**Тамбовское государственное автономное профессиональное**

**образовательное учреждение «Тамбовский бизнес-колледж»**

**Предметно-цикловая комиссия информационных технологий**

Утверждаю:

Директор ТОГАПОУ

«Тамбовский бизнес-колледж»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Н.В. Астахова

Пр. 104/1 от 28.08.2017

**Фонд оценочных средств**

текущего контроля и промежуточной аттестации по учебной дисциплине

**ОП.02 ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ   
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

среднее профессиональное образование

(программа подготовки специалистов среднего звена)

**10.02.05 Обеспечение информационной безопасности автоматизированных систем**

Тамбов 2017

**Лист согласования**

**программы фонда оценочных средств учебной дисциплины**

**ОП.02 ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ   
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Дисциплина ОП.02 Организационно-правовое обеспечение информационной безопасности входит в общепрофессиональный цикл основной профессиональной образовательной программы в соответствии с ФГОС по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, квалификация – техник по защите информации., является дисциплиной, закладывающей базу для последующего изучения профессиональных модулей: ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении, ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами, ПМ.03 Защита информации техническими средствами.

Программа ОП.02 Организационно-правовое обеспечение информационной безопасности может быть использована для изучения дисциплин специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, изучаемых в учреждениях среднего профессионального образования при подготовке квалифицированных специалистов среднего звена.

**Организация разработчик:**

Тамбовское областное государственное автономное профессиональное образовательное учреждение «Тамбовский бизнес-колледж»

**Разработчики:**

Машков С.Н. преподаватель высшей категории ТОГАПОУ «Тамбовский бизнес-колледж».

Программа учебной дисциплины рассмотрена и рекомендована на заседании ПЦК информационных технологий.

Протокол №1 от «28» августа 2017 г.

СОГЛАСОВАНО:

Коммерческий директор ИЦ «НАШ ГОРОД»

\_\_\_\_\_\_\_\_\_\_\_\_\_ В.А. Колесов

«28» августа 2017 г.

**Аннотация**

**Цели и задачи учебной дисциплины:**

Целью дисциплины является получение обучающимися опыта осуществлять организационное обеспечение информационной безопасности автоматизированных (информационных) систем в рамках должностных обязанностей техника по защите информации.

**Задачи дисциплины**:

1. применять нормативные правовые акты и нормативные методические документы в области защиты информации;
2. контролировать соблюдение персоналом требований по защите информации при ее обработке с использованием средств вычислительной техники;
3. оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации;
4. защищать свои права в соответствии с трудовым законодательством

В результате изучения дисциплины обучающийся должен**:**

уметь :

– осуществлять организационное обеспечение информационной безопасности автоматизированных (информационных) систем в рамках должностных обязанностей техника по защите информации;

– применять нормативные правовые акты и нормативные методические документы в области защиты информации;

– контролировать соблюдение персоналом требований по защите информации при ее обработке с использованием средств вычислительной техники;

– оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации;

– защищать свои права в соответствии с трудовым законодательством

знать:

– основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;

– правовые основы организации защиты информации, содержащей сведения, составляющие государственную тайну и информации конфиденциального характера, задачи органов защиты государственной тайны;

– нормативные документы в области обеспечения защиты информации ограниченного доступа;

– организацию ремонтного обслуживания аппаратуры и средств защиты информации;

– принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности в организации;

– правовое положение субъектов правоотношений в сфере профессиональной деятельности (включая предпринимательскую деятельность);

– нормативные методические документы, регламентирующие порядок выполнения мероприятий по защите информации, обрабатываемой в автоматизированной (информационной) системе;

– законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения.

Изучение данной учебной дисциплины направлено на достижение общеобразовательных, воспитательных и практических задач, на дальнейшее развитие личностных способностей и дальнейшего профессионального роста выпускника-будущего специалиста.

**1. Общие положения**

Дисциплина ОП.02 Организационно-правовое обеспечение информационной безопасности входит в общепрофессиональный цикл основной профессиональной образовательной программы в соответствии с ФГОС по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, квалификация – техник по защите информации., является дисциплиной, закладывающей базу для последующего изучения профессиональных модулей: ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении, ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами, ПМ.03 Защита информации техническими средствами.

Программа ОП.02 Организационно-правовое обеспечение информационной безопасности может быть использована для изучения дисциплин специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, изучаемых в учреждениях среднего профессионального образования при подготовке квалифицированных специалистов среднего звена.

