Структура государственных органов, осуществляющих контроль за выполнением требований по защите информации. Организационная поддержка мер за-щиты. Отраслевые стандарты. Пакет руководящих документов Гостехкомиссии России. ISO 15408. Единые критерии. Особенности ISO 15408 по сравнению с другими стандартами в области безопасности. Документы ФСТЭК России, разработанные на базе ISO 15408.

Тема 5. Механизмы защиты, реализуемые на основе программных продуктов фирмы Microsoft

Возможности КСЗ ОС семейства Windows

- Подсистема разграничения доступа
- Подсистема регистрации и учёта
- Подсистема обеспечения целостности
- Криптографическая подсистема
- Интерфейс администратора безопасности

Вывод системы из нестабильного состояния: по-иск и устранение источника неполадок в дисковой подсистеме ОС Windows; поиск и устранение источника неполадок в се-тевой подсистеме ОС Windows; поиск и устранение источника неполадок в распределении виртуальной памяти ОС Windows; поиск и устранение источника неполадок в распределении ресурсов центрального процессора ОС Windows.

Тема 6. Механизмы защиты, реализуемые на базе ОС семейства Linux

Возможности комплекса средств защиты (КСЗ) ОС семейства Linux

- Подсистема разграничения доступа
- Подсистема регистрации и учёта
- Подсистема обеспечения целостности
- Криптографическая подсистема

- Интерфейс администратора безопасности

Пересборка ядра ОС Вы-вод системы из нестабильного состояния: по-иск и устранение источника неполадок в дисковой подсистеме ОС семейства Linux; поиск и устранение источника неполадок в сетевой под-системе ОС семейства Linux; поиск и устранение источника неполадок в распределении виртуальной памяти ОС семейства Linux; поиск и устранение источника неполадок в распределении ресурсов центрально-го процессора ОС семейства Linux.

Тема 7. Средства защиты информации, реализованные в активном сетевом оборудовании

Используемое сетевое оборудование. Его классификация. Архитектура построения без-опасных сетей. Средства обеспечения безопасности корпоративных сетей. Основные защитные механизмы и примеры их реализации: построение защиты сетевых средств и сервисов, построение системы межсетевого экранирования, построение системы обнаружения вторжений, построение системы анализа сетевой без-опасности, построение системы кодирования информации, передаваемой по открытым каналам связи.

Тема 8. Средства защиты информации, реализованные в прикладном программном обеспечении

Возможности реализации средств защиты на прикладном уровне. Использование API и библиотек. Использование системных вызовов. Реализация собственных библиотек. При-меры реализации механизмов защиты на прикладном уровне. Стандарты разработки ПО. Понятие о Единой Системе Программной Документации. Стадии разработки программного обеспечения. Виды программ и программных документов. Техническое задание, требования к содержанию и оформлению. Пояснительная записка. Требования к содержанию и оформлению. Описание применения. Требования к содержанию и оформлению. Описание про-граммы.

Тема 9. Разработка средств защиты, реализуемых на программно-аппаратном уровне на примере выполнения опытно-конструкторской работы(ОКР).

Порядок выполнения ОКР. Этап разработки эскизного проекта. Этап разработки технического проекта. Этап разработки рабочей конструкторской документации для изготовления опытного образца. Этап изготовления опытного образца и проведения предварительных испытаний. Этап проведения государственных испытаний опытного образца (межведомственных испытаний опытного образца). Этап утверждения рабочей конструкторской документации для организации промышленного (серийного) производства. Требования к порядку разработки рабочей конструкторской документации

Тема 10. Сертификация средств защиты информации.

Понятие сертификации. Основные участники сертификации: федеральный орган, аккредитованный орган, испытательная лаборатория, заявитель. Основные системы обязательной сертификации средств защиты информации: системы ФСТЭК России, Минобороны России, ФСБ России. Добровольные системы сертификации средств защиты информации. Схемы сертификационных испытаний. Инспекционный контроль. Выбор требу-емого класса защищенности и уровня контроля отсутствия недекларированных возможно-стей. Сертификация на соот-ветствие техническим услови-ям. Особенности сертификации средств защиты конфиденци-альной информации и средств защиты персональных данных. Требования к заявке на проведение сертификационных испытаний и к техническим условиям. Структура требований руководящего документа Гостехкомиссии России по НДВ. Порядок проведения испытаний для каждого из уровней контроля отсутствия недекларированных возможностей.

