Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Структурное подразделение «Институт информационных технологий и анализа данных»

УТВЕРЖДЕНА:
на заседании Совета института ИТиАД им. Е.И.Попова
Протокол №8 от 24 февраля 2025 г.

Рабочая программа дисциплины

«ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ»

Направление: 10.04.01 Информационная безопасность

Безопасность киберфизических систем

Квалификация: Магистр

Форма обучения: очная

Документ подписан простой электронной подписью Составитель программы: Маринов Александр Андреевич Дата подписания: 22.06.2025	Документ подписан простой электронной подписью Утвердил: Говорков Алексей Сергеевич Дата подписания: 23.06.2025	Документ подписан простой электронной подписью Согласовал: Маринов Александр Андреевич Дата подписания: 22.06.2025

Год набора – 2025

Иркутск, 2025 г.

1 Перечень планируемых результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы

1.1 Дисциплина «Технологии защиты информации в автоматизированных информационных системах» обеспечивает формирование следующих компетенций с учётом индикаторов их достижения

Код, наименование компетенции	Код индикатора компетенции
ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ОПК-1.2
ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ОПК-2.1
ОПК-4 Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок	ОПК-4.1
УК-2 Способен управлять проектом на всех этапах его жизненного цикла	УК-2.2
УК-6 Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	УК-6.2

1.2 В результате освоения дисциплины у обучающихся должны быть сформированы

Код индикатора	Содержание индикатора	Результат обучения
ОПК-1.2	Владеет техниками освоения новых методов, позволяющих решать профессиональные задачи, самостоятельно использовать потенциал интегрированных знаний для освоения новых областей и совершенствования уровня своей квалификационной подготовки	**Знать** методы технологий разработки программного обеспечения для использования в профессиональной деятельности. **Уметь** решать нестандартные профессиональные задачи, в том числе в новой или незнакомой среде с применением технологий разработки программного обеспечения. **Владеть** навыками: теоретического и экспериментального исследования объектов профессиональной деятельности с применением технологий разработки программного обеспечения, в том числе в новой или незнакомой среде.
ОПК-2.1	Организует и осуществляет контроль за проектированием сложных систем и комплексов	**Знать** методы технологий разработки программного обеспечения для разработки

	управления информационной безопасностью с учетом особенностей объектов защиты	оригинальных алгоритмов и программных средств, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач. **Уметь** решать нестандартные профессиональные задачи, в том числе в новой или незнакомой среде с применением технологий разработки программного обеспечения. **Владеть** навыками: теоретического и экспериментального исследования объектов профессиональной деятельности с применением технологий разработки программного обеспечения для создания оригинальных алгоритмов и программных средств, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач.
ОПК-4.1	Разрабатывает программы и методики испытаний средств и систем обеспечения информационной безопасности	**Знать** проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности **Уметь** ставить цели и находить способы ее достижения используя научное представление о результатах защиты информации. **Владеть** методиками постановки цели и способами ее достижения, научными представлениями о результатах обработки информации.
УК-2.2	Планирует необходимые ресурсы, в том числе с учетом их заменимости; разрабатывает план реализации проекта с использованием инструментов планирования; осуществляет мониторинг хода реализации проекта, корректирует отклонения, вносит дополнительные изменения в план реализации проекта, уточняет зоны ответственности участников проекта	**Знать** основные требования к представлению результатов защиты информации в АСУ. **Уметь** подготовить результаты по технической защите информации, в том числе с учетом их заменимости; разработать план реализации проекта с использованием инструментов планирования. **Владеть** навыками самоанализа и может применять технологии защиты информации в АСУ.
УК-6.2	Определяет приоритеты профессионального роста и	**Знать** планирование и организацию своей деятельности на основе

	способы совершенствования собственной деятельности на основе самооценки по выбранным критериям	приоритетов и поставленных целей. **Уметь** ставить личные цели и обоснованно определяет их приоритетность. является инициатором запросов недостающих знаний и понимает их значимость. **Владеть** вопросами организаторской деятельности участвовать в рефлексии на позиции соорганизатора.

