Автономная некоммерческая организация
дополнительного профессионального образования
«Учебный центр «Информзащита»

УТВЕРЖДАЮ

Директор АНО ДПО «Учебный центр «Информзащита»

_____ / Степаненко А.А. /
(подпись)

«__» _____ 2018 г.

М.П

ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СЕТЕЙ НА БАЗЕ TCP/IP»

Сокращенное наименование: «БИТС»

Код: БТ153

Москва
2018

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ ... 3
2. ЦЕЛЬ РЕАЛИЗАЦИИ ПРОГРАММЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ ... 6
2.1 Характеристика вида профессиональной деятельности ... 6
а. Область профессиональной деятельности ... 6
б. Объекты профессиональной деятельности: ... 7
в. Виды профессиональной деятельности и решаемые задачи ... 7
3. ТРЕБОВАНИЯ К КВАЛИФИКАЦИИ ПОСТУПАЮЩЕГО НА ОБУЧЕНИЕ ... 9
4. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ... 10
4.1 Приобретаемые профессиональные компетенции ... 10
4.2 Приобретаемые знания, умения и навыки ... 11
5. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ... 14
5.1 Особенности организации учебного процесса ... 14
5.2 Порядок передачи Программы другой образовательной организации ... 14
5.3 Порядок внесения изменений в Программу ... 14
6. ФОРМЫ АТТЕСТАЦИИ И ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ... 16
6.1 Оценка качества освоения Программы ... 16
6.2 Оценочные материалы ... 17
7. УЧЕБНЫЙ ПЛАН ПРОГРАММЫ ... 18
7.1 Категории обучающихся ... 18
7.2 Формы обучения ... 18
7.3 Продолжительность (трудоёмкость) обучения ... 18
7.4 Режим занятий ... 18
7.5 План учебного процесса ... 19
7.6 Сводные данные по бюджету времени ... 28
8. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК ... 28
9. РАБОЧАЯ ПРОГРАММА УЧЕБНОГО КУРСА ... 29
9.1 Содержание учебных разделов (модулей, тем) ... 29
9.2 Лабораторный практикум ... 35
9.3 Семинары ... 36
9.4 Практические занятия ... 36
9.5 Примерная тематика курсовых работ ... 36
9.6 Учебно-методическое и информационное обеспечение ... 36
в) программное обеспечение: ... 47
9.7 Материально-техническое обеспечение учебного курса ... 48
9.8 Методические рекомендации по организации изучения учебного курса ... 49
9.9 Оценочные материалы ... 49
10. Перечень сведений, составляющих государственную тайну, используемых в учебном процессе ... 55

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая программа повышения квалификации «Безопасность информационных технологий и сетей на базе TCP/IP» (далее – «Программа») относится к дополнительным профессиональным программам в области информационной безопасности (далее - ИБ) и разработана с учетом положений:

- Федерального закона от 29 декабря 2012 г. № 273-03 «Об образовании в Российской Федерации»;
- Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам (утв. приказом Министерства образования и науки РФ от 1 июля 2013 г. № 499);
- Порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности (утв. приказом Министерства образования и науки РФ от 05 декабря 2013 г. № 1310);
- Методических рекомендаций по разработке программ профессиональной переподготовки и повышения квалификации специалистов, работающих в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия иностранным техническим разведкам и технической защиты информации, утвержденных ФСТЭК России 4 апреля 2015 г.;
- Методических рекомендаций-разъяснений по разработке дополнительных профессиональных программ на основе профессиональных стандартов (письмо Минобрнауки России от 22 апреля 2015 г. № ВЖ-1032/06).

Программа сформирована с учётом видов профессиональной деятельности, трудовых функций и уровней квалификации, установленных в профессиональных стандартах:

- «Специалист по защите информации в автоматизированных системах», утвержденного приказом Минтруда России от 15 сентября 2016 г. № 522н;
- «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Минтруда России от 1 ноября 2016 г. № 598н;

При разработке содержания Программы учтены требования обеспечения преемственности по отношению к федеральным государственным образовательным стандартам высшего образования (ФГОС ВО) по направлению подготовки «Информационная безопасность», а именно:

- ФГОС ВО по специальности 10.05.01 Компьютерная безопасность (уровень специалитета), утвержденного приказом Минобрнауки России от 1 декабря 2016 г. № 1512;
- ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (уровень специалитета), утвержденного приказом

Минобрнауки России от 1 декабря 2016 г. № 1509;

Программа повышения квалификации реализуется в АНО ДПО «Учебный центр «Информзащита».

Программа разработана в инициативном порядке в соответствии с Приказом Директора от «01» октября 2017 г. №01/10/17.

Программа обсуждена и одобрена на заседании Методического совета АНО ДПО «Учебный центр «Информзащита» «02» февраля 2018 г., протокол № 2 и утверждена Приказом Директора от «02» февраля 2018 г. № 01/02/18.

