Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯИ РАДИОЭЛЕКТРОНИКИ» (ТУСУР)

Кафедра комплексной информационной безопасности
электронно- вычислительных систем (КИБЭВС)

Методические указания к программе

государственного экзамена по специальности 10.05.03
«Информационная безопасность автоматизированных систем»,
специализация «Информационная безопасность автоматизированных банковских систем»

2017

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯИ РАДИОЭЛЕКТРОНИКИ» (ТУСУР)

Кафедра комплексной информационной безопасности
электронно- вычислительных систем (КИБЭВС)

Методические указания к программе государственного экзамена по специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Информационная безопасность автоматизированных банковских систем»

2017

1. Общие положения

Итоговая государственная аттестация выпускников программы подготовки специалиста по направлению «Информационная безопасность» специальность 10.05.03 «Информационная безопасность автоматизированных систем», проводится в соответствии с Федеральным государственным образовательным стандартом высшего профессионального образования, и завершается выдачей диплома установленного образца об уровне образования и квалификации.

Итоговые аттестационные испытания включают государственный экзамен и защиту выпускной квалификационной работы.

Программы государственного экзамена по направлению (специальности) подготовки и критерии оценки выпускных квалификационных работ утверждаются высшим учебным заведением с учетом рекомендаций учебно-методических объединений вузов.

Итоговые аттестационные испытания (госэкзамен и защита выпускной квалификационной работы) не могут быть заменены оценками качества освоения образовательных программ на основании текущего контроля успеваемости (рейтинга) и промежуточной аттестации студента.

Государственную аттестацию проводит государственная экзаменационная комиссия (ГЭК), председателем которой утверждается, как правило, лицо, не работающее в данном вузе из числа докторов наук, профессоров соответствующего профиля или крупных специалистов предприятий, организаций, учреждений, являющихся потребителями кадров данного профиля. Государственные экзаменационные комиссии действуют в течение одного календарного года.

Порядок проведения государственных аттестационных испытаний разрабатывается вузом и доводится до сведения студентов не позднее, чем за месяц до начала итоговой государственной аттестации. Студенты должны быть обеспечены программой госэкзамена, необходимыми условиями для подготовки и консультациями.

В государственную экзаменационную комиссию представляются следующие документы: приказ о составе ГЭК, приказ о допуске студентов к государственному экзамену, программа экзамена, экзаменационные билеты, оформленные зачетные книжки студентов, книга протоколов заседаний государственной экзаменационной комиссии по приему государственных экзаменов.

Государственный экзамен проводится с целью проверки уровня и качества подготовки выпускников и имеет целью оценить теоретическую подготовку, практические навыки и умения, а также готовность выпускника к следующим видам профессиональной деятельности:

- научно-исследовательская;
- проектно-конструкторская;

– контрольно-аналитическая;
– организационно-управленческая;
– эксплуатационная.

Государственный итоговый междисциплинарный экзамен нацелен на проверку у обучающегося овладение следующими общекультурными компетенциями:

способностью использовать основы философских знаний для формирования мировоззренческой позиции (ОК-1);

способностью использовать основы экономических знаний в различных сферах деятельности (ОК-2);

способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма (ОК-3);

способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4);

способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5);

способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6);

способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности (ОК-7);

способностью к самоорганизации и самообразованию (ОК-8);

способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности (ОК-9).

Общепрофессиональными компетенциями:

способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач (ОПК-1);

способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники (ОПК-2);

способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности (ОПК-3);

способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах (ОПК-4);

способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-5);

способностью применять нормативные правовые акты в профессиональной деятельности (ОПК-6);

способностью применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций (ОПК-7);

способностью к освоению новых образцов программных, технических средств и информационных технологий (ОПК-8).