2 Место дисциплины в структуре ООП

Изучение дисциплины «Технологии защиты информации в автоматизированных информационных системах» базируется на результатах освоения следующих дисциплин/практик: «Управление информационной безопасностью», «Защита персональных данных при обработке в автоматизированных информационных системах», «Технологии обеспечения информационной безопасности объектов»

Дисциплина является предшествующей для дисциплин/практик: «Защита объектов критической информационной инфраструктуры», «Системы менеджмента информационной безопасности», «Математическое моделирование объектов и систем»

3 Объем дисциплины

Объем дисциплины составляет – 5 ЗЕТ

Вид учебной работы	**Трудоемкость в академических часах** (Один академический час соответствует 45 минутам астрономического часа)	
	Всего	Семестр № 2
Общая трудоемкость дисциплины	180	180
Аудиторные занятия, в том числе:	104	104
лекции	52	52
лабораторные работы	0	0
практические/семинарские занятия	52	52
Самостоятельная работа (в т.ч. курсовое проектирование)	40	40
Трудоемкость промежуточной аттестации	36	36
Вид промежуточной аттестации (итогового контроля по дисциплине)	Экзамен	Экзамен

4 Структура и содержание дисциплины

4.1 Сводные данные по содержанию дисциплины

Семестр № 2

№ п/п	**Наименование раздела и темы дисциплины**	**Виды контактной работы**						СРС		**Форма текущего контроля**
		Лекции		ЛР		ПЗ(СЕМ)				
		№	Кол.	№	Кол.	№	Кол.	№	Кол.	

			Час.		Час.		Час.		Час.	
1	2	3	4	5	6	7	8	9	10	11
1	Законодательные меры информационной безопасности	1	5			1	5	1	4	Устный опрос
2	Организационные меры информационной безопасности автоматизированных систем	2	5			2	5	1	3	
3	Сопровождение мер информационной безопасности автоматизированных систем	3	5			3	5			Устный опрос
4	Аппаратно-техническое обеспечение информационной безопасности	4	5			4	5	2	5	Устный опрос
5	Техническая разведка и противодействие	5	5			5	5	1	5	Устный опрос
6	Программные методы защиты информации	6	4			6	4	2	6	Устный опрос
7	Типовые хакерские атаки и противодействие	7	5			7	5	3	6	Устный опрос
8	Вирусные атаки и их нейтрализация	8	4			8	4	1	6	Доклад
9	Криптографические методы защиты	9	5			9	5			Устный опрос
10	Программно-аппаратная защита сетей в автоматизированных информационных системах	10	4			10	4			Устный опрос
11	Комплексное обеспечение информационной безопасности в автоматизированных информационных системах	11	5			11	5	3	5	Устный опрос
	Промежуточная аттестация								36	Экзамен
	Всего		52				52		76	

4.2 **Краткое содержание разделов и тем занятий**

Семестр № 2

№	Тема	Краткое содержание
1	Законодательные меры информационной безопасности	В информационной сфере основу информационной безопасности составляют нормы Конституции РФ о праве каждого на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени (ч. 1 ст. 23), а также на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ч. 2 ст. 23). Конституция РФ провозглашает недопустимость разглашения информации, которой обмениваются между собой люди. Вся эта информация не должна подвергаться цензуре. Работники организаций, обслуживающие каналы коммуникаций, должностные и иные официальные лица (следователи, понятые, присутствующие при выемке корреспонденции, и т.п.) Несут ответственность за разглашение содержания корреспонденций. Нормативно-законодательная база информационной безопасности является частью всего комплекса информационной безопасности. В состав этой базы входит весь комплекс нормативно-технических и нормативно-методических документов по защите информации. Различают: - Законодательные акты или законы РФ; - Постановления Правительства РФ; - Доктрины Российской Федерации в области защиты информации; - Нормативно-методические документы по защите информации; - Документы уполномоченных федеральных органов; - Национальные стандарты в области защиты информации; - Международные стандарты в области защиты информации; - Международные соглашения в области защиты информации. Рассмотрим наиболее важнейшие из них. Как было указано ранее, первая составляющая государственных интересов в информационной сфере включает в себя обеспечение конституционных прав и свобод гражданина в области получения информации и пользования ею.
2	Организационные меры информационной безопасности автоматизированных систем	Организационные меры являются той основой, которая объединяет различные меры защиты в единую систему. Достижение высокого уровня безопасности невозможно без принятия должных организационных мер. С одной стороны, эти меры