Разработчики:

- Ершов Дмитрий Вячеславович, к.т.н., заместитель директора по учебно-методической работе;
- Лепихин Владимир Борисович, заведующий кафедрой сетевой безопасности;
- Журавлёв Владимир Владимирович, заведующий кафедрой юридических проблем защиты конфиденциальной информации;
- Бондарев Валерий Васильевич, к.в.н., преподаватель;
- Нугаев Рашид Рустамович, преподаватель;
- Сотский Алексей Николаевич, преподаватель.

Обучение по данной Программе направлено на решение следующих основных задач:

- получение и углубление профессиональных знаний и умений обучающимися по правовым основам защиты информации, организационным мерам и техническим средствам обеспечения безопасности при использовании современных информационных технологий на предприятиях и в организациях;
- удовлетворение потребности специалистов в получении знаний об актуальных нормативных требованиях к защите и о новейших достижениях в области защиты конфиденциальной информации и систем её обработки (в приобретении или комплексном обновлении их профессиональных компетенций, в рамках указанного вида профессиональной деятельности);
- популяризация передовых технологий, подходов, решений, методов и средств обеспечения защиты конфиденциальной информации предприятий (объединений), организаций и учреждений, распространение передового опыта по успешному решению задач обеспечения информационной безопасности;
- оказание помощи предприятиям (объединениям), организациям и учреждениям в повышении квалификации руководителей и инженерно-технических работников (специалистов) служб безопасности и подразделений защиты информации по вопросам построения и эффективного применения комплексных систем и средств защиты информации;
- повышение квалификации руководителей и инженерно-технических работников

(специалистов по защите информации) предприятий и организаций, в соответствии с квалификационными требованиями к персоналу в штате у соискателя лицензии (лицензиата) на осуществление лицензируемых видов деятельности по направлениям ФСТЭК России.

2. ЦЕЛЬ РЕАЛИЗАЦИИ ПРОГРАММЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Целью реализации Программы является повышение профессионального уровня обучающихся (слушателей) в рамках имеющейся квалификации, формирование и (или) совершенствование у них компетенций, необходимых для выполнения трудовых функций (должностных обязанностей) в рамках профессиональной деятельности по обеспечению информационной безопасности автоматизированных систем и обеспечению защищенности объектов информатизации на базе компьютерных систем и сетей.

Программа направлена на формирование у слушателей знаний по проблематике и умений по основам обеспечения безопасности предприятий и организаций при использовании ими (в целях повышения эффективности управления) информационных технологий на базе современных средств автоматизированной обработки и передачи информации. Особое внимание в первом модуле Программы уделяется рассмотрению технологии обеспечения информационной безопасности, подходов к рациональному распределению функций и ответственности по вопросам защиты информации и организации эффективного взаимодействия всех подразделений и сотрудников, использующих и обеспечивающих функционирование автоматизированных систем, вопросам регламентации их деятельности и разработки нормативно-методических и организационно-распорядительных документов с учетом требований российского законодательства, национальных и международных стандартов, необходимых для реализации рассмотренной технологии обеспечения информационной безопасности.

Обучение по Программе второго модуля имеет целью формирование и (или) совершенствование у слушателей теоретических знаний по источникам угроз и причинам появления уязвимостей компьютерных сетей, возможностям и недостаткам основных защитных механизмов, типичным приемам и инструментам, используемым нарушителями, по типовым хакерским атакам на сетевые протоколы и службы, а также практических умений использования решений обеспечения безопасности корпоративных сетей и рационального выбора средств защиты информации в компьютерных сетях.

Значительная часть курса посвящена практической работе со средствами поиска уязвимостей систем и обнаружения атак (как свободно распространяемых, так и коммерческих) на специальных реконфигурируемых стендах, позволяющих моделировать реальные корпоративные сети предприятий.

2.1 Характеристика вида профессиональной деятельности

a. **Область профессиональной деятельности** слушателей, обучающихся по Программе, включает сферы техники и технологий, охватывающие совокупность проблем, связанных с:
   - анализом, оценкой и обеспечением требуемого уровня защищенности компьютерных систем и сетей от вредоносных программно-технических воздействий;
   - защитой информации в автоматизированных системах управления и

обеспечением их безопасности в условиях существования угроз в информационной сфере;
- эксплуатацией и администрированием средств и систем защиты информации компьютерных систем.

б. Объекты профессиональной деятельности:
- объекты информатизации, включающие автоматизированные информационные системы, входящие в них средства обработки, хранения и передачи информации и информационно-технологические ресурсы, подлежащие защите и функционирующие в условиях существования угроз в информационной сфере;
- угрозы безопасности и технологии обеспечения информационной безопасности автоматизированных систем;
- системы управления информационной безопасностью автоматизированных систем;
- методы и реализующие их средства защиты информации в компьютерных системах и сетях;
- процессы, возникающие при защите информации, обрабатываемой в компьютерных системах;
- методы и реализующие их системы и средства контроля эффективности защиты информации в компьютерных системах;
- система нормативных правовых актов, методических документов и национальных стандартов в области информационной безопасности.