**1. Паспорт фонда оценочных средств**

**1.1. Область применения**

Комплект фонда оценочных средств предназначен для проверки результатов освоения учебной дисциплины ОП15 «Защищенные документооборот» программы подготовки специалистов среднего звена по специальности СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

**1.1.1 Карта компетенций**

Таблица 1

|  |  |
| --- | --- |
| Контролируемые компетенции (шифр компетенции) | Планируемые результаты обучения (знает, умеет, владеет, имеет навык) |
| ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес. | **Знать:** возможности трудоустройства и варианты построения трудовой карьеры на базе профессии обучения; видов и типов предприятий, форм занятости для трудоустройства по профессии обучения |
| **Уметь:** обосновывать выбор своей будущей профессии, ее преимущества и значимость на современном рынке труда России |
| **Владеть:** возможностями использования умений и навыков, приобретенных в ходе изучения учебного курса (дисциплины), в будущей профессионально-трудовой деятельности |
| ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество | **Знать:** виды и типы проблем в профессиональной деятельности, обобщенные способы их разрешения; типов и видов планирования работ, построения планов-графиков профессиональной деятельности; возможности повышения профессиональной квалификации |
| **Уметь:** планировать профессиональную деятельность, самообразование и организовывать их выполнение в соответствии с планом; выбирать эффективный способ решения проблем при наличии альтернативы и обосновывать его |
| **Владеть:** практическим опытом планирования работ, исходя из целей и задач деятельности, определенных руководителем; выбора средств реализации целей и задач, поставленных руководителем |
| ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личного развития | **Знать:** типы и виды источников информации в профессиональной области, их особенности и способы получения, способов работы с информацией при разрешении профессионально-трудовых проблем. |
| **Уметь:** осуществлять поиск, обработку и представление информации в различных форматах (таблицы, графики, диаграммы, текст и т.д.), в том числе – с использованием компьютерных программ; выделять существенное содержание в технических инструкциях и регламентах |
| **Владеть:** практическим опыта самостоятельного поиска информации из различных источников (в том числе – профессиональных изданий, Интернета и т.д.), необходимой для решения профессионально- трудовых задач; обработки и представления информации в различных форматах для разных групп пользователей (в том числе – администрации, коллег, клиентов и т.д.) |
| ОК 5. Владеть информационной культурой, анализировать и оценивать информацию с использованием информационно-коммуникативных технологий | **Знать:** основы работы с текстовыми редакторами, электронными таблицами, электронной почтой, мультимедийным оборудованием; способов работы с информацией при разрешении профессионально-трудовых проблем. |
| **Уметь:** осуществлять поиск, обработку и представление информации в различных форматах, с использованием компьютерных программ; (электронные таблицы, графики, диаграммы, текст и т.д.) |
| **Владеть:** практическим опытом самостоятельного поиска информации с использованием информационно-коммуникационных технологий, необходимой для решения профессионально-трудовых задач; обработки и представления информации в различных форматах для разных групп пользователей (в том числе – администрации, коллег, клиентов и т.д.) |
| ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями. | **Знать:** основные профессиональные технические термины и определения профессиональной области |
| **Уметь:** грамотно разъясняться с коллегами на профессиональные темы; сформулировать задачу |
| **Владеть:** практическим опытом коллективного решения задач в профессиональной области |
| ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. | **Знать:** ответственность за работу членов команды (подчиненных), результат выполнения заданий |
| **Уметь:** нести ответственность за работу членов команды (подчиненных), результат выполнения заданий |
| **Владеть:** практическим опытом несенияответственности за работу членов команды (подчиненных), результат выполнения заданий |
| ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации. | **Знать:** принципы определения задачи профессионального и личностного развития |
| **Уметь:** самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации. |
| **Владеть:** навыками самостоятельного определения задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации. |
| ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности. | **Знать:** основополагающие принципы функционирования технологий в профессиональной деятельности |
| **Уметь:** ориентироваться в условиях частой смены технологий в профессиональной деятельности |
| **Владеть:** навыками самостоятельного освоения новых методов и технологий в профессиональной деятельности |
| ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках. | **Знать:** уметь пользоваться профессиональной документацией на государственном и иностранном языках. |
| **Уметь:** Пользоваться профессиональной документацией на государственном и иностранном языках. |
| **Владеть:** Навыками пользования профессиональной документацией на государственном и иностранном языках |
| ПК 2.1 Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами | **Знать:** методы обеспечения защиты информации в автоматизированных системах отдельными программами, программно-аппаратными средствами |
| **Уметь:** Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами |
| **Владеть:** навыками обеспечения защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами |
| ПК 2.4 Осуществлять обработку, хранение и передачу информации ограниченного доступа | **Знать:** способы осуществления обработки, хранения и передачи информации ограниченного доступа |
| **Уметь:** Осуществлять обработку, хранение и передачу информации ограниченного доступа |
| **Владеть:** приемами осуществления обработки, хранения и передачи информации ограниченного доступа |