		должны быть направлены на обеспечение правильности функционирования механизмов защиты и выполняться администратором безопасности системы. С другой стороны, руководство организации, эксплуатирующей средства автоматизации, должно регламентировать правила автоматизированной обработки информации, включая и правила ее защиты, а также установить меру ответственности за нарушение этих правил. Организационное обеспечение заключается в регламентации взаимоотношений исполнителей на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к информации становится невозможным или будет существенно затруднен за счет проведения организационных мероприятий. К основным организационным и режимным мероприятиям относятся: - Привлечение к проведению работ по защите информации организаций, имеющих лицензию на деятельность в области защиты информации, выданную соответствующими органами; - Категорирование и аттестация объектов технических средств передачи информации (ТСПИ) и выделенных для проведения закрытых мероприятий помещений (далее выделенных помещений) по выполнению Требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности; - Использование на объекте сертифицированных ТСПИ и вспомогательных технических средств и систем (ВТСС); - Установление контролируемой зоны вокруг объекта; - Привлечение к работам по строительству, реконструкции объектов ТСПИ, монтажу аппаратуры организаций, имеющих лицензию на деятельность в области защиты информации по соответствующим пунктам; - Организация контроля и ограничение доступа на объекты ТСПИ и В выделенные помещения; - Введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите.
3	Сопровождение мер	Сопровождение мер информационной безопасности автоматизированных систем

	информационной безопасности автоматизированных систем	включает: - Мониторинг и аудит. Сбор и анализ информации о событиях в системе для выявления подозрительной активности и потенциальных угроз. - Обучение персонала. Проведение тренингов и семинаров по вопросам информационной безопасности для сотрудников, работающих с системой. - Использование технических средств защиты. Например, антивирусов, систем обнаружения вторжений, шифрования данных. - Физическую защиту. Ограничение доступа к оборудованию и компонентам системы с помощью ограждений, систем контроля доступа и видеонаблюдения.
4	Аппаратно-техническое обеспечение информационной безопасности	Под аппаратными средствами защиты понимаются специальные средства, непосредственно входящие в состав технического обеспечения и выполняющие функции защиты как самостоятельно, так и в комплексе с другими средствами, например с программными. Можно выделить некоторые наиболее важные элементы аппаратной защиты: 1) Защита от сбоев в электропитании; 2) Защита от сбоев серверов, рабочих станций и локальных компьютеров, сетевых карт и т.д.; 3) Защита от сбоев дисковых систем, устройств для хранения информации; 4) Защита от утечек информации, несанкционированного доступа.
5	Техническая разведка и противодействие	Одним из важных средств добывания информации является техническая разведка, проводимая с помощью разнообразных специальных технических устройств. Вид применяемых технических средств разведки зависит, прежде всего, от физической природы и особенностей демаскирующих признаков объектов, являющихся источниками информации. По используемым техническим средствам в технической разведке Различают следующие основные виды разведки: - Оптико-электронную; - Радиоэлектронную; - Электромагнитную; - Компьютерную; - Гидроакустическую. Оптико-электронная разведка – это разведка с помощью видеосистем и оптических систем с электронными схемами обработки полученных изображений.

		Радиоэлектронная разведка − это процесс получения информации в результате приема и анализа электромагнитных излучений (ЭМИ) радиодиапазона, создаваемых работающими радиоэлектронными средствами (РЭС). Такая разведка в частности активно использовалась в Великую отечественную войну. Радисты прослушивали эфир, запоминали почерк работы радистов «противника» и по их исчезновению или появлению устанавливали передислокацию сил противника.
6	Программные методы защиты информации	Программная защита информации сводится к созданию компьютерных программ, которые ограничивают доступ к информации, следят за её сохранностью и конфиденциальностью. Все программное обеспечение, установленное на компьютерном оборудовании предприятия, является собственностью и должно использоваться исключительно в производственных целях, поэтому сотрудникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их производственной деятельности. Если в ходе выполнения технического обслуживания будет обнаружено не разрешенное к установке программное обеспечение, то оно должно быть удалено, а сообщение о нарушении направлено руководителю сотрудника и в отдел защиты информации. Все компьютеры, подключенные к корпоративной сети, должны быть оснащены системой антивирусной защиты, утвержденной руководителем. Сотрудники не должны: - блокировать антивирусноепрограммное обеспечение; - устанавливать другоеантивирусное программное обеспечение; - изменять настройки и конфигурацию антивирусного программного обеспечения.
7	Типовые хакерские атаки и противодействие	В целом хакером предпочтительно именовать лицо, стремящееся обойти защиту компьютерной системы вне зависимости от того, преследуются по закону его действия или нет. Статистика компьютерных преступлений свидетельствует о том, что уровень профессиональной подготовки хакера отличается удивительным разнообразием. Им может стать