в. Виды профессиональной деятельности и решаемые задачи

Программа ориентирована на подготовку слушателей к следующим видам профессиональной деятельности:
- организационно-управленческая;
- проектная;
- контрольно-аналитическая.

Слушатели, успешно завершившие обучение по данной Программе, должны решать следующие задачи в соответствии с видами профессиональной деятельности:
- **в организационно-управленческой деятельности:**
  - планирование и управление информационной безопасностью объекта;
  - организация работ по выполнению требований режима защиты информации, в том числе информации ограниченного доступа;
  - осуществление организационно-правового обеспечения информационной безопасности объекта защиты;
  - разработка нормативных и методических документов, регламентирующих работу по защите информации и иных организационно-распорядительных документов;
  - организация работы малых коллективов исполнителей с учетом требова-

ний защиты информации;

- анализ безопасности распределенных компьютерных систем, защиты информации в них, мониторинг, аудит и контрольные проверки их работоспособности и защищенности;
- организация защиты информации в распределенных компьютерных системах, включая формирование, реализацию и контроль эффективности политики их информационной безопасности;
- участие в определении потребности в средствах защиты информации, контроль их поставки и эксплуатации;
- внедрение методов и средств обеспечения безопасности объектов информатизации на основе компьютерных систем и сетей.

– **в проектной деятельности:**
  - сбор и анализ исходных данных для проектирования систем защиты информации;
  - определение угроз безопасности автоматизированных информационных систем на объектах информатизации и рисков от их реализации;
  - формирование требований к обеспечению безопасности информации в автоматизированных информационных системах;
  - разработка предложений по применению конкретных способов, методов и программно-аппаратных средств обеспечения безопасности информации и иных ресурсов в компьютерных системах и сетях;
  - поиск рациональных решений при выборе средств защиты информации с учетом требований качества, надежности и стоимости, а также сроков исполнения.
– **в контрольно-аналитическая деятельности:**
  - контроль эффективности реализации политики информационной безопасности объекта;
  - проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средствах защиты информации;
  - предварительная оценка, выбор и разработка необходимых методик поиска уязвимостей;
  - применение методов и методик оценивания безопасности компьютерных систем при проведении контрольного анализа системы защиты;
  - участие в обследовании объектов информатизации, их категорировании и аттестации по требованиям безопасности информации;
  - участие в экспериментально-исследовательских работах при аттестации объектов с учетом требований к обеспечению защищенности компьютерной системы;
  - проведение инструментального мониторинга защищенности

компьютерных систем;

- подготовка аналитического отчета по результатам проведенного анализа и выработка предложений по устранению выявленных уязвимостей.

3. ТРЕБОВАНИЯ К КВАЛИФИКАЦИИ ПОСТУПАЮЩЕГО НА ОБУЧЕНИЕ

Лица, желающие освоить Программу, должны иметь высшее образование, или получать высшее образование (проходить обучение в настоящее время), при условии, что они получат дипломы о первичном образовании в период прохождения обучения по Программе. Кандидаты на зачисление на обучение по данной Программе документально подтверждают свой уровень образования, предоставляя копии и предъявляя документы об образовании государственного или установленного образца.

Поступающим на обучение желательно иметь стаж работы (не менее 1 года), связанной с процессами обеспечения информационной безопасности в компаниях или организациях, или связанного с внедрением и эксплуатацией автоматизированных информационных систем и компьютерных сетей.

4. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

4.1 Приобретаемые профессиональные компетенции

Процесс освоения обучающимися данной Программы направлен на формирование и(или) совершенствование у них следующих компетенций[1]:

а) общепрофессиональных**:**

способность понимать сущность и значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска и обработки больших объемов информации по профилю деятельности в глобальных компьютерных системах, сетях, в библиотечных фондах и в иных источниках информации (ОПК-3);

способность использовать нормативные правовые акты, методические документы, международные и национальные стандарты в области защиты информации в своей профессиональной деятельности (ОПК-5);

способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности (ОПК-7);

способность определять виды и формы информации, подверженной угрозам, возможные методы реализации угроз на основе анализа структуры и содержания информационных процессов организации, целей и задач деятельности объекта защиты;

способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах (ОПК-11).

б) профессиональных:

В проектной деятельности:

способность разрабатывать модели угроз, формировать требования к обеспечению информационной безопасности объектов информатизации на базе компьютерных систем и сетей;

способность проводить сбор и анализ исходных данных для проектирования систем защиты информации (ПК-21);

способность участвовать в разработке системы защиты информации предприятия (организации) и подсистемы информационной безопасности компьютерной системы (ПК-24);

В организационно-управленческой деятельности:

способность организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности (ПК-30);

способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы (ПК-32);

---

[1] Коды компетенций указаны в соответствии с ФГОС ВО 10.05.01

способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности (ПК-33);

В контрольно-аналитической деятельности:

способность участвовать в проведении экспериментального исследования компьютерных систем с целью выявления уязвимостей (ПК-27).