ФОС предназначен для контроля и оценки результатов освоения учебной дисциплины ОП.02 Организационно-правовое обеспечение информационной безопасности по ППССЗ 10.02.05Обеспечение информационной безопасности автоматизированных систем

1. ЗАДАНИЕ ДЛЯ СТУДЕНТА

**Часть А:**

1. Назовите Федеральный закон, который регулирует отношения, возникающие при обеспечении защиты информации:

а) Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

б) Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

в) Доктрина информационной безопасности Российской Федерации от 9 сентября 2000 г. № Пр-1895.

1. Как Федеральный закон Российской Федерации от 27 июля 2006 г. №149 подразделяет информацию в зависимости от категории доступа к ней:

а) на общедоступную информацию;

б) на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа);

в) на общедоступную информацию, а также на информацию, доступ ккоторой ограничен федеральными законами (информацияограниченного доступа).

1. Перечислите принципы, на которых основывается правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации:

а) свобода поиска, получения, передачи, производства ираспространения информации любым законным способом;

б) установление ограничений доступа к информации только федеральными законами и решением руководителя;

в) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такойинформации, кроме случаев, установленных федеральнымизаконами;

г) равноправие языков народов Российской Федерации при созданииинформационных систем и их эксплуатации;

д) обеспечение безопасности Российской Федерации при созданииинформационных систем, их эксплуатации и защите содержащейся в них информации;

е) достоверность информации и своевременность ее предоставления;

ж) неприФОСновенность частной жизни, недопустимость сбора,хранения, использования и распространения информации о частнойжизни лица без его согласия;

з) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационныхтехнологий перед другими.

1. Что такое конфиденциальность информации:

а) конфиденциальность информации - обязательное для выполнениялицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам безсогласия ее обладателя;

б) конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без законодательно оформленного соглашения;

в) конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без росписи в журнале посетителей о полученной информации.

1. Требованиями каких законов регулируется защита информации,

составляющей государственную тайну:

а) Законом Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне»;

б) Указом президента Российской Федерации «О перечне сведений, отнесенных к государственной тайне»;

в) в соответствии с законодательством Российской Федерации огосударственной тайне.

1. Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии:

а) с федеральными законами и (или) по решению суда;

б) с федеральными законами;

в) по решению суда.

1. Назовите виды информационных систем:

а) государственные информационные системы;

б) муниципальные информационные системы;

в) личные информационные системы.

1. Что представляет собой защита информации:

а) принятие правовых, организационных и технических мер;

б) принятие правовых и технических мер;

в) принятие правовых и организационных мер.

1. На что направлено принятие правовых, организационных, технических и экономических мер защиты информации:

а) на обеспечение защиты информации от неправомерного доступа,уничтожения, модифицирования, блокирования, копирования,предоставления, распространения, а также от иных неправомерныхдействий в отношении такой информации;

б) на соблюдение конфиденциальности информации ограниченного доступа;

в) на реализацию права на доступ к информации.

1. В каких случаях не требуется обеспечение конфиденциальности персональных данных:

а) в случае обезличивания персональных данных, а также в отношении общедоступных персональных данных;

б) в отношении общедоступных персональных данных;

в) в случае обезличивания персональных данных.

1. Какова должна быть категория объектов информатизации, на которых обрабатывается информация с грифом «Секретно»:

а) первая;

б) вторая;

в) третья.

1. Какова должна быть категория объектов информатизации, на которых обрабатывается информация с грифом «Сов. Секретно»:

а) первая;

б) вторая;

в) третья.

1. Какова должна быть категория объектов информатизации, на которых обрабатывается информация с грифом «Особой важности»:

а) первая;

б) вторая;

в) третья.