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Самостоятельная работа обучающихся выполняется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия. Самостоятельная работа подразделяется на самостоятельную работу на аудиторных занятиях и на внеаудиторную самостоятельную работу. Самостоятельная работа обучающихся включает как полностью самостоятельное освоение отдельных тем (разделов) дисциплины, так и проработку тем (разделов), осваиваемых во время аудиторной работы. Во время самостоятельной работы обучающиеся читают и конспектируют учебную, научную и справочную литературу, выполняют задания, направленные на закрепление знаний и отработку умений и навыков, готовятся к текущему и промежуточному контролю по дисциплине.

Организация самостоятельной работы обучающихся регламентируется нормативными документами, учебно-методической литературой и электронными образовательными ресурсами, включая:

Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры (утвержден приказом Министерства образования и науки Российской Федерации от 5 апреля 2017 года №301)

Письмо Министерства образования Российской Федерации №14-55-996ин/15 от 27 ноября 2002 г. "Об активизации самостоятельной работы студентов высших учебных заведений"

Устав федерального государственного автономного образовательного учреждения "Казанский (Приволжский) федеральный университет"

Правила внутреннего распорядка федерального государственного автономного образовательного учреждения высшего профессионального образования "Казанский (Приволжский) федеральный университет"

Локальные нормативные акты Казанского (Приволжского) федерального университета

6. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств по дисциплине (модулю) включает оценочные материалы, направленные на проверку освоения компетенций, в том числе знаний, умений и навыков. Фонд оценочных средств включает оценочные средства текущего контроля и оценочные средства промежуточной аттестации.

В фонде оценочных средств содержится следующая информация:

- соответствие компетенций планируемым результатам обучения по дисциплине (модулю);
- критерии оценивания сформированности компетенций;
- механизм формирования оценки по дисциплине (модулю);
- описание порядка применения и процедуры оценивания для каждого оценочного средства;
- критерии оценивания для каждого оценочного средства;
- содержание оценочных средств, включая требования, предъявляемые к действиям обучающихся, демонстрируемым результатам, задания различных типов.

Фонд оценочных средств по дисциплине находится в Приложении 1 к программе дисциплины (модулю).

7. Перечень литературы, необходимой для освоения дисциплины (модуля)

Освоение дисциплины (модуля) предполагает изучение основной и дополнительной учебной литературы. Литература может быть доступна обучающимся в одном из двух вариантов (либо в обоих из них):

- в электронном виде - через электронные библиотечные системы на основании заключенных КФУ договоров с правообладателями;
- в печатном виде - в Научной библиотеке им. Н.И. Лобачевского. Обучающиеся получают учебную литературу на абонементе по читательским билетам в соответствии с правилами пользования Научной библиотекой.

Электронные издания доступны дистанционно из любой точки при введении обучающимся своего логина и пароля от личного кабинета в системе "Электронный университет". При использовании печатных изданий библиотечный фонд должен быть укомплектован ими из расчета не менее 0,5 экземпляра (для обучающихся по ФГОС 3++ - не менее 0,25 экземпляра) каждого из изданий основной литературы и не менее 0,25 экземпляра дополнительной литературы на каждого обучающегося из числа лиц, одновременно осваивающих данную дисциплину.

Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля), находится в Приложении 2 к рабочей программе дисциплины. Он подлежит обновлению при изменении условий договоров КФУ с правообладателями электронных изданий и при изменении комплектования фондов Научной библиотеки КФУ.

8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

Интернет-портал образовательных ресурсов по ИТ - http://www.intuit.ru

Интернет-портал по информационной безопасности - http://all-ib.ru/

Сайт федеральной службы по техническому и экспортному контролю - www.fstec.ru

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Вид работ	Методические рекомендации
лекции	Теоретический материал излагается на лекциях. Причем конспект лекций, который остается у студента в результате прослушивания лекции не может заменить учебник. Его цель-формулировка основных утверждений и определений. Прослушав лекцию, полезно ознакомиться с более подробным изложением материала в учебнике. Список литературы разделен на две категории: необходимый для сдачи зачета минимум и дополнительная литература.