4.2 Приобретаемые знания, умения и навыки

Освоившие программу обучающиеся (слушатели) должны:

а) **знать:**

- сущность понятия «информационная безопасность», характеристики ее составляющих;
- место и роль информационной безопасности в системе национальной безопасности Российской Федерации;
- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСТЭК России, ФСБ России в данной области;
- основы построения информационных систем и формирования информационных ресурсов ограниченного доступа;
- правовые основы организации защиты государственной тайны и конфиденциальной информации;
- основы лицензирования деятельности по технической защите информации и деятельности по разработке и производству средств защиты информации;
- основы действующей системы сертификации средств защиты информации по требованиям безопасности информации;
- принципы построения и управления системой обеспечения информационной безопасности в ведомстве (организации, на предприятии);
- источники угроз информационной безопасности;
- механизмы реализации вредоносных программно-технических и информационных воздействий в компьютерных системах;
- методы и способы несанкционированного доступа (НСД) к информации, способы и средства защиты от НСД к информации на объектах информатизации;
- принципы организации информационных систем в соответствии с требованиями по защите информации;
- систему организации комплексной защиты информации ограниченного доступа, включая защиту персональных данных;
- требования по составу и характеристикам подсистем защиты информации для различных классов защищенных систем, методы их практической реализации;
- основные виды политик управления доступом и информационными потоками в компьютерных системах;
- методы и способы защиты информации;

- защитные механизмы и средства обеспечения сетевой безопасности;
- современные программно-аппаратные средства и способы обеспечения информационной безопасности в компьютерных системах;
- средства и методы предотвращения и обнаружения вторжений;
- основные средства и методы анализа уязвимостей программных средств;
- требования по составу и характеристикам подсистем защиты информации для различных классов защищенных систем, методы их практической реализации;
- современные программно-аппаратные средства и способы обеспечения информационной безопасности в компьютерных системах и сетях;
- защищённые протоколы IPsec, SSL, SSH;
- существующие криптографические схемы и алгоритмы, используемые в виртуальных частных сетях;

б) уметь:

- проводить информационные обследования, анализировать и оценивать угрозы информационной безопасности объекта;
- пользоваться нормативными документами по защите информации;
- планировать защиту и рационально распределять соответствующие функции и ответственность между подразделениями и сотрудниками предприятия, организовывать их взаимодействие на различных этапах жизненного цикла автоматизированных систем;
- участвовать в организации деятельности служб технической защиты информации в действующих и проектируемых системах защиты информации;
- разрабатывать концепции, политики и иные организационно-распорядительные документы, необходимые для эффективного функционирования комплексных систем информационной безопасности объектов информатизации в организации;
- формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе;
- оценивать полноту и качество выполнения работниками организации требований политики безопасности;
- ориентироваться в проблемах информационной безопасности в сетях Интернет/Интранет, уязвимостях сетевых протоколов и служб, атаках в IP-сетях;
- ориентироваться в средствах защиты информации от несанкционированного доступа, межсетевых экранах, средствах контроля контента, средствах анализа защищенности и средствах обнаружения атак для обеспечения информационной безопасности в IP-сетях;
- организовывать поиск и использование оперативной информации о новых уязвимостях в системном и прикладном программном обеспечении, а также других актуальных для обеспечения информационной безопасности данных;
- осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;
- анализировать и оценивать угрозы информационной безопасности в сетях;
- работать со средствами выявления уязвимостей и обнаружения сетевых атак;

- использовать сетевые анализаторы для мониторинга трафика;
- использовать хакерские инструменты: Cain, Nmap, Netcat и другие;
- управлять пакетным фильтром на базе Linux;
- квалифицированно использовать протоколы защиты трафика: IPsec, SSL;
- обоснованно выбирать необходимые программные и программно-аппаратные средства защиты информации в автоматизированных системах на базе компьютерных сетей;
- строить «сети-приманки» для изучения поведения нарушителей.

в) **владеть навыками:**

- работы с действующей нормативной правовой и методической базой в области ЗИ и оценки защищенности ресурсов в компьютерных системах и сетях;
- определения задач, проведения организационных и технических мероприятий по ЗИ.
- выявления и оценки угроз безопасности информации в компьютерных системах и сетях.

5. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

5.1 Особенности организации учебного процесса

Обучение по Программе осуществляется единовременно (без разрывов), в порядке, определённом образовательной программой на основе договоров об обучении. Форма обучения и конкретные сроки освоения Программы определяются с учётом расписания курсов в Учебном центре и указываются в договоре об обучении.