1. Назовите виды конфиденциальной информации, утвержденные Указом президента Российской Федерации «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 г. № 188:

а) сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

б) сведения, составляющие тайну следствия и судопроизводства;

в) служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

г) сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т. д.);

д) сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна);

е) сведения о стихийных бедствиях;

ж) сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

1. Каким руководящим документом определены требования по порядку разработки и содержанию «Положения о подразделении (специалисте) по защите информации»:

а) Решением Гостехкомиссии России № 42 от 03.10.1995 г.;

б) Решением Гостехкомиссии России № 42 от 03.10.1995 г. и Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

в) Решением Гостехкомиссии России от 14.03.1995 № 32.

1. Каким руководящим документом определены требования по порядку разработки и содержанию «Руководства по защите информации...»:

а) Решением Гостехкомиссии России № 42 от 03.10.1995 г.;

б) Решением Гостехкомиссии России № 42 от 03.10.1995 г. и Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

в) Решением Гостехкомиссии России от 14.03.1995 № 32.

1. Каким руководящим (нормативно правовым) документом определены требования к содержанию и порядку определения политики безопасности предприятия:

а) Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

б) Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

в) Доктриной информационной безопасности Российской Федерации от 9 сентября 2000 г. № Пр-1895;

г) никаким.

1. Сколько существует классов защищенности АС от

несанкционированного доступа:

а) три;

б) пять;

в) семь;

г) девять.

1. На сколько групп разбиты классы защищенности АС от

несанкционированного доступа:

а) на две;

б) на три;

в) на пять.

1. Основные способы НСД к информации:

а) непосредственное обращение к объектам доступа;

б) создание программных и технических средств, выполняющихобращение к объектам доступа в обход средств защиты;

в) модификация средств защиты, позволяющая осуществить НСД;

г) поиск необходимой информации по Интернету;

д) внедрение в технические средства СВТ или АС программных илитехнических механизмов, нарушающих предполагаемую структуру и функции СВТ или АС и позволяющих осуществить НСД.

1. Основными характеристиками технических средств защиты являются:

а) степень полноты охвата ПРД реализованной СРД и ее качество;

б) состав и качество обеспечивающих средств для СРД;

в) гарантии правильности функционирования СРД иобеспечивающих ее средств;

г) рейтинг производителя;

д) стоимость технических средств и качество эксплуатации.

1. Какие характеристики объектов и субъектов защиты должны быть положены в основу системы классификации АС:

а) информационные - определяющие ценность информации, ее объем и степень (гриф) конфиденциальности, а также возможныепоследствия неправильного функционирования АС из-за искажения(потери) информации;

б) организационные - определяющие полномочия пользователей;

в) уровень образования сотрудников;

г) технологические - определяющие условия обработки информации(способ обработки, время циркуляции, вид АС).

1. Основные этапами классификации АС:

а) разработка и анализ исходных данных;

б) выявление основных признаков АС, необходимых дляклассификации;

в) сравнение выявленных признаков АС с классифицируемыми;

г) разработка матрицы доступа;

д) присвоение АС соответствующего класса защиты информации отНСД.

1. Необходимые исходные данные для проведения классификации конкретной АС:

а) перечень защищаемых информационных ресурсов АС и уровень их

конфиденциальности;

б) перечень лиц, имеющих доступ к штатным средствам АС, суказанием уровня их полномочий;

в) матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;

г) наличие инструкции пользователю;

д) режим обработки данных в АС.

1. Что относят к числу определяющих признаков, по которым производится группировка АС в различные классы:

а) наличие в АС информации различного уровня конфиденциальности;

б) уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;

в) наличие приказа по организации об установлении класса защищенности АС;

г) режим обработки данных в АС: коллективный или индивидуальный.

1. Из каких подсистем условно состоит в общем случае комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД в рамках системы защиты информации от НСД ИСПДн:

а) управления доступом;

б) регистрации и учета;

в) криптографической;

г) мониторинга вторжений;

д) обеспечения целостности;

е) круглосуточного видеонаблюдения;

ж) антивирусной.

