МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

«СОГЛАСОВАНО»
Руководитель ОП
«Информационная безопасность»
_____ Варлатая С.К.
(подпись) (Ф.И.О. рук. ОП)
« 5 » июля 2018 г.

«УТВЕРЖДАЮ»
Заведующий (ая) кафедрой
информационной безопасности
(название кафедры)
_____ Добржинский Ю.В.
(подпись) (Ф.И.О. рук. ОП)
« 5 » июля 2018 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ (РПУД)
«Основы информационной безопасности»
Направление –10.03.01 «Информационная безопасность»
Профиль подготовки - «Комплексная защита объектов информатизации**»**
Форма подготовки – очная

курс 2 семестр 3
лекции 36 час.
практические занятия 18 час.
лабораторные работы не предусмотрено
в том числе с использованием МАО лек. ____ / пр. ____ / лаб. ____ час.
всего часов аудиторной нагрузки 54 час.
в том числе с использованием МАО ____ час.
самостоятельная работа 9 час.
в том числе на подготовку к экзамену 45 час.
контрольные работы (количество) не предусмотрено
курсовая работа / курсовой проект не предусмотрено
зачет ____ семестр
экзамен 3 семестр

Рабочая программа составлена в соответствии с требованиями образовательного стандарта, самостоятельно устанавливаемого ДВФУ, утвержденного приказом ректора от 20.07.2017 №12-13-1479.

Рабочая программа обсуждена на заседании кафедры информационной безопасности
протокол № 10 от « 15 » июня 2019 г.

Заведующий (ая) кафедрой: Добржинский Ю.В., к.т.н., с.н.с.
Составитель (ли): Смирнов М.Е.

I. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20__г. № _____

Заведующий кафедрой _____ _Ю.В. Добржинский_
(подпись) (и.о. фамилия)

II. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 200__г. № _____

Заведующий кафедрой _____ _Ю.В. Добржинский _
(подпись) (и.о. фамилия)

Аннотация к рабочей программе дисциплины «Основы информационной безопасности»

Курс «Основы информационной безопасности» является важной составной частью общепрофессиональной подготовки специалиста по организации и технологии защиты информации. Рабочая программа дисциплины «Основы информационной безопасности» разработана для студентов 2 курса специальности 10.03.01 «Информационная безопасность».

Общая трудоемкость освоения дисциплины составляет 108 часов (3 з.е.). Учебным планом предусмотрены лекционные занятия (36 час.), практические занятия (18 час.), самостоятельная работа студентов (9 час.), контроль качества обучения студентов (45 час.). Дисциплина реализуется на 2 курсе в 3 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина является вводной в проблематику информационной безопасности, поэтому требований к входным знаниям, умениям и компетенциям студента, необходимым для ее изучения, не предъявляется.

Дисциплина является предшествующей для таких дисциплин профессионального цикла как «Программно-аппаратные средства защиты информации», «Криптографические методы защиты информации», «Организационное и правовое обеспечение информационной безопасности».

Цели:

- привитие стремления к поиску оптимальных, простых и надежных решений;
- изучение основ информационной безопасности, формирование у студентов информационного мировоззрения на основе знания принципов защиты информации; воспитание информационной культуры для эффективного применения полученных знаний в профессиональной деятельности;
- развитие творческих подходов при решении сложных научно-

технических задач, связанных с обеспечением информационной безопасности государства и его информационной инфраструктуры;

- развитие профессиональной культуры, формирование научного мировоззрения и развитие системного мышления;
- привитие стремления к поиску оптимальных, простых и надежных решений.