При использовании дистанционных образовательных технологий (онлайн-вебинаров) слушатели из других часовых поясов должны учитывать, что занятия с онлайн-трансляцией (онлайн-вебинары) проводятся по рабочим дням с 10:00 до 17:30 по московскому времени. При наличии групп слушателей из удалённых регионов (одного или смежных часовых поясов) для них занятия могут быть проведены в иное, специально назначенное для этого, время (с учётом сдвига по времени).

Доступ к электронным учебным пособиям, к системе тестирования, а также к стендам (виртуальным машинам в центре обработки данных - ЦОД) для дистанционного выполнения лабораторных (практических) работ должен предоставляется слушателям круглосуточно.

Предоставление прав и реквизитов удалённого доступа обучающихся к их «личным кабинетам» и назначенным им курсам и тестам целесообразно осуществлять на весь период обучения по Программе. Контроль за прохождением этапов обучения слушателей должен вестись как лицами, ответственными за СДО и обеспечение проведения занятий с применением дистанционных технологий, и преподавателями, ведущими занятия, так и менеджерами, отвечающими за договора об обучении конкретных слушателей.

5.2 Порядок передачи Программы другой образовательной организации

Передача Учебным центром настоящей дополнительной профессиональной программы другим образовательным организациям не предусматривается.

Передача Программы повышения квалификации другой образовательной организации допускается при создании необходимых условий её реализации и соблюдении требований законодательства Российской Федерации о порядке обращения со служебной информацией ограниченного распространения и наличии разрешения органов управления, в ведении которых находятся организации, осуществляющие образовательную деятельность.

5.3 Порядок внесения изменений в Программу

Внесение изменений в настоящую дополнительную профессиональную программу осуществляются в соответствии с требованиями, установленными законодательными и иными нормативными правовыми актами Российской Федерации в области образования, защиты государственной тайны и информационной безопасности.

Перечень основной литературы может дополняться руководителями образовательных организаций при поступлении новых (уточненных) учебных пособий.

Перечень дополнительной литературы подлежит обновлению и (или) уточнению, с учетом введения в действие новых и утративших актуальность нормативных правовых актов и методических документов.

Незначительные правки, вызванные изменениями в нормативной базе или в составе учебных дисциплин (модулей, курсов) вносятся в рабочем порядке.

Существенные изменения в программу рассматривается Методическим советом Учебного центра, а сама Программа повторно утверждается директором Учебного центра и проходит процедуру согласования в установленном порядке.

6. ФОРМЫ АТТЕСТАЦИИ И ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

6.1 Оценка качества освоения Программы

Система оценки качества освоения Программы включает текущий контроль успеваемости (контроль посещаемости и активности на занятиях, опросы в начале очередного учебного дня, контроль выполнения практических и лабораторных работ), промежуточные по завершении освоения каждой учебной дисциплины (модуля, курса) Программы и итоговую аттестацию обучающихся.

Освоение каждой дисциплины (модуля, курса) Программы завершается зачетом (без оценки) в форме теста, который подразумевает ответы на контрольные вопросы по материалу курса. Зачет проводится с использованием электронной системы тестирования (основной вариант) или в бумажной форме (резервный вариант). Зачет принимает преподаватель, ведущий занятия по данной дисциплине.

Если краткосрочная программа повышения квалификации состоит только из одной учебной дисциплины (курса, модуля), то для неё промежуточная аттестация по дисциплине (курсу, модулю) является одновременно и итоговой по Программе.

Для каждого теста разработана система оценки, параметрами которой являются количество вопросов, их сложность, полнота ответа на вопрос. По результатам ответа на вопрос испытуемому присваивается определенное системой оценки количество баллов. Итоговое решение о прохождении теста принимается на основании превышения суммарно набранного количества баллов по всем вопросам над определенным системой оценки пороговым значением.

При использовании средств электронного тестирования, тесты для промежуточной аттестации по каждой учебной дисциплине (модулю, курсу) содержат от 10 до 30 вопросов. К каждому вопросу предлагается по четыре варианта ответов, только один из которых правильный (наиболее точный и полный). Проходной бал зачёта 2/3 правильных ответов.

Итоговая аттестация слушателей проводится в форме тестирования (обычно в электронном виде) по основным темам изученных дисциплин (модулей, курсов).

Тест итоговой аттестации для каждого слушателя формируется индивидуально и содержит 45 вопросов, выбираемых системой случайным образом из пула в 120 вопросов, сформированного из тестовых вопросов изучаемых дисциплин (модулей, курсов). Проходной бал зачёта 2/3 правильных ответов.

На прохождение теста отводится полтора часа (2 академических часа).

По результатам успешного тестирования и собеседования по каждому слушателю оформляется отдельное решение о прохождении (не прохождении) итоговой аттестации. В случае неуспешной попытки сдачи итогового теста, слушателю предоставляется время на самоподготовку и возможность повторно пройти тестирование.