1. Из каких подсистем условно состоит в общем случае комплекс программно-технических средств и организационных решений (процедурных) по защите информации от НСД в рамках системы защиты информации в АС:

а) управления доступом;

б) регистрации и учета;

в) круглосуточного видеонаблюдения;

г) криптографической;

д) обеспечения целостности;

1. Типовая структура службы безопасности:

а) отдел режима и охраны, в составе сектора режима и сектора охраны;

б) отдел защиты информации;

в) группа бухгалтерского учета;

г) инженерно-техническая группа;

д) группа безопасности внешней деятельности.

1. Основные документы, регламентирующие деятельность подразделения (специалиста) по защите информации:

а) Конституция Российской Федерации;

б) Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

в) Положение о подразделении (специалисте) по защите

информации;

г) Решением Гостехкомиссии России от 14.03.1995 № 42.

1. Какой основной нормативно-правовой акт должен быть оформлен сотруднику перед допуском его к работе с информацией ГТ с грифом

совершенно секретно:

а) трудовой договор;

б) дополнение к трудовому договору;

в) форма допуска №3.

1. Какой основной нормативно-правовой акт должен быть оформлен сотруднику перед допуском его к работе с информацией ГТ с грифом совершенно секретно:

а) приказ по организации о процентной надбавки за секретность;

б) должностная инструкция;

в) форма допуска №2.

1. Кто оформляет форму допуска №3:

а) Руководитель территориального Управления ФСТЭК по

федеральному округу;

б) Руководитель организации;

в) Территориальный орган ФСБ России.

1. Кто оформляет форму допуска №2:

а) Руководитель территориального Управления ФСТЭК по

федеральному округу;

б) Руководитель организации;

в) Территориальный орган ФСБ России.

1. Сколько классов защищенности ИСПДн от НСД:

а) три;

б) четыре;

в) пять.

1. Доктрина информационной безопасности Российской Федерации

представляет собой совокупность официальных взглядов на:

а) цели

б) взгляды

в) задачи

г) принципы

1. Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных:

а) угрозах

б) интересов личности

в) общества

г) государства

1. Источники угроз информационной безопасности Российской Федерации подразделяются на:

а) внешние

б) основные

в) внутренние

1. Успешному решению вопросов обеспечения информационной безопасности Российской Федерации способствуют системы:

а) государственная система защиты информации

б) система зашиты президента

в) система защиты государственной тайны

г) системы сертификации средств защиты информации

1. Общие методы обеспечения информационной безопасности Российской Федерации разделяются на:

а) экономические

б) внешние

в) правовые

г) организационно-технические

1. Наибольшую опасность в сфере внутренней политики представляют следующие угрозы информационной безопасности Российской Федерации:

а) нарушение конституционных прав и свобод граждан

б) распространение дезинформации о политике РФ

в) деятельность общественных объединений, направленная на насильственное изменение основ конституционного строя и нарушение целостности РФ

г) мероприятиями в области обеспечения информационной безопасности РФ

1. Основными направлениями обеспечения информационной безопасности Российской Федерации в сфере духовной жизни являются:

а) распространение дезинформации о политике РФ

б) развитие в России основ гражданского общества

в) государственная поддержка мероприятий по сохранению и возрождению культурного наследия народов и народностей РФ

г) противодействие негативному влиянию иностранных религиозных организаций и миссионеров.

1. Основными направлениями международного сотрудничества Российской Федерации в области обеспечения информационной безопасности являются

а) запрещение разработки, распространения и применения "информационного оружия”

б) обеспечение безопасности международного информационного обмена

в) обеспечение безопасности для торговли людьми

г) предотвращение несанкционированного доступа к конфиденциальной информации в международных банковских телекоммуникационных сетях

1. Государственная политика обеспечения информационной безопасности РФ основывается на следующих основных принципах:

а) соблюдение Конституции РФ, законодательства РФ, общепризнанных принципов и норм международного права

б) правовое равенство всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса

в) соблюдении правил дорожного движения

г) приоритетное развитие отечественных современных информационных и телекоммуникационных технологий

1. Г осударство в процессе реализации своих функций по обеспечению информационной безопасности Российской Федерации:

а) обеспечивает безопасность интересов граждан

б) проводит объективный и всесторонний анализ и прогнозирование угроз информационной безопасности РФ, разрабатывает меры по ее обеспечению

в) проводит необходимую протекционистскую политику в отношении производителей средств информатизации и защиты информации на территории РФ

г) способствует интернационализации глобальных информационных сетей и систем

1. Первоочередными мероприятиями по реализации государственной политики обеспечения информационной безопасности Российской Федерации являются:

а) разработка и внедрение механизмов реализации правовых норм, регулирующих отношения в информационной сфере

б) развитие системы подготовки кадров, используемых в области обеспечения информационной безопасности РФ

в) гармонизация отечественных стандартов в области информатизации и обеспечения информационной безопасности автоматизированных систем управления

г) переход к рыночным отношениям в экономике

1. Основными функциями системы обеспечения информационной безопасности Российской Федерации являются:

а) создание условий для реализации прав граждан и общественных объединений на разрешенную законом деятельность в информационной сфере

б) обеспечение безопасности компьютерного пиратства

в) разработка нормативной правовой базы в области обеспечения информационной безопасности РФ

г) предупреждение, выявление и пресечение правонарушений, связанных с посягательствами на законные интересы граждан, общества и государства в информационной сфере

1. Компетенция федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов, входящих в состав системы обеспечения информационной безопасности РФ определяется:

а) федеральными законами

б) нормативными правовыми актами Президента РФ

в) Правительством РФ

г) компьютерным пиратством

1. Система обеспечения информационной безопасности Российской Федерации строится на основе разграничения полномочий органов:

а) законодательной власти

б) народной власти

в) исполнительной власти

г) судебной власти

1. Основными элементами организационной основы системы обеспечения информационной безопасности Российской Федерации являются:

а) принцип законности

б) Президент Российской Федерации

в) Совет Безопасности РФ

г) Государственная Дума Федерального Собрания РФ

1. Правовая база, регулирующая отношения, возникающие при обеспечении защиты информации:

Федеральный закон Российской Федерации от 27 июля 2006 г. № 149- ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральный закон Российской Федерации от 27 июля 2006 г. № 152- ФЗ «О персональных данных»;

Доктрина информационной безопасности Российской Федерации от 9 сентября 2000 г. № Пр-1895.

1. Основные способы НСД к информации: непосредственное обращение к объектам доступа; создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты; поиск необходимой информации по сети Интернет; модификация средств защиты, позволяющая осуществить НСД; внедрение в технические средства СВТ или АС программных или технических механизмов, нарушающих предполагаемую структуру и функции СВТ или АС и позволяющих осуществить НСД.
2. Виды информации в зависимости от категории доступа к ней согласно законодательства РФ делятся:

на общедоступную информацию;

на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа);

на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

1. Каким руководящим (нормативно правовым) документом определены требования к содержанию и порядку определения политики безопасности предприятия:

Федеральным законом Российской Федерации от 27 июля 2006 г.

№ 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральным законом Российской Федерации от 27 июля 2006 г.

№ 152-ФЗ «О персональных данных»;

Доктриной информационной безопасности Российской Федерации от 9

сентября 2000 г. № Пр-1895;

никаким.

1. Классы защищенности средств вычислительной техники от несанкционированного доступа.

три;

четыре;

пять.

1. Факторы, влияющие на требуемый уровень защиты информации. Гриф секретности;

Режим обработки информации;

Права пользователей.

1. Укажите основные законы, относящиеся к организации и функционированию системы информационной безопасности и защиты информации

Федеральный закон Российской Федерации от 27 июля 2006 г. № 149- ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральный закон Российской Федерации от 27 июля 2006 г. № 152- ФЗ «О персональных данных»;

Доктрина информационной безопасности Российской Федерации от 9 сентября 2000 г. № Пр-1895.

1. Каковы основные отечественные и зарубежные стандарты в области информационной безопасности?

ISO 17799

ГОСТ Р ИСО/МЭК 15408;

ГОСТ Р 51241-98.

1. Что такое политика безопасности?

Свод правил предприятия по обеспечению информационной безопасности;

Мнение руководителя предприятия;

Должностные инструкции сотрудников.

1. Что такое государственная тайна?

Конфиденциальная информация;

Информация для служебного пользования;

Информация ограниченного распространения.

1. Что такое коммерческая тайна?

Конфиденциальная информация;

Информация для служебного пользования;

Информация ограниченного распространения.

1. Что такое служебная тайна?

Конфиденциальная информация;

Информация для служебного пользования;

Информация с грифом секретно.

1. Что такое профессиональная тайна?

Конфиденциальная информация;

Информация для служебного пользования;

Информация с грифом секреетно.

1. Что такое персональные данные?