		обычный школьник, случайно обнаруживший программу взлома на одном из специализированных хакерских серверов в Internet. В то же время отмечено и появление настоящих хакерских «сообществ», лидерами которых являются компьютерные специалисты высочайшей квалификации. Хакерская атака – это попытка использовать несовершенство системы безопасности жертвы для получения информации или для нанесения вреда системе. Причиной любой удачной хакерской атаки является недостаточная компетенция администратора системы безопасности в частности, несовершенство программного обеспечения и слабое внимание к вопросам безопасности организации или пользователя в целом.
8	Вирусные атаки и их нейтрализация	Вирусные атаки осуществляются с помощью компьютерных вирусов (КВ). Компьютерными вирусами называются саморазмножающиеся программы, созданные для разрушения логической структуры ПК, уничтожения его программного обеспечения, создания помех или полной блокировки работы ПК, а также для несанкционированного съёма (воровства) информации. Основными путями проникновения вирусов в ПК являются съемные диски, переносные жесткие диски, которые используются для переноса большого объема с ПК на другой лазерный диск и компьютерные сети. Если вирус попал в ПК, то важно быстро его обнаружить (один из принципов – чем раньше болезнь выявлена, тем легче лечить).
9	Криптографические методы защиты	Криптографические методы защиты информации – это специальные методы шифрования, кодирования или иного преобразования информации, в результате которых ее содержание становится недоступным без предъявления ключа криптограммы и обратного преобразования. Криптографический метод защиты, безусловно, самый надежный метод защиты, так как охраняется непосредственно сама информация, а Не доступ к ней (например, зашифрованный файл нельзя прочесть даже в случае кражи носителя). Данный метод защиты реализуется в виде программ или пакетов программ. Шифрование – преобразовательныйпроцесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом. Дешифрование

		– обратный шифрованию процесс, на основе ключа шифрованный текст преобразуется в исходный. Ключ – информация, необходимая для беспрепятственного шифрования и дешифрования текстов. Шифрование данных может осуществляться в режимах On-line (в темпе поступления информации) и Off-line (автономном).
10	Программно-аппаратная защита сетей в автоматизированных информационных системах	Работа с сетью налагает свои особенности программной безопасности, поскольку именно через коммуникации сетей происходит наибольшее число вирусных хакерских атак. Для начала необходимо привести краткую справку, которая может понадобиться для понимания данного материала тем, кто не знаком с сетевыми технологиями. Те, кто знаком с ними, могут пропустить эту часть, потому что всё дано только в базовых понятиях без технических деталей вся информация в сети передаётся пакетами, т.е. "порциями". У пакета есть адрес отправителя, получателя, порт отправителя и порт получателя, а также некоторые другие служебные данные. пакеты могут быть фрагментированы, т.е. один пакет может быть разбит на несколько фрагментов и отправлен в таком виде. Информация о фрагментации добавляется к служебной, поэтому компьютер-получатель знает, как правильно собрать фрагменты в один пакет. Для понимания материала укажем три типа пакета: TCP; UDP; ICMP. Связь между двумя компьютерами в модели клиент-сервер: клиент посылает серверу на открытый порт SYN-пакет (т.е. Пакет, у которого установлен флаг SYN), на что сервер отвечает SYN/ACK-пакетом (в том случае, если он готов установить соединение), после этого клиент посылает ACK-пакет, и связь считается установленной. Это элементарная модель, которая может понадобиться для понятия некоторых атак, за более подробной информацией нужно обратиться к справочнику по сетевым технологиям.
11	Комплексное обеспечение информационной безопасности в автоматизированных информационных системах	В последние годы на смену полусистемному приходит комплексный подход к организации защиты информации. Для этого подхода характерен взгляд на защиту информации как на непрерывный процесс, осуществляемый на всех этапах жизненного цикла автоматизированных систем с помощью использования всех имеющихся средств защиты, причем все