Лицам, успешно освоившим Программу повышения квалификации, выполнившим все требования учебного плана и прошедшим итоговую аттестацию, выдается Удостоверение о повышении квалификации установленного образца.

Слушателям, не прошедшим итоговой аттестации или показавшим на итоговой аттестации неудовлетворительные результаты, а также слушателям, освоившим лишь

часть Программы и/или отчисленным из организации, выдается справка об обучении (а также Свидетельства о прохождении обучения по отдельным модулям (курсам) Программы).

При освоении Программы слушателем параллельно с получением высшего образования Удостоверение о повышении квалификации выдаётся ему после получения соответствующего документа об основном образовании и о квалификации.

6.2 Оценочные материалы

Оценочные материалы по Программе включают наборы тестовых вопросов, используемые для контроля усвоения материала при проведении промежуточных аттестаций по каждой учебной дисциплине (курсу, модулю), а также скомпонованный из них пул тестов итоговой аттестации, реализуемые в рамках системы дистанционного тестирования на базе сервера управления обучением и тестированием Учебного центра.

Основные вопросы, включаемые в оценочные материалы промежуточных аттестаций приведены в соответствующих Рабочих программах по данным дисциплинам (модулям, курсам).

Перечень вопросов Итоговой аттестации (для экзамена) формируется из перечней основных вопросов, выносимых для контроля знаний обучающихся при проведении промежуточных аттестаций по учебным дисциплинам (курсам, модулям) Программы.

Основные группы тестовых вопросов, выносимые на итоговую аттестацию:

1. Основные понятия ИБ и ЗИ	15 вопросов, случайная выборка 6
2. Правовые вопросы	18 вопросов, случайная выборка 5
4. Организационные вопросы	14 вопросов, случайная выборка 4
5. Защитные механизмы	12 вопросов, случайная выборка 4
6. Средства сетевой безопасности	16 вопросов, случайная выборка 5
7. Штатные и дополнительные СЗИ от НСД	25 вопросов, случайная выборка 5
8. Безопасность компьютерных сетей	23 вопроса, случайная выборка 5

7. УЧЕБНЫЙ ПЛАН ПРОГРАММЫ

7.1 Категории обучающихся

Программа ориентирована на следующие категории обучающихся (слушателей):

- начальники служб безопасности, руководители подразделений обеспечения информационной безопасности (ОИБ), технической защиты (конфиденциальной) информации (ТЗИ, ТЗКИ), ответственные за состояние и обеспечение ИБ и организацию работ по созданию комплексных систем защиты конфиденциальной информации предприятий;
- аналитики подразделений ОИБ (ТЗКИ), отвечающие за анализ состояния информационной безопасности, определение требований к защищенности различных подсистем ИС и путей обеспечения их защиты, а также за разработку необходимых нормативно-методических и организационно-распорядительных документов по вопросам защиты информации;
- администраторы средств защиты и специалисты подразделений ОИБ (ТЗКИ), ответственные за защиту конфиденциальной информации техническими средствами.

7.2 Формы обучения

Программа реализуется в форме обучения с отрывом от основной работы при проведении обучения в очной форме, - с частичным отрывом от работы, при обучении с использованием дистанционных образовательных технологий (онлайн-вебинаров) и/или электронного обучения.

7.3 Продолжительность (трудоёмкость) обучения

Общий объём времени, отводимого на освоение данной Программы, составляет 96 часов, включая 80 академических часов аудиторных занятий (включая зачёты) и 16 академических часов самостоятельной учебной работы слушателя.

7.4 Режим занятий

Режим занятий: 8 академических часов учебных (аудиторных) занятий с преподавателем и 1 час самостоятельной работы в день.

Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

Учебные занятия организованы в одну смену. Время проведения очных занятий и онлайн-вебинаров - по рабочим дням с 10:00 до 17:30 по московскому времени. Доступ к электронным учебным пособиям и виртуальным стендам (в центре обработки данных - ЦОД) для дистанционного выполнения лабораторных работ предоставляется слушателям круглосуточно.

7.5 План учебного процесса

№№ п/п	Наименование учебных модулей, разделов (тем)	Всего учебных часов	Часы занятий с преподавателем	Распределение времени по видам занятий, час					Самостоятельная работа обучающихся	Формы аттестации и контроля знаний
				Лекции	Семинары	Практические занятия	Лабораторные работы	Промежуточная аттестация		
	МОДУЛЬ 1. Безопасность информационных технологий									
1.	**Раздел I**. Основы безопасности информационных технологий	**18**		**16**					**2**	Опрос на лекции
1.1.	Тема 1: Актуальность проблемы обеспечения безопасности информационных технологий.	2		2						
1.2.	Тема 2: Основные понятия в области безопасности информационных технологий.	2,5		2					0.5	
1.3.	Тема 3: Угрозы безопасности информационных технологий.	2,5		2					0.5	
1.4.	Тема 4: Виды мер и основные принципы обеспечения безопасности информационных технологий.	2		2						
1.5.	Тема 5: Правовые основы обеспечения безопасности информационных технологий.	6		6						
1.6.	Тема 6: Государственная система защиты информации.	1,5		1					0.5	
1.7.	Тема 7: Основные защитные механизмы,	1,5		1					0.5	