Вид работ	Методические рекомендации
лабораторные работы	Изучение курса подразумевает не только овладение теоретическим материалом, но и получение практических навыков для более глубокого понимания разделов на основе выполнения лабораторных работ, а также развитие абстрактного мышления и способности самостоятельно доказывать утверждения. По каждой лабораторной работе преподавателю должен быть представлен отчёт следующей структуры: 1. Отчет должен иметь заголовок со следующей информацией - фамилия и.о. студента, группа, тема лабораторной работы (название). Содержание , включающее в себя как минимум названия упражнений, включенных в отчет(подряд или выборочно, если это необходимо). Если упражнение одно, название можно не включать. 2. Отчет по каждому упражнению составляется в следующей последовательности. 2.1. Постановка задачи: - формулировка задания к упражнению лабораторной работы; - цель (задание выполняется ради наблюдения некоторого эффекта, изучения типичной особенности; задание моделирует распространенную на практике ситуацию и т.п.). В данном пункте проверяется понимание студента, какой результат ожидается получить, зачем ему получаемый результат, где его можно применить. также фиксируются ожидания студента; - какие средства используются; если формулировка оставляет свободу выбора каких-либо методов или параметров, произвести и обосновать этот выбор. 2.2. Начальная ситуация (подчеркнуть, что будет создано, изменено, дополнено или удалено в ходе выполнения задания) - если применимо. 2.3. Выполнение задания: - алгоритм выполнения задания и пояснения к его шагам; - какие проблемы возникли и как они были решены - какие результаты достигнуты (подтвердить листингами/снимками экрана, выделить основной момент). 3. При написании отчета следует стремиться к сжатому, но четкому изложению. Руководствуйтесь критерием: отчет должен быть понятен читателю, не знакомому с заданием, но являющемуся достаточным специалистом в этой области. 4. Отчет, идентичный целиком или фрагментами ранее поступившему отчету другого студента, независимо от того, совместно или раздельно выполнялась работа, при выставлении рейтингов в расчёт не принимается и наказывается дополнительным вопросом/заданием на зачёте. 5. Больше требований к оформлению отчета и стилю изложения нет. В то же время отчет, не соответствующий требованиям пп. 1-4, оценивается с существенным штрафом(до 50% баллов). 6. Отчеты по заданиям выполняются в электронном виде, в одном из форматов winword-DOC, RTF, ODT. По каждой теме рекомендуется составлять один отчет, охватывающий все задания темы. 7. Имя файла отчета: name_labN_course.ext где name - фамилия студента латинскими буквами, N - номер темы, course - аббревиатура курса, ext - расширение файла (doc, txt, rtf), например: 'ivanov_lab2_ПАСЗИ.doc';
самостоя-тельная работа	Важнейшим этапом практического занятия является самостоятельная работа обучающихся. В зависимости от конкретной темы занятия обучающиеся самостоятельно выполняют контрольные задания. Во время разбора контролируется качество выполнения самостоятельной работы и сформированных навыков и умений. Преподаватель индивидуально оценивает выполнение целей практического занятия. Самостоятельная (внеаудиторная) работа обучающихся складывается из нескольких разделов: 1. Теоретическая самоподготовка обучающихся по учебным темам, входящим в примерный тематический учебный план. 2. Знакомство с дополнительной учебной литературой и другими учебными методическими материалами, закрепляющими некоторые практические навыки обучающихся.