Задачи:

- изучение структур и тенденций развития концептуальных, методологических и организационных основ и современных принципов защиты информации для обеспечения информационной безопасности государства;
- формирование основных теоретических и практических знаний, раскрывающих сущность и значение национальной безопасности и защиты информации в условиях локальных и глобальных вычислительных сетей, автоматизированных информационных систем и систем телекоммуникаций;
- изучить основные положения Доктрины информационной безопасности РФ;
- изучить основы комплексной системы защиты информации;
- изучить основы организационно-правового обеспечения защиты информации;
- изучить методы и средства ведения информационных войн;
- изучить методологии создания систем защиты информации;

В результате изучения данной дисциплины у обучающихся формируются следующие профессиональные, общекультурные, профессионально-специализированные компетенции (элементы компетенций).

Код и формулировка компетенции	**Этапы формирования компетенции**	
(ОК-12) способностью понимать социальную значимость своей будущей	Знает	основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения

профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики		информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации
	Умеет	анализировать и оценивать угрозы информационной безопасности объекта
	Владеет	навыками работы с нормативными правовыми актами
(ПК-10) способностью оценивать уязвимости информационных систем, разрабатывать требования и критерии оценки информационной безопасности, согласованных со стратегией развития информационных систем	Знает	средства и методы предотвращения и обнаружения вторжений
	Умеет	применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности
	Владеет	методами организации и управления деятельностью служб защиты информации на предприятии
(ПСК-3.2) способностью формировать предложения по оптимизации комплекса технических средств, применяемых в функциональном процессе защищаемого объекта и его информационных составляющих, с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объектов и локализации защищаемых элементов	Знает	организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации
	Умеет	разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации
	Владеет	методами формирования требований по защите информации

Для формирования вышеуказанных компетенций в рамках дисциплины «Основы информационной безопасности» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), конспект (ПР-7).

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

МОДУЛЬ 1. Основы информационной политики Российской Федерации и понятие информационной войны (13 ч)

РАЗДЕЛ 1. Основы государственной информационной политики и информационной безопасности Российской Федерации (5 ч)

ТЕМА 1. Понятие национальной безопасности (2 ч)

Интересы и угрозы в области национальной безопасности. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание.

ТЕМА 2. Информационная безопасность в системе национальной безопасности Российской Федерации (3 ч)

Основные понятия, общеметодологические принципы обеспечения информационной безопасности. Национальные интересы в информационной сфере. Источники и содержание угроз в информационной сфере.

РАЗДЕЛ 2. Информационная война, методы и средства её ведения (8 ч)

ТЕМА 1. Основы ведения информационной войны (4 ч)

Информационная эра. Военные информационные функции. Понятие информационной войны. Составные части информационной войны. Виды информационных атак. Цели информационной войны. Методы ведения информационных войн.

ТЕМА 2. Сущность и структура информационного противоборства (4 ч)

Информационная безопасность и информационное противоборство.

Оружие информационного противоборства. Модели информационного противоборства.

МОДУЛЬ 2. Защита автоматизированных систем (23 ч)

РАЗДЕЛ 1. Информационная безопасность автоматизированных систем (23 ч)

ТЕМА 1. Организационно-правовое обеспечение информационной безопасности (3 ч)

Информация как объект юридической защиты. Основные принципы засекречивания информации. Государственная система правового обеспечения защиты информации в Российской Федерации.

ТЕМА 2. Информационные системы (2 ч)

Информация как продукт. Информационные услуги. Источники конфиденциальной информации в информационных системах. Виды технических средств информационных систем.

ТЕМА 3. Угрозы информации (3 ч)

Классы каналов несанкционированного получения информации. Причины нарушения целостности информации. Виды угроз информационным системам. Модель нарушителя информационных систем.

ТЕМА 4. Криптографические методы защиты информации (3 ч)

Требования к криптосистемам. Основные алгоритмы шифрования. Цифровые подписи. Криптографические хэш-функции. Криптографические генераторы случайных чисел. Криптоанализ и атаки на криптосистемы.

ТЕМА 5. Анализ существующих методик определения требований к защите информации (3 ч)

Требования к безопасности информационных систем в России. Классы защищенности средств вычислительной техники от несанкционированного доступа. Факторы, влияющие на требуемый уровень защиты информации.