		используемые средства и методы объединены в единую систему, одной из основ функционирования которой является созданная на этом этапе нормативно-правовая база защиты информации. К указанным средствам относятся законы, стандарты и другие нормативно- правовые акты, регламентирующие правила обращения с защищаемой информацией и являющиеся обязательными для соблюдения. Расширяется типизация и стандартизация проектных решений, стремление к аппаратной реализации функций защиты, переход на поточно-индустриальные принципы производства и использования. Отчетливо просматривается тенденция выработки и реализации концепции защиты, направленной на решение трех классов задач – задач анализа, синтеза и управления. Задача анализа заключается в объективной оценке потенциальных угроз информации и возможного ущерба от их проявления. Задачи синтеза – определение наиболее эффективных форм и способов организации механизмов защиты. Задачей управления является обеспечение рационального использования созданных механизмов защиты в процессе обработки защищаемой информации.

4.3 Перечень лабораторных работ

Лабораторных работ не предусмотрено

4.4 Перечень практических занятий

Семестр № 2

№	Темы практических (семинарских) занятий	Кол-во академических часов
1	Законодательные меры информационной безопасности	5
2	Организационные меры информационной безопасности автоматизированных систем	5
3	Сопровождение мер информационной безопасности автоматизированных систем	5
4	Аппаратно-техническое обеспечение информационной безопасности	5
5	Техническая разведка и противодействие	5
6	Программные методы защиты информации	4
7	Типовые хакерские атаки и противодействие	5
8	Вирусные атаки и их нейтрализация	4
9	Криптографические методы защиты	5
10	Программно-аппаратная защита сетей в автоматизированных информационных системах	4

11	Комплексное обеспечение информационной безопасности в автоматизированных информационных системах	5

4.5 Самостоятельная работа

Семестр № 2

№	Вид СРС	Кол-во академических часов
1	Подготовка к практическим занятиям (лабораторным работам)	18
2	Расчетно-графические и аналогичные работы	11
3	Решение специальных задач	11

В ходе проведения занятий по дисциплине используются следующие интерактивные методы обучения: интерактивные лекции, групповая дискуссия

5 Перечень учебно-методического обеспечения дисциплины

5.1 Методические указания для обучающихся по освоению дисциплины

5.1.1 Методические указания для обучающихся по практическим занятиям

https://el.istu.edu/course/view.php?id=6885

5.1.2 Методические указания для обучающихся по самостоятельной работе:

https://el.istu.edu/course/view.php?id=6885

6 Фонд оценочных средств для контроля текущей успеваемости и проведения промежуточной аттестации по дисциплине

6.1 Оценочные средства для проведения текущего контроля

6.1.1 семестр 2 | Устный опрос

Описание процедуры.

Проведение устного опроса в форме «вопрос-ответ»

Критерии оценивания.

ответ раскрыт полностью 8-10 баллов
ответ раскрыт частично 4-7 баллов
имеет только общее представление о проблеме 2-4 баллов
не ответил – 0 баллов

6.1.2 семестр 2 | Доклад

Описание процедуры.

Публичное выступление по теме доклада с использованием презентации.

Критерии оценивания.

Оценка доклада определяется следующими критериями:
формулировка цели и задач проекта – 30 б.;----
качество анализа и обоснование выводов по теме проекта – 30 б.;
логика и структура презентации доклада – 20 б.;
качество оформления презентации – 10 б.;
организация речи докладчика – 10 б.
Критерии оценки за доклад определяются по числу баллов за защиту выпускной аттестационной работы:----
менее 54 б. – неудовлетворительно;
от 55%-74 б. – удовлетворительно;
от 75%-84 б. – хорошо;
от 85% -100 б. – отлично

6.2 Оценочные средства для проведения промежуточной аттестации

6.2.1 Критерии и средства (методы) оценивания индикаторов достижения компетенции в рамках промежуточной аттестации