Профессиональными компетенциями:

способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке (ПК-1);

способностью создавать и исследовать модели автоматизированных систем (ПК-2);

способностью проводить анализ защищенности автоматизированных систем (ПК-3);

способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4);

способностью проводить анализ рисков информационной безопасности автоматизированной системы (ПК-5);

способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности (ПК-6);

способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-7);

способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-8);

способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-9);

способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-10);

способностью разрабатывать политику информационной безопасности автоматизированной системы (ПК-11);

способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-12);

способностью участвовать в проектировании средств защиты информации автоматизированной системы (ПК-13);

способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14);

способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем (ПК-15);

способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации (ПК-16);

способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17);

способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности (ПК-18);

способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-19);

способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20);

способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21);

способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22);

способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-23);

способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24);

способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25);

способностью администрировать подсистему информационной безопасности автоматизированной системы (ПК-26);

способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27);

способностью управлять информационной безопасностью автоматизированной системы (ПК-28).

способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности автоматизированных банковских систем (ПСК-5.1);

способностью разрабатывать и реализовывать политики информационной безопасности автоматизированных банковских систем (ПСК-5.2);

способностью участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью автоматизированных банковских систем (ПСК-5.3);

способностью участвовать в организации и проведении контроля обеспечения информационной безопасности автоматизированных банковских систем (ПСК-5.4);

способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной банковской системы (ПСК-5.5).

Компетенции оцениваются в соответствии со следующей шкалой:

отлично - компетенция освоена полностью на профессиональном уровне;

хорошо – компетенция освоена частично, на продвинутом уровне;

удовлетворительно – компетенция освоена частично, на базовом уровне;

неудовлетворительно – компетенция не освоена.

Трудоемкость итоговой государственной аттестации составляет 9 зачетных единиц. Время проведения государственного экзамена определено календарным графиком учебного процесса и проводится в 9 семестре очной формы обучения. На проведение государственного экзамена отведено 3 зачетные единицы.

В ходе государственного экзамена студент должен продемонстрировать знание теоретических основ основных учебных дисциплин, входящих в основную образовательную программу по направлению 10.05.03 «Информационная безопасность автоматизированных систем», понимание междисциплинарных связей между основными профессиональными дисциплинами основной образовательной программы.

2. Порядок проведения государственного экзамена.

Государственный экзамен по направлению Информационная безопасность, специальность 10.05.03 – «Информационная безопасность автоматизированных систем: поводится в два этапа: письменный этап и устный этап.

В день государственного экзамена в 9-00 студенты получают билет для выполнения письменного этапа. В билете два задания. На выполнение заданий письменного этапа отводиться 4 академических часа. Студентам предос-

тавляется рабочее место и ЭВМ в учебном классе. По необходимости разрешается выход из аудитории, разрешается пользоваться любой литературой.

Для сдающих экзамен, открывается доступ к разделу государственный экзамен в единой образовательной среде MOODLe для «выкладывания решений». Доступ к разделу закрывается в 12-20.

Начиная с 12 - 20 до 14 - 00 члены комиссии проводят проверку решений в системе MOODLe.

Защита письменного этапа назначается на 14 - 00 в тот же день. Для защиты письменного задания отводится не более 30 минут для каждого студента. По ходу защиты задаются вопросы, подтверждающие овладение соответствующими компетенциями.

На заключительном этапе защиты студенту задаются дополнительные вопросы из списка. Вопросы, предоставляются студентам заранее.

После защиты всех работ студентами, объявляется закрытое заседание государственной экзаменационной комиссии для подведения итогов освоения компетенций и выставления оценок.

3. Требования к письменному и устному этапам государственного экзамена

3.1 Требования к письменному этапу

В ответе на первое задание билета студент должен показать знания, умения и навыки, освоенные в дисциплинах: **«Разработка и эксплуатация защищенных автоматизированных систем», «Программно-аппаратные средства обеспечения информационной безопасности», «Управление средствами защиты информации», «Организационное и правовое обеспечение информационной безопасности».**

В отчете по первому заданию следует обратить внимание на:

- определение основных законодательных требований к ведению деятельности организации, связанные с обеспечением информационной безопасности. Особое внимание уделить вопросам лицензирования и сертификации;
- выбор средств защиты информации (провести анализ с объяснением причины выбора);
- список нормативно-правовых актов, применяемых в области деятельности организации.