ТЕМА 6. Методы и модели оценки уязвимости информации (2 ч)

Эмпирический подход к оценке уязвимости информации. Система с полным перекрытием.

ТЕМА 7. Функции и задачи защиты информации (3 ч)

Методы формирования функций защиты. Классы задач защиты информации. Функции защиты. Состояния и функции системы защиты информации.

ТЕМА 8. Архитектура систем защиты информации (4 ч)

Требования к архитектуре СЗИ. Построение СЗИ. Ядро системы защиты информации. Ресурсы системы защиты информации. Организационное построение.

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Тематика практических работ

Тема 1. Информация как объект правового регулирования. Законодательство Российской Федерации в области информационной безопасности. **(8 ч)**

Тема 2. Преступления в сфере компьютерной информации. **(4 ч)**

Тема 3. Выявление источников и носителей информации на промышленном предприятии **(8 ч)**

Тема 4. Выявление и анализ угроз безопасности информации на предприятии. **(8 ч)**

Тема 5. Анализ рисков безопасности информации. **(8 ч)**

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Основы информационной безопасности» представлено в Приложении 1 и включает в себя:

план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;

характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;

требования к представлению и оформлению результатов самостоятельной работы;

критерии оценки выполнения самостоятельной работы.

IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				текущий контроль	промежуточная аттестация
1	МОДУЛЬ 1. Основы информационной политики Российской Федерации и понятие информационной войны.	ОК-12 ПК-10 ПСК-3.2	Знает	ПР-7	1-20
			Умеет	ПР-7	1-20
			Владеет	ПР-7	1-20
2	МОДУЛЬ 2. Защита автоматизированных систем.	ОК-12 ПК-10 ПСК-3.2	Знает	ПР-7	21-41
			Умеет	ПР-7	21-41
			Владеет	ПР-7	21-41

Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков и опыта деятельности, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 2.

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

(электронные и печатные издания)

1. Информационная безопасность: учебное пособие. Т.Л. Партыка, И.И. Попов. М.: Форум, 2011. - 432 с. http://lib.dvfu.ru:8080/lib/item?id=chamo:355949&theme=FEFU

2. Мельников, Д.А. Информационная безопасность открытых систем [Электронный ресурс] : учебник / Д.А. Мельников. — Электрон. дан. — Москва : ФЛИНТА, 2014. — 448 с. — Режим доступа: https://e.lanbook.com/book/48368. — Загл. с экрана.

3. Информационная безопасность: учеб. пособие для студ. сред. проф.образования / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под ред. С.А. Клейменова. - 5-е изд., стер. - М.: Издательский центр «Академия», 2012. - 336 с. http://lib.dvfu.ru:8080/lib/item?id=BookRu:BookRu-920736&theme=FEFU

Дополнительная литература

(печатные и электронные издания)

1. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии. Второе издание. - М.: Гелиос АРВ, 2012. http://lib.dvfu.ru:8080/lib/item?id=chamo:1640&theme=FEFU

2. Информатика и ИКТ. Учебник. 11 класс. Базовый уровень. Макарова Н.В., Николайчук Г.С., Титова Ю.Ф. СПб.: Питер, 2012. - 256 с. http://lib.dvfu.ru:8080/lib/item?id=chamo:276459&theme=FEFU

3. Кожуханов, Н.М. Обеспечение информационной безопасности таможенной дея-тельности на основе инноваций в праве [Электронный ресурс] : монография / Н.М. Кожуханов. — Электрон. дан. — Москва : РТА, 2010. — 92 с. — Режим доступа: https://e.lanbook.com/book/74056

4. И. В. Мешков Информационная безопасность : методические указания для организации практических занятий всех форм обучения. Владивосток : Изд. дом Дальневосточного федерального университета, 2012. – 35 с. Режим доступа: http://lib.dvfu.ru:8080/lib/item?id=chamo:669920&theme=FEFU

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. http://bookre.org/reader?file=756095 Семкин С.Н., Беляков Э.В., Гребенев С.В. «Основы организационного обеспечения информационной безопасности объектов информатизации.».