Индикатор достижения компетенции	**Критерии оценивания**	**Средства (методы) оценивания промежуточной аттестации**
ОПК-1.2	1. Разрабатывает этапы решения поставленной задачи, выделяя ее основные составляющие. 2. Производит разбор задачи с указанием этапов и конечных целей используя новые методы (обработки и защиты информации), позволяющие решать профессиональные задачи. 3. Анализирует пути решения задачи с их оценкой и критическим анализом недостатков и достоинств.	Устное собеседование по теоретическим вопросам и/или выполнение практических заданий.
ОПК-2.1	Способен продемонстрировать специализированные знания в области проектирования сложных систем государственных система защиты информации (ГИС); объектов КИИ; область применения проектируемой системы ИБ.	Опрос, собеседование, практикоориентированные задания, тесты письменные и/или компьютерные, дискуссия
ОПК-4.1	Способен продемонстрировать специализированные знания в области разработки систем обеспечения информационной безопасности: программ и методик испытаний информационных систем	Устное собеседование по теоретическим вопросам и индивидуальные практические задания, дискуссия.
УК-2.2	1. Разрабатывает этапы решения защиты информации.	Устное собеседование по

	2. Производит разбор задачи с указанием этапов и конечных целей защиты информации в автоматизированных информационных системах.	теоретическим вопросам и индивидуальные практические задания.
УК-6.2	Эффективно планирует и организует свою деятельность. Ставит личные цели и обоснованно определяет их приоритетность. Является инициатором запросов недостающих знаний и понимает их значимость. Участвует в рефлексии на позиции соорганизатора.	Устное собеседование по теоретическим вопросам и индивидуальные практические задания. Вид промежуточной аттестации – экзамен.

6.2.2 Типовые оценочные средства промежуточной аттестации

6.2.2.1 Семестр 2, Типовые оценочные средства для проведения экзамена по дисциплине

6.2.2.1.1 Описание процедуры

1) Экзамен по дисциплине проводится согласно расписанию в назначенной аудитории, в которую приглашается к установленному началу экзамена группа студентов.
2) К экзамену допускаются студенты, которые выполнили все предусмотренные работы по освоению курса: сданы практические работы по выбранной теме.
3) Каждый студент из числа допущенных выбирает один билет и готовится к ответу в течение не менее 30 - 45 минут письменно на поставленные три вопроса в билете.
Экзамен проводится в форме устного опроса по экзаменационным билетам.
1. Криптографические системы и их использование в VipNet. ПО VipNet. Понятие прикладной и адресной администрации.
2. Современные технологии виртуализации. Технологии защиты в виртуальных средах.
3. Аппаратные ключи защиты серии HASP
4. Использование программно-аппаратных средств для защиты ПО
5. Виртуальные защищенные сети: виды, характеристики и варианты реализации.
6. Виды угроз информационной безопасности в телекоммуникационных системах.
7. Использование аппаратных ключей защиты eToken и HASP для защиты ПО и информации пользователей.
8. Методы, способы и средства защиты информации
9. Защита программного обеспечения с помощью аппаратных ключей серии Guardant.
10. Электронные цифровые сертификаты. Принцип работы. Формальное описание. Структура сертификата. Российские стандарты.
11. Электронный ключ (аппаратный ключ). Принципы работы, классификация, примеры использования.
12. Семейство электронных ключей Guardant для защиты программного обеспечения от несанкционированного копирования и распространения.
13. Защита программного обеспечения — общие подходы и принципы.
14. Аутентификация, авторизация, идентификация.
15. Центры сертификации – назначение, техническая реализация.