Второе задание связано с дисциплинами: **«Основы программирования», «Безопасность программного обеспечения», «Безопасность систем баз данных», «Технологии и методы программирования».**

При подготовке к решению второго задания необходимо проработать вопросы, связанные с:

- реляционными моделями баз данных, проектированием реляционной базы данных, нормализацией структуры базы данных, безопасностью баз данных;

- объектно-ориентированным анализом и проектированием;

- функциональным тестированием программного обеспечения, процедурным программированием, рекурсивными функциями;

- видами и способами представления алгоритмов, процедурным программированием, функциями, рекурсивными функциями.

Письменное задание должно быть оформлено с использованием текстового редактора в соответствии с ОС ТУСУР 01-2013 г. http://www.tusur.ru/export/sites/ru.tusur.new/ru/education/documents/inside/tech_01-2013_new.pdf.

Письменное задание направлено на выявления способностей по следующим компетенциям:

способностью использовать языки, системы и инструментальные средства программирования в профессиональной деятельности (ОПК-3);

способностью разрабатывать и исследовать модели автоматизированных систем (ПК-2);.

способностью проводить синтез и анализ проектных решений по обеспечению информационной безопасности автоматизированных банковских систем (ПК-8).

способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-19);

способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20);

способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21);

способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22);

способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-23);

способностью управлять информационной безопасностью автоматизированной системы (ПК-28).

В письменном задании студенты должны дополнительно показать освоение следующих компетенций:

№	Номер	Компетенция	Примечание
1.	ОПК-5	способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами.	Необходимо обосновать решение в письменном задании в соответствии с общенаучными методами эмпирического, теоретического, общелогические познания

	ПК-1	способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке	Обосновать применение соответствующего физико-математического аппарата
	ПК-6	способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	Необходимо обосновать решение в письменном задании в соответствии с методами: анализ; синтез; сравнение; абстрагирование; конкретизация; обобщение; формализация; индукция; дедукция; идеализация; аналогия; моделирование; мысленный эксперимент; воображение.
	ПК-7	способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	Правильно оформленное письменное задание в соответствии с ГОСТ 34.XXX, 19.XXX

Для защиты письменного задания отводится не более 20 минут. По ходу защиты задаются вопросы, в соответствии с решенными задачами письменного этапа и подтверждающие степень овладения компетенциями:

способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4);

способностью проводить анализ рисков информационной безопасности автоматизированной системы (ПК-5);

способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14);

способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем (ПК-15);

способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации (ПК-16);

способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17);

способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25);

способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27);

способностью участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью автоматизированных банковских систем (ПСК-5.3);

способностью участвовать в организации и проведении контроля обеспечения информационной безопасности автоматизированных банковских систем (ПСК-5.4).

Список источников

1) Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных";

2) Постановление Правительства РФ от 01.11.2012 N1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";

3) Приказ ФСТЭК России от 18.02.2013 N 21 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных";

4) Приказ ФСБ России от 10 июля 2014 г. N 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности";

5) Приказ ФСТЭК России от 11.02.2013 N17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах";

6) Государственный реестр сертифицированных средств защиты информации ;

7) Федеральный закон от 04.05.2011 N 99-ФЗ "О лицензировании отдельных видов деятельности";

8) Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации";

9) Федеральный закон от 06.04.2011 N 63-ФЗ "Об электронной подписи" ;

10) Федеральный закон от 02.12.1990 N 395-1 "О банках и банковской деятельности";

11) Инструкция Банка России от 02.04.2010 N 135-И "О порядке принятия Банком России решения о государственной регистрации кредитных организаций и выдаче лицензий на осуществление банковских операций";