2. http://bookre.org/reader?file=630269 Девянин П.Н. «Модели безопасности компьютерных систем. Управление доступом и информационными потоками»

3. http://telecomlaw.ru/studyguides/is_varfolomeev.pdf Варфоломеев А.А. «Основы информационной безопасности»

Перечень информационных технологий и программного обеспечения

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 318, Компьютерный класс кафедры информационной безопасности, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	1) IBM SPSS Statistics Premium Campus Edition. Поставщик ЗАО Прогностические решения. Договор ЭА-442-15 от 18.01.16 лот 5. Срок действия договора 30.06.2016. Лицензия бессрочно. 2) SolidWorks Campus 500. Поставщик Солид Воркс Р. Договор 15-04-101 от 23.12.2015. Срок действия договора 15.03.2016. Лицензия бессрочно. 3) АСКОН Компас 3D v17. Поставщик Навиком. Договор 15-03-53 от 20.12.2015. Срок действия договора 31.12.2015. Лицензия бессрочно. 4) MathCad Education Universety Edition. Поставщик Софт Лайн Трейд. Договор 15-03-49 от 02.12.2015. Срок действия договора 30.11.2015. Лицензия бессрочно. 5) Corel Academic Site. Поставщик Софт Лайн Трейд. Договор ЭА-442-15 от 18.01.16 лот 4. Срок действия договора 30.06.2016. Лицензия закончилась 28.01.2019. 6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18 лот 4. Срок действия договора 20.09.2018. Лицензия до 30.06.2020 7) Dallas Lock. Поставщик Конфидент. Партнерское соглашение БП-8-16/576-16-ЦЗ/1 от 23.11.2016. Срок действия договора 23.11.2019. Лицензия до 23.11.2019

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Для более эффективного освоения и усвоения материала рекомендуется ознакомиться с теоретическим материалом по той или иной теме до проведения семинарского занятия. Работу с теоретическим материалом по теме с использованием учебника или конспекта лекций можно проводить по следующей схеме:

- название темы;
- цели и задачи изучения темы;
- основные вопросы темы;
- характеристика основных понятий и определений, необходимых для усвоения данной темы;
- список рекомендуемой литературы;

– наиболее важные фрагменты текстов рекомендуемых источников, в том числе таблицы, рисунки, схемы и т.п.;

– краткие выводы, ориентирующие на определенную совокупность сведений, основных идей, ключевых положений, систему доказательств, которые необходимо усвоить.

В ходе работы над теоретическим материалом достигается:

– понимание понятийного аппарата рассматриваемой темы;

– воспроизведение фактического материала;

– раскрытие причинно-следственных, временных и других связей;

– обобщение и систематизация знаний по теме.

При подготовке к экзамену рекомендуется проработать вопросы, рассмотренные на лекционных и практических занятиях и представленные в рабочей программе, используя основную литературу, дополнительную литературу и интернет-ресурсы.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 318, Компьютерный класс кафедры информационной безопасности, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 15) Оборудование: Моноблок HPP-B0G08ES#ACB/8200E AIO i52400S 500G 4.0G 28 PC Электронная доска Poly Vision Walk-and-Talk WTL 1810 Мультимедийная аудитория: Экран проекционный ScreenLine Trim White Ice 50 см черная кайма сверху, размер рабочей области 236x147 см Документ-камера Avervision CP355AF ЖК-панель 47", Full HD, LG M4716 CCBA Мультимедийный проектор Mitsubishi EW33OU, 3000 ANSI Lumen, 1280x800 Сетевая видеокамера Multipix MP-HD718 Доска аудиторная