16. Основы информационной безопасности. Персональные данные. Законодательство в области защиты персональных данных.
17. Персональные данные. Законодательство в области защиты персональных данных. Модель угроз ПД. Организационно-распорядительная документация по защите ПД.
18. История компьютерных вирусов. Классификация вирусов.
19. Основные признаки присутствия на компьютере вредоносных программ. Методы защиты от вредоносных программ.
20. Антивирусная защита компьютерной сети. Классификация антивирусов.
21. Институты сертификата ключа электронной цифровой подписи и владельца сертификата.
22. Институт удостоверяющих центров.
23. Особенности использования электронной цифровой подписи.
24. Законодательство Российской Федерации о техническом регулировании.
25. Подсистема защиты каналов передачи данных.
26. Защита прав и законных интересов субъектов информационной сферы.
27. Классы угроз информационной безопасности.
28. Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти.
29. Административный уровень обеспечения информационной безопасности.
30. Организационные структуры системы обеспечения информационной безопасности предприятия (организации).
31. Корпоративная нормативная база по защите информации.
32. Комплексная система защиты информации.
33. Организация пропускного режима на предприятии (организации).
34. Методы разграничения доступа.
35. Мандатное и дискретное управление доступом.
36. Режим секретности и конфиденциального делопроизводства.
37. Технология SPAN (Switch Port Analyzer).
38. Защита информации при проведении совещаний и переговоров.
39. Защита информации при работе с посетителями.
40. Основные подсистемы программно-технической реализации комплексной защиты информации.
41. Нормативно-методические документы по обеспечению безопасности информации.
42. Защита беспроводных сетей Wi-Fi.
43. Анализ сетевого трафика снифером Ethereal.
44. Подделка аппаратного адреса (MAC spoofing).
45. Подбор и расстановка кадров.
46. Мотивация добросовестной деятельности сотрудников.
47. Порядок проведения служебных расследований.
48. Организация подготовки кадров и повышения квалификации в области обеспечения информационной безопасности.
49. Взлом криптозащиты.
50. Общие положения по категорированию объектов информатизации.
51. Порядок проведения категорирования объектов на предприятий.
52. Классификация автоматизированных систем в составе объектов вычислительной техники.
53. Правовые основы лицензирования.
54. Основные понятия и принципы лицензирования.
55. Общие положения по организации лицензирования.
56. Государственная система лицензирования.
57. Система лицензирования деятельности в области защиты государственной тайны.

58. Правовые основы сертификации и аттестации средств защиты информации.
59. Основные направления и этапы работ по созданию комплексной системы безопасности.
60. Организация и проведение сертификации.
61. Принцип комплексного подхода к обеспечению информационной безопасности.
62. Комплексное обеспечение информационной безопасности.

Пример задания:

1. Классы угроз информационной безопасности.
2. Подделка аппаратного адреса (MAC spoofing).

6.2.2.1.2 Критерии оценивания

Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
Уверенно и без ошибок отвечает на все вопросы билета	Допускает незначительные ошибки в ответе на один из вопросов, включая дополнительные по результатам собеседования	Знает ответы на два вопроса или допускает ошибки в ответах на вопросы	Не отвечает на два и более вопросов

7 Основная учебная литература

1. Емельянова Н. З. Основы построения автоматизированных информационных систем : учебное пособие для среднего профессионального образования / Н. З. Емельянова, Т. Л. Партыка, И. И. Попов, 2007. - 416.

2. Грибунин В. Г. Комплексная система защиты информации на предприятии : учебное пособие для вузов по специальностям "Организация и технология защиты информации" / В. Г. Грибунин, 2009. - 411.

8 Дополнительная учебная литература и справочная

1. Математические методы в автоматизированных информационных системах и банках данных : сб. науч. тр. / АН УССР, Ин-т кибернетики им. В. М. Глушкова, 1985. - 80.

2. Основы построения автоматизированных информационно-управляющих систем в области метрологического обеспечения управления качеством : сб. науч. тр. / ВНИИ метрологии измер. и упр. систем, 1987. - 93.

3. Методы повышения эффективности и качества функционирования автоматизированных информационно-управляющих систем / В. В. Кульба, С. С. Ковалевский, И. А. Горгидзе и др., 2001. - 343.

9 Ресурсы сети Интернет

1. http://library.istu.edu/
2. https://e.lanbook.com/

10 Профессиональные базы данных

1. http://new.fips.ru/
2. http://www1.fips.ru/

11 Перечень информационных технологий, лицензионных и свободно распространяемых специализированных программных средств, информационных справочных систем

1. Свободно распространяемое программное обеспечение Microsoft Windows Seven Professional (Microsoft Windows Seven Starter) - Seven, Vista, XP_prof_64, XP_prof_32 - поставка 2010

2. Свободно распространяемое программное обеспечение Microsoft Windows Seven Professional [1x100] RUS (проведен апгрейд с Microsoft Windows Seven Starter [1x100]) - поставка 2010

3. Свободно распространяемое программное обеспечение Microsoft Windows Server Standard 2008 R2 Russian Academic OPEN 1 License No Level

12 Материально-техническое обеспечение дисциплины

1. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

2. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

3. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

4. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

5. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

6. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

7. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

8. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

9. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

10. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

11. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

12. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

13. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

14. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

15. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

16. МФУ FS-1128 MFP