Конфиденциальная информация;

Информация для служебного пользования;

Информация ограниченного распространения.

1. Что такое источники права на доступ к информации?

Правовая база РФ по безопасности информации;

Форма допуска сотрудника;

Решение руководителя организации.

1. Каковы уровни доступа к информации с точки зрения законодательства?

Форма допуска 1;

Форма допуска 2;

Форма допуска 5 Форма допуска 3.

1. Что такое информация ограниченного распространения? Конфиденциальная информация;

Информация для служебного пользования;

Информация ограниченного распространения;

Государственная тайна.

1. Источники угроз?

Внешние источники угроз;

Служебные разногласия;

Внутренние источники угроз.

1. Что делает правительство РФ в пределах своих полномочий? Организует работы по защите информации;

Осуществляет методическое руководство;

Выполняет мероприятия по защите информации;

Осуществляет контроль

1. Что делает Совет Безопасности РФ?

Разрабатывает Концепцию национальной безопасности; Организует работы по защите информации;

Осуществляет методическое руководство;

Осуществляет контроль.

1. Что делают Федеральные органы исполнительной власти? Организуют работы по защите информации;

Осуществляют методическое руководство;

Осуществляют контроль

1. Что делают Межведомственные и государственные комиссии? Организует работы по защите информации;

Осуществляет методическое руководство;

Осуществляет контроль

1. Что делают Органы исполнительной власти субъектов Российской Федерации?

Организуют работы по защите информации;

Осуществляют методическое руководство;

Осуществляют контроль;

Проводят работы по защите информации.

1. Что делают Органы местного самоуправления?

Организуют работы по защите информации;

Осуществляют методическое руководство в организациях (на предприятиях);

Осуществляют контроль

1. Что делают Органы судебной власти?

Организуют работы по защите информации;

Осуществляют методическое руководство;

Осуществляют контроль

Осуществляют прокурорский контроль и принимают решение о привлечении к ответственности за нарушения в области

информационной безопасности.

1. Модели нарушителей информационной безопасности на объекте.

Две;

Три;

Четыре.

1. Типовая структура службы безопасности.

отдел защиты информации;

отдел режима и охраны, в составе сектора режима и сектора охраны;

инженерно-техническая группа;

отдел по борьбе с националистическими проявлениями;

группа безопасности внешней деятельности.

**Часть Б:**

1. Что понимается под национальной безопасностью РФ?
2. В чем заключаются национальные интересы РФ?
3. Какими факторами обусловлены угрозы национальным интересам РФ в международной сфере?
4. Назовите важнейшие задачи обеспечения информационной безопасности РФ.
5. Как влияют процессы информатизации общества на содержание национальной безопасности?
6. Назовите основные угрозы конституционным правам и свободам человека и гражданина.
7. Назовите основные угрозы информационному обеспечению государственной политики РФ.
8. Назовите основные угрозы безопасности информационных и телекоммуникационных средств и систем.
9. Что представляют собой внешние и внутренние источники угроз информационной безопасности РФ?
10. В чем состоит государственная политика обеспечения информационной безопасности РФ?
11. Какие действия предпринимает государство по совершенствованию правовых механизмов в области обеспечения информационной безопасности РФ?
12. На каких принципах должно базироваться правовое обеспечение информационной безопасности РФ?
13. Что понимается под информационным оружием? Представьте его классификацию.
14. Назовите основные виды и объекты воздействия в информационной войне.
15. Назовите отличительные особенности информации как продукта.
16. Какую информацию относят к открытой, конфиденциальной, секретной?
17. Что включает понятие «государственная тайна»?
18. Какова структура государственной системы информационной безопасности?
19. Какими полномочиями наделена ФСТЭК России? Какие задачи в области обеспечения информационной безопасности она решает?
20. Какими полномочиями наделена ФСБ России? Какие задачи в области обеспечения информационной безопасности она решает?
21. Какие задачи призвана решать государственная система обеспечения информационной безопасности?
22. Назовите основные категории источников конфиденциальной информации в информационных системах.
23. Что понимается под способом несанкционированного доступа к источнику конфиденциальной информации?
24. Какие способы несанкционированного доступа к источнику конфиденциальной информации Вам известны?
25. Укажите угрозы конфиденциальной информации.
26. В чем состоит правовая защита конфиденциальной информации?
27. Какими законами Российской Федерации регламентируется охранная деятельность?
28. В каких целях в Российской Федерации проводится лицензирование отдельных видов деятельности?
29. Какие виды деятельности подлежат лицензированию в области технической защиты информации?
30. Какой порядок установлен для лицензирования деятельности по технической защите конфиденциальной информации?
31. С какой целью проводится аттестация информационной системы? Каков порядок проведения аттестации?
32. С какой целью проводится сертификация средств защиты информации по требованиям безопасности информации?
33. Каков порядок сертификации средств защиты информации?
34. Какой порядок установлен для сертификации средств защиты информации зарубежного производства?
35. Каковы особенности механизма закрепления права на интеллектуальную собственность?
36. Кто выступает в качестве объекта и субъекта информационных правоотношений в системе авторского права?
37. Каковы особенности правового регулирования авторского и имущественного права при производстве и распространении программ для ЭВМ и баз данных?
38. Как должны действовать правообладатели при защите своего права на интеллектуальную собственность?
39. Каков порядок правового регулирования информационных отношений при производстве и распространении топологий интегральных микросхем?
40. Каковы особенности регулирования информационных отношений институтом патентного права?
41. Что относится к объектам изобретения, полезным моделям, промышленным образцам?
42. Кто может стать автором изобретения, полезной модели, промышленного образца?
43. В чем заключается разница между автором и правообладателем?
44. Что относится к персональным данным? Укажите их особенности.
45. Какие функции выполняет оператор персональных данных?
46. Назовите основные принципы обработки персональных данных.
47. В чем состоят права субъекта персональных данных?
48. В чем состоят обязанности оператора при сборе и обработке персональных данных?
49. Какие санкции могут быть наложены на оператора, его руководителей и должностных лиц при нарушении законодательства