12) Положение ЦБР от 9 июня 2005 г. N 271-П "О рассмотрении доку-

ментов, представляемых в территориальное учреждение Банка России для принятия решения о государственной регистрации кредитных организаций, выдаче лицензий на осуществление банковских операций" ;

13) Постановление Правительства РФ от 16.04.2012 N 313 "Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)";

14) Приказ ФСБ РФ от 09.02.2005 N 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)";

15) Федеральный закон от 07.07.2003 N 126-ФЗ "О связи";

16) Постановление Правительства РФ от 16.03.2009 N 228 "О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций" (вместе с "Положением о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций");

17) Постановление Правительства РФ от 03.02.2012 N 79 "О лицензировании деятельности по технической защите конфиденциальной информации";

18) Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.;

19) Федеральный закон от 29.07.2004 N 98-ФЗ (ред. от 12.03.2014) "О коммерческой тайне";

20) Базы данных : Учебное пособие / Е. М. Давыдова, Н. А. Новгородова ; Федеральное агентство по образованию, Томский государственный университет систем управления и радиоэлектроники, Кафедра комплексной информационной безопасности электронно-вычислительных систем. - Томск : ТУСУР, 2005. - 127 с. : ил. - Библиогр.: с. 114;

21) Ларман Крэг. Применение UML и шаблонов проектирования. Введение в объектно-ориентированный анализ и проектирование. Пер. с англ.: Уч. Пос. — М: Издательский дом “Вильямс”, 2001. — 496 с.: ил;

22). Основы программирования на языке С++ : учебное пособие / В. Н. Кирнос ; Федеральное агентство по образованию, Томский государственный

университет систем управления и радиоэлектроники, Кафедра комплексной информационной безопасности электронно-вычислительных систем. - 2-е изд., перераб. и доп. - Томск : В-Спектр, 2007. - 129[1] с. : ил. - Библиогр.: с. 109;

23) Практическая отладка в C++ : пер. с англ. / А. Р. Форд, Т. Дж. Теори. - М. : КУДИЦ-ОБРАЗ, 2002. - 140[4] с. : ил. - Загл. обл. : Практика отладки в C++. - Библиогр.: с. 141. - ISBN 5-93378-040-5.

3.2 Вопросы и компетенции, оцениваемые по ответу на дополнительные вопросы устного этапа

Компетенции ОК-1, …, ОК-9 формируются гуманитарными дисциплинами. Комиссия может задать дополнительный вопрос по любой из них.

Дисциплина «Управление средствами защиты информации». Преподаватель: Конев А.А.

способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности (ПК-18);

способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-19);

способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20);

способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21);

способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22);

способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-23);

способностью управлять информационной безопасностью автоматизированной системы (ПК-28).

Вопросы:

1. Перечислите требования к описанию условий создания и использования защищаемой информации и приведите примеры информационно-технологических ресурсов, подлежащих защите. Л.1, с. 10.
2. Приведите перечень направлений классификации угроз информационной безопасности, на основании которых составляются частные модели угроз персональным данным. Л.2, с. 11-16.

3. Охарактеризуйте категории нарушителей в зависимости от наличия доступа, способа доступа и полномочий доступа к автоматизированной системе. Л.2, с. 24-27.

4. Перечислите этапы оценки рисков информационной безопасности автоматизированных систем. Л.3, с. 8-14.

5. Приведите примеры источников информации об инцидентах информационной безопасности и перечислите аспекты анализа этих инцидентов, направленные на совершенствование системы управления информационной безопасностью. Л.4, с. 22-23, 32-33.

6. Приведите требования к формированию политики информационной безопасности организации и учитываемые в ней категории безопасности. Л.5, с.3-6

Список источников

1. Методические рекомендации по обеспечению с помощью криптосредст в безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. Утв. ФСБ РФ 21.02.2008 N 149/54-144.

2. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). Утв. ФСТЭК РФ 15.02.2008.

3. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. Утв. приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2010 г. N 632-ст.

4. ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. Утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2007 г. N 513-ст.

5. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. Утв. приказом Федерального агентства по техническому регулированию и метрологии от 24 сентября 2012 г. N 423-ст.

Дисциплина «Системный анализ». Преподаватель Сопов М.А.

Компетенции:

способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-5);

способностью создавать и исследовать модели автоматизированных систем (ПК-2).

Вопросы:

1. Представьте и объясните алгоритм анализа проекторного решения.

2. Какие модели порождает процедура анализа проектного решения. Их место и назначение в процедуре анализа проектного решения.

3. Представьте и объясните алгоритм синтеза проекторного решения.

4. Какие модели порождает процедура синтеза проектного решения. Их место и назначение в процедуре синтеза проектного решения.

Список источников

1.Прикладной системный анализ : учебное пособие / Ф.П. Тарасенко. — М. : КНОРУС, 2010. — 224 с. , с. 59-61.

Дисциплины «Разработка и эксплуатация защищенных автоматизированных систем», «Программно-аппаратные средства обеспечения информационной безопасности». Преподаватели: Рахманенко И.А., Новохрестов А.К.

Компетенции:

способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-8);

способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-9);

способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-10);

способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-12);

способностью участвовать в проектировании средств защиты информации автоматизированной системы (ПК-13);

способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20);

способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25);

способностью администрировать подсистему информационной безопасности автоматизированной системы (ПК-26);

способностью управлять информационной безопасностью автоматизированной системы (ПК-28).

Вопросы:

1. Обоснуйте необходимость использования систем обнаружения вторжений. Приведите примеры, проанализируйте и коротко опишите существующие решения.

2. Обоснуйте необходимость использования средств защиты информации от несанкционированного доступа. Приведите примеры, проанализируйте и коротко опишите существующие решения.

3. Опишите модель разработки защищенных автоматизированных систем в соответствии с ГОСТ Р ИСО/МЭК 15408-1-2012 "Критерии оценки безопасности информационных технологий" ("Общие критерии").

4. Дайте определение понятию "Профиль защиты". Опишите назначение профиля защиты с точки зрения разработки защищенных автоматизированных систем (ГОСТ Р ИСО/МЭК 15408-1-2012).

5. Перечислите и кратко опишите разделы технического задания на создание автоматизированной системы (ГОСТ 34.602-89).

6. Перечислите классы функциональных требований безопасности ГОСТ Р ИСО/МЭК 15408-2-2012. Опишите один из классов на примере базового профиля защиты операционных систем общего назначения.

7. Перечислите и опишите этапы разработки системы управления информационной безопасностью (ГОСТ Р ИСО/МЭК 27001).

8. Перечислите и опишите основные варианты стратегии анализа рисков организации (ГОСТ Р ИСО/МЭК 27005-2010).

9. Сформулируйте стадии проектирования средств защиты информации и средств контроля защищенности автоматизированной системы.

10. Опишите многоуровневый подход к построению компьютерных сетей. Модели OSI, TCP/IP.

11. Планирование и управление сетевой безопасностью. Кратко изложите общий процесс достижения и поддержки необходимой сетевой безопасности (ГОСТ Р ИСО/МЭК 27033-1-2011).

12. Перечислите основные этапы, исходные данные и критерии отнесения автоматизированной системы к классам защищенности от НСД к информации (РД АС. Защита от НСД к информации. Классификация АС и требования по ЗИ).

Список источников

1. ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель [Текст]. - Введ. 2012-11-15. - М.: Стандартинформ, 2014.

2. ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности [Текст]. - Введ. 2013-11-08. - М.: Стандартинформ, 2014.

3. ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы [Текст]. - Введ. 1990-01-01. - М.: ИПК ИЗДАТЕЛЬСТВО СТАНДАРТОВ, 2004.

4. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования [Текст]. - Введ. 2006-12-27. - М.:

Стандартинформ, 2008.

5. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности [Текст]. - Введ. 2011-12-01. - М.: Стандартинформ, 2011.

6. ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции [Текст]. - Введ. 2012-01-01. - М.: Стандартинформ, 2012.

7. Руководящий документ Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации [Текст]: . Утв. решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. 29 с.

8. ГОСТ 34.601-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания [Текст]. - Введ. 1992-01-01. - М.: Стандартинформ, 2009.

9. Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты [Электронный ресурс] // Режим доступа: http://fstec.ru/component/attachments/download/317

10. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. – СПб.: Питер, 2012. – 960 с.: ил.

11. Комплексная защита информации в корпоративных системах [Текст] : учебное пособие для вузов / В. Ф. Шаньгин. - М. : ФОРУМ, 2012 ; М. : ИНФРА-М, 2012. - 592 с. : ил.

Дисциплины «Криптографические методы защиты информации», «Теоретические основы компьютерной безопасности». Преподаватель Евсютин О.О.

Компетенции:

способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники (ОПК-2).

Вопросы:

1. Каким образом может быть проведен анализ автоматизированной системы на предмет возможности утечки права доступа?

2. Каким образом может быть формализована политика разграничения прав доступа в автоматизированной системе?

3. Для обеспечения свойств конфиденциальности и целостности информации в автоматизированной банковской системе используется протокол, основанный на использовании отечественных криптографических стандартов. Предложите формат пакета данных для такого протокола.

4. Перечислите и охарактеризуйте задачи информационной безопасности, для решения которых предназначен стандарт ГОСТ 28147-89?

5. Укажите, каким образом связаны между собой криптографические стандарты ГОСТ Р 34.10 и ГОСТ Р 34.11.

6. Каким образом пользователь может удостовериться в аутентичности открытого ключа другого пользователя, который содержится в сертификате, выданном центром сертификации, неизвестным первому пользователю?

Список источников

1. Мещеряков Р.В. Теоретические основы компьютерной безопасности: учебное пособие для студентов специальности 075500 / Р. В. Мещеряков, Г. А. Праскурин. — 2-е изд., перераб. и доп. — Томск: В-Спектр, 2007. — 343 с.

2. Девянин П.Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах.— М.: Радио и связь, 2006. — 175 с.

3. Девянин П.Н. Модели безопасности компьютерных систем: учебное пособие для вузов. — М.: Академия, 2005. — 142 с.

1. Основы криптографии: учебное пособие для вузов / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. — 3-е изд., испр. и доп. — М.: Гелиос АРВ, 2005. — 479 с.

2. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости: учебное пособие для студентов учреждений высшего профессионального образования. — М.: Издательский центр «Академия», 2009. — 272 с.

3. Смарт Н. Криптография: учебник для вузов. — М.: Техносфера, 2005. — 525 с.

4. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. — М.: ИПК Издательство стандартов, 1996. — 26 с.

5. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. — М.: Стандартинформ, 2015. — 21 с.

6. ГОСТ Р 34.13-2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. — М.: Стандартинформ, 2015. — 38 с.

7. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. — М.: Стандартинформ, 2012. — 34 с.

8. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. — М.: Стандартинформ, 2012. — 29 с.

Дисциплина «Организационное и правовое обеспечение информационной безопасности». Преподаватель Новгородова Н.А.

Компетенция:

способностью создавать и исследовать модели автоматизированных систем (ПК-2);

способностью проводить анализ защищенности автоматизированных систем (ПК-3);

способностью разрабатывать политику информационной безопасности автоматизированной системы (ПК-11);

способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20);

способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21);

способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22);

способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-23);

Вопросы:

1. Приведите типовую/возможную структуру инструкции по парольной защите.

2. Приведите типовую/возможную структуру должностной инструкции специалиста по защите информации.

Список источников

1 Справочные правовые системы (СПС). СПС «КонсультантПлюс», СПС «Гарант».

2 "Квалификационный справочник должностей руководителей, специалистов и других служащих" (утв. Постановлением Минтруда России от 21.08.1998 N 37) (ред. От 12.02.2014).