Приложение 1 к рабочей программе учебной дисциплины

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

по дисциплине «Основы информационной безопасности»
Направление подготовки 10.03.01 «Информационная безопасность»
Профиль подготовки - «Комплексная защита объектов информатизации»
Форма подготовки - очная

Владивосток
2019

План-график выполнения самостоятельной работы по дисциплине

I Семестр

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1	5 неделя	Реферат	13	ПР-7
2	8 неделя	Конспект	13	ПР-7
3	19 неделя	зачет	10	УО-1

II Семестр

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1	5 неделя	Тест остаточных знаний за 1 семестр	2	ПР-2
2	8 неделя	Тест	2	ПР-2
3	10 неделя	Реферат	5	ПР-7
4	19 неделя	экзамен	27	УО-1

Самостоятельная работа студентов включает:

- освоение лекционного материала;
- подготовку к контрольным работам;
- выполнение индивидуального домашнего задания;
- оформление выполненного индивидуального домашнего задания;
- подготовку к защите выполненного индивидуального домашнего задания.

В отчет по индивидуальному домашнему заданию должны входить:

1) Тема реферата (конкретное задание выдается преподавателем);
2) Основная мысль;
3) Вывод.

Самостоятельная работа студентов по дисциплине складывается из времени, необходимого для освоения лекционного материала, освоения и совершенствования навыков решения задач и времени выполнения и оформления индивидуального домашнего задания.

Приложение 2 к рабочей программе учебной дисциплины

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Основы информационной безопасности»
Направление подготовки 10.03.01 «Информационная безопасность»
Профиль подготовки - «Комплексная защита объектов информатизации»
Форма подготовки - очная

Владивосток
2019

Обучающиеся должны выполнять индивидуальные задания. Задания должны быть выполнены в процессе изучения соответствующего раздела курса. При выполнении заданий возможно использование учебно-методической литературы и электронных лекций курса.

Вопросы к зачету

1. Виды безопасности и сферы жизнедеятельности личности, общества и государства: экономическая, внутриполитическая, социальная, международная, информационная, военная, пограничная, экологическая и другие. Виды защищаемой информации.
2. Интересы общества в информационной сфере.
3. Интересы государства в информационной сфере.
4. Основные составляющие национальных интересов Российской Федерации в информационной сфере.
5. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России.
6. Угрозы информационному обеспечению государственной политики Российской Федерации.
7. Угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов.
8. Угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.
9. Внешние источники угроз. Внутренние источники угроз.

10. Направления обеспечения информационной безопасности государства.

11. Содержание информационного противоборства на межгосударственном уровне

12. Информационная безопасность и информационное противоборство.

13. Субъекты информационного противоборства.

14. Цели информационного противоборства. Составные части и методы информационного противоборства.

15. Информационное оружие, его классификация и возможности.

16. Компьютерная система как объект информационного воздействия.

17. Компьютерная система как объект информационной безопасности.

18. Методы оценки защищенности компьютерных систем от НСД.

19. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.

20. Классификация и возможности технических разведок.

Вопросы к экзамену

21. Компьютерная разведка, ее объекты и содержание.

22. Компьютерная система как объект информационной безопасности.

23. Общая характеристика методов и средств защиты информации.

24. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Общие критерии

25. Основные принципы засекречивания информации.

26. Методы формирований функций защиты.

27. Модель нарушителя информационных систем.

28. Виды угроз информационным системам.

29. Технические каналы утечки информации в АС.

30. Классы защищенности средств вычислительной техники от несанкционированного доступа.

31. Причины нарушения целостности информации.

32. Состояния и функции системы защиты информации.

33. Эмпирический подход к оценке уязвимости информации.

34. Требования к архитектуре СЗИ. Построение СЗИ.

35. Ядро системы защиты информации.

36. Требования к криптосистемам.

37. Основные алгоритмы шифрования.

38. Цифровые подписи.

39. Криптографические хэш-функции.

40. Криптографические генераторы случайных чисел.

41. Криптоанализ и атаки на криптосистемы.