о безопасности обработки персональных данных?

1. Назовите основные задачи Федеральных органов по контролю и надзору за соблюдением законодательства в области безопасности персональных данных.
2. Приведите примеры правонарушений в сфере компьютерной передачи информации.
3. Чем характеризуются признаки состава компьютерного преступления и из каких элементов оно может состоять?
4. В чем заключаются особенности расследования компьютерного преступления?
5. С какими факторами связаны проблемы судебного преследования за преступления в сфере компьютерной информации?
6. В чем заключается понятие международного информационного обмена.
7. Чем определяется правовой режим участия в международном обмене субъектов Российской Федерации?
8. Дайте краткую характеристику законодательству зарубежных стран в области защиты интеллектуальной собственности.
9. На чем основываются и чем характеризуются международные правовые аспекты защиты прав и свобод личности в связи с применением современных информационных технологий?
10. Какие примеры международного сотрудничества в области борьбы с преступностью в сфере информационных технологий Вам известны?

Учебники:

1. Барабаш П.А. Безопасность персональных данных. Учебное пособие Санкт-Петербург. : Политехника, 2012. - 167 с.
2. Доктрина информационной безопасности Российской Федерации.
3. Закон Российской Федерации «О государственной тайне».
4. Закон Российской Федерации «Об информации, информатизации и защите информации».
5. Закон Российской Федерации «О безопасности».
6. Закон Российской Федерации «О лицензировании отдельных видов деятельности».
7. Закон Российской Федерации «Об электронной цифровой подписи».
8. Закон Российской Федерации «О персональных данных».
9. Закон Российской Федерации «О техническом регулировании».
10. Закон Российской Федерации «О коммерческой тайне».
11. Закон Российской Федерации «Об обеспечении доступа к информации о деятельности судов в Российской Федерации».
12. Закон Российской Федерации «О частной детективной и охранной деятельности в Российской Федерации».
13. Закон Российской Федерации «Об оперативно-розыскной деятельности».
14. Руководящий документ Гостехкомиссии России. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. М: ГТК РФ, 1992.
15. Руководящий документ Гостехкомиссии России. Средства
16. вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности СВТ от НСД к информации. М.ТТК РФ, 1992.
17. Руководящий документ Гостехкомиссии России. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. М.: ГТК РФ, 1992.
18. Положение о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации. (Утверждено постановлением Правительства Российской Федерации от 31 августа 2006 г. №532).
19. Положение о сертификации средств защиты информации по требованиям безопасности информации. (Утверждено приказом председателя Г осударственной технической комиссии при Президенте Российской Федерации от 27 октября 1995 г. № 199).