Вид работ	Методические рекомендации
экзамен	При знакомстве с лекционным материалом, постарайтесь его понять, но не старайтесь запомнить. Результат для вас: общее обзорное представление обо всём данном учебном курсе. Помните, что лекции следует читать 2 раза - в начале вашей подготовки к экзамену и в конце - перед экзаменом. Итак, вечером накануне повторно перечитайте(или хотя бы пролистайте) свои конспекты лекций. Важнейшие определения стремитесь запомнить. Результат: обзорное запоминание важнейших положений данного курса. Вы будете меньше путаться при ответе на экзамене Дополнительная литература. По списку вопросов подберите соответствующие разделы литературы, чтобы знать ответы на эти вопросы. Книги более полно и развёрнуто объясняют то, что очень кратко было записано в ваших конспектах. Помните, что некоторые нюансы не освещаются на лекциях и вы должны их подготовить самостоятельно по литературе или лабораторным работам. Результат: более полное знание учебного материала курса, заполнение тех пробелов, которые неизбежно бывают в лекциях. Пересмотрите свои отчёты по лабораторным работам и разберитесь во всех выполненных работах. Здесь тоже могут встретиться полезные определения и выводы. Считается, что студент на практических занятиях должен получить подтверждения тем теоретическим положениям, которые излагаются в лекциях. Результат: умение доказать теоретические положения конкретными фактами. Вопросы. Просмотрите вопросы и попробуйте дать определения всем важнейшим понятиям, о которых там спрашивается. Если не получается дать определение, то найдите его и выучите. С него-то вам и надо будет начинать свой ответ на экзамене. Трудные вопросы. В последний день перед экзаменом пересмотрите список вопросов и убедитесь, что на большинство из них вы уже можете дать ответ. Дополнительно перечитайте учебный материал по самым сложным и 'страшным' для вас вопросам. Погружение. В материал каждой учебной дисциплины при подготовке к зачёту следует 'погружаться'. Это означает, что при подготовке не надо заниматься ничем другим, ничем посторонним. Отвлекаться можно только на отдых. А всё остальное время - учить, учить, учить... Высшее образование требует именно такой способности: способности к погружению в предмет и к усвоению больших объёмов знаний за относительно короткий срок.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем, представлен в Приложении 3 к рабочей программе дисциплины (модуля).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Материально-техническое обеспечение образовательного процесса по дисциплине (модулю) включает в себя следующие компоненты:

Помещения для самостоятельной работы обучающихся, укомплектованные специализированной мебелью (столы и стулья) и оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду КФУ.

Учебные аудитории для контактной работы с преподавателем, укомплектованные специализированной мебелью (столы и стулья).

Компьютер и принтер для распечатки раздаточных материалов.

Мультимедийная аудитория.

Компьютерный класс.

Специализированная лаборатория.

12. Средства адаптации преподавания дисциплины к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья

При необходимости в образовательном процессе применяются следующие методы и технологии, облегчающие восприятие информации обучающимися инвалидами и лицами с ограниченными возможностями здоровья:

- создание текстовой версии любого нетекстового контента для его возможного преобразования в альтернативные формы, удобные для различных пользователей;

- создание контента, который можно представить в различных видах без потери данных или структуры, предусмотреть возможность масштабирования текста и изображений без потери качества, предусмотреть доступность управления контентом с клавиатуры;

- создание возможностей для обучающихся воспринимать одну и ту же информацию из разных источников - например, так, чтобы лица с нарушениями слуха получали информацию визуально, с нарушениями зрения - аудиально;

- применение программных средств, обеспечивающих возможность освоения навыков и умений, формируемых дисциплиной, за счёт альтернативных способов, в том числе виртуальных лабораторий и симуляционных технологий;

- применение дистанционных образовательных технологий для передачи информации, организации различных форм интерактивной контактной работы обучающегося с преподавателем, в том числе вебинаров, которые могут быть использованы для проведения виртуальных лекций с возможностью взаимодействия всех участников дистанционного обучения, проведения семинаров, выступления с докладами и защиты выполненных работ, проведения тренингов, организации коллективной работы;

- применение дистанционных образовательных технологий для организации форм текущего и промежуточного контроля;

- увеличение продолжительности сдачи обучающимся инвалидом или лицом с ограниченными возможностями здоровья форм промежуточной аттестации по отношению к установленной продолжительности их сдачи:

- продолжительности сдачи зачёта или экзамена, проводимого в письменной форме, - не более чем на 90 минут;

- продолжительности подготовки обучающегося к ответу на зачёте или экзамене, проводимом в устной форме, - не более чем на 20 минут;

- продолжительности выступления обучающегося при защите курсовой работы - не более чем на 15 минут.