№№ п/п	Наименование учебных модулей, разделов (тем)	Всего учебных часов	Часы занятий с преподавателем	Распределение времени по видам занятий, час					Самостоятельная работа обучающихся	Формы аттестации и контроля знаний
				Лекции	Семинары	Практические занятия	Лабораторные работы	Промежуточная аттестация		
	реализуемые в рамках различных мер и средств защиты.									
2.	**Раздел II.** Обеспечение безопасности информационных технологий	**14**		**12**					**2**	Опрос на лекции
3.	Тема 8: Организационная структура системы обеспечения безопасности информационных технологий.	2,5		2					0.5	
3.1.	Тема 9: Обязанности конечных пользователей и ответственных за обеспечение безопасности информационных технологий в подразделениях.	2		2						
3.2.	Тема 10: Документы, регламентирующие правила парольной и антивирусной защиты.	1		1						
3.3.	Тема 11: Документы, регламентирующие порядок допуска к работе и изменения полномочий пользователей автоматизированной системы.	1		1						
3.4.	Тема 12: Документы, регламентирующие порядок изменения конфигурации аппаратно-	1		1						

№№ п/п	Наименование учебных модулей, разделов (тем)	Всего учебных часов	Часы занятий с преподавателем	Распределение времени по видам занятий, час					Самостоятельная работа обучающихся	Формы аттестации и контроля знаний
				Лекции	Семинары	Практические занятия	Лабораторные работы	Промежуточная аттестация		
	программных средств автоматизированной системы.									
3.5.	Тема 13: Регламентация процессов разработки, испытания, опытной эксплуатации, внедрения и сопровождения задач.	1.5		1					0.5	
3.6.	Тема 14: Определение требований к защите и категорирование ресурсов. Проведение информационных обследований и анализ подсистем автоматизированной системы как объекта защиты.	1.5		1.5						
3.7.	Тема 15: Планы защиты и планы обеспечения непрерывной работы и восстановления подсистем автоматизированной системы.	1.5		1.5						
3.8.	Тема 16: Основные задачи подразделений обеспечения безопасности информационных технологий. Организация работ по обеспечению безопасности информационных технологий.	1		0.5					0.5	
3.9.	Тема 17: Концепция безопасности информационных	1		0.5					0.5	

№№ п/п	Наименование учебных модулей, разделов (тем)	Всего учебных часов	Часы занятий с преподавателем	Распределение времени по видам занятий, час					Самостоятельная работа обучающихся	Формы аттестации и контроля знаний
				Лекции	Семинары	Практические занятия	Лабораторные работы	Промежуточная аттестация		
	технологий предприятия (организации).									
4.	**Раздел III.** Средства защиты информации от несанкционированного доступа	**6**		**3**		**1**			**2**	Опрос на лекции
4.1.	Тема 18: Назначение и возможности средств защиты информации от несанкционированного доступа.	1.5		1					0.5	
4.2.	Тема 19: Рекомендации по выбору средств защиты информации от несанкционированного доступа.	1.5		1					0.5	
4.3.	Тема 20: Аппаратно-программные средства защиты информации от несанкционированного доступа.	1.5		1					0.5	
4.4.	Тема 21: Возможности применения штатных и дополнительных средств защиты информации от несанкционированного доступа.	1.5				1			0.5	
5.	**Раздел IV.** Обеспечение безопасности компьютерных систем и сетей	**8**		**5**		**1**			**2**	Опрос на лекции
5.1.	Тема 22: Проблемы обеспечения безопасности в компьютерных системах и сетях.	1		1						

№№ п/п	Наименование учебных модулей, разделов (тем)	Всего учебных часов	Часы занятий с преподавателем	Распределение времени по видам занятий, час					Самостоятельная работа обучающихся	Формы аттестации и контроля знаний
				Лекции	Семинары	Практические занятия	Лабораторные работы	Промежуточная аттестация		
5.2.	Тема 23: Назначение, возможности и основные защитные механизмы межсетевых экранов.	1		1						
5.3.	Тема 24: Анализ содержимого почтового и Web-трафика (Content Security).	1.5		1					0.5	
5.4.	Тема 25: Виртуальные частные сети.	1		0.5					0.5	
5.5.	Тема 26: Антивирусные средства защиты.	1				1				
5.6.	Тема 27: Обнаружение и устранение уязвимостей. Возможности сканеров уязвимостей.	1.5		1					0.5	
5.7.	Тема 28: Мониторинг событий безопасности.	1		0.5					0.5	
	Промежуточное тестирование	2						2		Зачёт в форме тестирования
	Итого по Модулю 1:	**48**		**36**		**2**		**2**	**8**	
	МОДУЛЬ 2. Безопасность компьютерных сетей									
1.	**Введение.** Стек протоколов TCP/IP	**10**	**8**	**4**			**4**		**2**	Опрос на лекции
1.1.	Базовые принципы сетевого взаимодействия	0,5	0,5	0,5			0			
1.2.	Обзор современных сетевых технологий	1,5	1	0,5			0,5		0,5	
1.3.	Обзор современных сетевых протоколов	1	0,5	0,5			0		0,5	