3 Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов и др.; Под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. - М.: Горячая линия — Телеком, 2009. - 552 с.: ил.

4 Приказ Роспатента от 14.07.2015 N 97 "Об утверждении Положения по организации парольной защиты в Федеральной службе по интеллектуальной собственности".

5 Приказ ФАС России от 23.10.2012 N 654 "Об утверждении Положения по организации парольной защиты автоматизированных систем Федеральной антимонопольной службы".

6 Приказ Роспатента от 05.07.2013 N 82 "Об утверждении инструкций по обеспечению режима секретности при обработке секретной информации с использованием компьютерной системы в режимно-секретном подразделении Роспатента".

Дисциплина «Нормативная база обеспечения информационной безопасности банковской организации». Преподаватель Егошин Н.С.

Компетенции:

способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности автоматизированных банковских систем (ПСК-5.1);

способностью разрабатывать и реализовывать политики информационной безопасности автоматизированных банковских систем (ПСК-5.2);

способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной банковской системы (ПСК-5.5);

Вопросы:

1. Опишите комплекс отраслевых стандартов (СТО БР ИББС) и рекомендаций (РС БР ИББС) Центрального Банка Российской Федерации в области информационной безопасности банковской системы Российской Федерации.
2. Какова общая политика информационной безопасности банковской организации.
3. Поясните назначение РАБИС-НП в банковской системе РФ
4. Какие средства и методы технической защиты информации, используются в банковской системе РФ.

Список источников

1. "Стандарт Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения" СТО БР ИББС-1.0-2014" (принят и введен в действие Распоряжением Банка России от 17.05.2014 N Р-399).
2. "Стандарт Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014" СТО БР ИББС-1.2-2014" (принят и введен в действие Распоряжением Банка России от 17.05.2014 N Р-399).

Дисциплина «Распределенные автоматизированные информационные системы». Преподаватель Праскурин Г.А.

Компетенции:

способностью проводить анализ защищенности автоматизированных систем (ПК-3);

способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24);

способностью администрировать подсистему информационной безопасности автоматизированной системы (ПК-26).

Вопросы

1. Опишите комплекс мер для обеспечения информационной безопасности автоматизированной системы на базе автоматизированного рабоче-

го места без подключения к вычислительной сети. Какие нормативные документы регламентируют состав и содержание мер для обеспечения информационной безопасности?

2. Опишите различие в подходах к обеспечению информационной безопасности для локальных и распределенных информационных систем. Какие дополнительные меры обеспечения информационной безопасности необходимо применять для защиты распределенных информационных систем?

Список источников

1. Федеральный закон от 27.07.206 №149 «Об информации, информационных технологиях и о защите информации»;

2. Федеральный закон от 27.07.2006 №152 «О персональных данных»;

3. Постановление Правительства РФ №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

4. Приказ ФСТЭК от 11.02.2013 №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

5. Приказ ФСТЭК от 18.02.2013 №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

6. Приказ ФСБ от 10.07.2014 №378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

Дисциплина «Моделирование автоматизированных информационных систем». Преподаватель Давыдова Е.М.

Компетенции:

способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники (ОПК-2);

способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-5);

способностью создавать и исследовать модели автоматизированных систем (ПК-2).

Вопросы:

1.С каких работ следует начинать разработку модели автоматизирован-

ной системы?

2.Какие методы исследования модели применяются для автоматизированных систем?

Список источников

1 Решетникова, Г.Н. Моделирование систем : Учебное пособие / Г. Н. Решетникова; Федеральное агентство по образованию, Томский государственный университет систем управления и радиоэлектроники. - 2-е изд., перераб. и доп. - Томск : ТУСУР, 2007. - 440 с.

2 Серафинович Л.П. Основы теории подобия и моделирования : учебное пособие / Л. П. Серафинович; Федеральное агентство по образованию, Томский государственный университет систем управления и радиоэлектроники, Кафедра комплексной информационной безопасности электронно-вычислительных систем. - Томск: ТУСУР, 2005. - 202 с.