Программа составлена в соответствии с требованиями ФГОС ВО и учебным планом по направлению 10.03.01 "Информационная безопасность" и профилю подготовки "Безопасность компьютерных систем".

Приложение 2
к рабочей программе дисциплины (модуля)
Б1.Б.08 Программно-аппаратные средства защиты информации

Перечень литературы, необходимой для освоения дисциплины (модуля)

Направление подготовки: 10.03.01 - Информационная безопасность
Профиль подготовки: Безопасность компьютерных систем
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2020

Основная литература:

1. Мельников, Д.А. Информационная безопасность открытых систем : учебник / Д.А. Мельников. - 3-е изд., стер. - Москва : ФЛИНТА, 2019. - 444 с. - ISBN 978-5-9765-1613-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1042499 (дата обращения: 20.02.2020). - Режим доступа: по подписке.

2. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва : РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/405000 (дата обращения: 20.02.2020). - Режим доступа: по подписке.

3. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П. Б. Хорев. - 3-е изд., испр. и доп. - Москва : ИНФРА-М, 2020. - 327 с. - (Высшее образование: Бакалавриат). - ISBN 978-5-16-015471-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1035570 (дата обращения: 20.02.2020). - Режим доступа: по подписке.

4. Жукова, М. Н. Управление информационной безопасностью. Ч. 2: Управление инцидентами информационной безопасности : учебное пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 100 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/463061 (дата обращения: 20.02.2020). - Режим доступа: по подписке.

Дополнительная литература:

1. Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. - 5-е изд., стер. - Санкт-Петербург : Лань, 2019. - 324 с. - ISBN 978-5-8114-4067-2. - Текст : электронный // Лань : электронно-библиотечная система. - URL: https://e.lanbook.com/book/114688 (дата обращения: 20.02.2020). - Режим доступа: для авториз. пользователей.

2. Партыка, Т. Л. Информационная безопасность : учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - Москва : ФОРУМ : ИНФРА-М, 2020. - 432 с. - (Среднее профессиональное образование). - ISBN 978-5-00091-473-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1081318 (дата обращения: 20.02.2020). - Режим доступа: по подписке.

3. Васильков, А. В. Безопасность и управление доступом в информационных системах : учебное пособие / А.В. Васильков, И.А. Васильков. - Москва : ФОРУМ : ИНФРА-М, 2020. - 368 с. - (Среднее профессиональное образование). - ISBN 978-5-91134-360-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1082470 (дата обращения: 20.02.2020). - Режим доступа: по подписке.

Приложение 3
к рабочей программе дисциплины (модуля)
Б1.Б.08 Программно-аппаратные средства защиты информации

Перечень информационных технологий, используемых для освоения дисциплины (модуля), включая перечень программного обеспечения и информационных справочных систем

Направление подготовки: 10.03.01 - Информационная безопасность
Профиль подготовки: Безопасность компьютерных систем
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2020

Освоение дисциплины (модуля) предполагает использование следующего программного обеспечения и информационно-справочных систем:

Операционная система Microsoft Windows 7 Профессиональная или Windows XP (Volume License)

Пакет офисного программного обеспечения Microsoft Office 365 или Microsoft Office Professional plus 2010

Браузер Mozilla Firefox

Браузер Google Chrome

Adobe Reader XI или Adobe Acrobat Reader DC

Kaspersky Endpoint Security для Windows

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен обучающимся. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, учебно-методические комплексы, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего образования (ФГОС ВО) нового поколения.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе Издательства "Лань" , доступ к которой предоставлен обучающимся. ЭБС Издательства "Лань" включает в себя электронные версии книг издательства "Лань" и других ведущих издательств учебной литературы, а также электронные версии периодических изданий по естественным, техническим и гуманитарным наукам. ЭБС Издательства "Лань" обеспечивает доступ к научной, учебной литературе и научным периодическим изданиям по максимальному количеству профильных направлений с соблюдением всех авторских и смежных прав.