№№ п/п	Наименование учебных модулей, разделов (тем)	Всего учебных часов	Часы занятий с преподавателем	Распределение времени по видам занятий, час					Самостоятельная работа обучающихся	Формы аттестации и контроля знаний
				Лекции	Семинары	Практические занятия	Лабораторные работы	Промежуточная аттестация		
1.4.	Организация взаимодействия со средой передачи в стеке TCP/IP	1,5	1	0,5			0,5		0,5	
1.5.	Сетевой уровень в стеке TCP/IP. Протокол IP как основа межсетевого взаимодействия	1,5	1,5	0,5			1			
1.6.	Транспортный уровень в стеке TCP/IP	2	1,5	0,5			1			
1.7.	Службы прикладного уровня	1	1	0,5			0,5			
1.8.	Электронная почта	1	1	0,5			0,5		0,5	
2.	**Тема 1.** Безопасность компьютерных сетей	**2**	**1**	**1**					**1**	Опрос на лекции
2.1.	Типовая IP-сеть организации Классификация сетевых уязвимостей и атак. Работа с базами атак и уязвимостей	1	0,5	0,5					0,5	
2.2.	Базовые принципы сетевого взаимодействия. Защитные механизмы и средства обеспечения безопасности	1	0,5	0,5					0,5	
3.	**Тема 2.** Безопасность физического и канального уровней	**2**	**2**	**1**			**1**			
3.1.	Технология Ethernet. Адресация на канальном уровне	1	1	0,5			0,5			
3.2.	Сетевые анализаторы. Изучение трафика атаки	1	1	0,5			0,5			

№№ п/п	Наименование учебных модулей, разделов (тем)	Всего учебных часов	Часы занятий с преподавателем	Распределение времени по видам занятий, час					Самостоятельная работа обучающихся	Формы аттестации и контроля знаний
				Лекции	Семинары	Практические занятия	Лабораторные работы	Промежуточная аттестация		
4.	**Тема 3.** Проблемы безопасности протокола разрешения адресов ARP	**2**	**2**	**1**			**1**			
4.1.	Назначение, схема работы и атаки на протокол ARP	1	1	0,5			0,5			
4.2.	Направления защиты от атак на протокол ARP	1	1	0,5			0,5			
5.	**Тема 4.** Стандарт 802.1x. Безопасность на уровне порта	**2**	**2**	**1**			**1**			
5.1.	Стандарт IEEE802.1x	1	1	0,5			0,5			
5.2.	Протокол аутентификации EAP	1	1	0,5			0,5			
6.	**Тема 5.** Безопасность сетевого уровня модели OSI	**2**	**2**	**1**			**1**			
6.1.	Атаки на протокол IP	1	1	0,5			0,5			
6.2.	Протокол ICMP с точки зрения безопасности	1	1	0,5			0,5			
7.	**Тема 6.** Защита периметра сети	**6**	**3**	**1**			**2**		**3**	
7.1.	Базовые принципы защиты периметра	4	1	1					3	
7.2.	Пакетный фильтр в ОС Linux	1	1				1			
7.3.	Многофункциональные межсетевые экраны	1	1				1			
8.	**Тема 7.** Виртуальные частные сети	**3**	**3**	**1**			**2**			
8.1.	Разновидности и реализации VPN-технологий	1	1	1						
8.2.	Настройка IPsec средствами Windows	1	1				1			
8.3.	Организация удалённого доступа	1	1				1			

№№ п/п	Наименование учебных модулей, разделов (тем)	Всего учебных часов	Часы занятий с преподавателем	Распределение времени по видам занятий, час					Самостоятельная работа обучающихся	Формы аттестации и контроля знаний
				Лекции	Семинары	Практические занятия	Лабораторные работы	Промежуточная аттестация		
9.	**Тема 8.** Проблемы безопасности протокола IP версии 6	**1**	**1**	**1**						
9.1.	Протокол IP версии 6	0,5	0,5	0,5						
9.2.	Рекомендации по безопасному использованию протокола IP версии 6	0,5	0,5	0,5						
10.	**Тема 9.** Безопасность транспортного уровня модели OSI	**2**	**2**	**1**			**1**			
10.1.	Уязвимости протокола TCP, подмена участника соединения	1	1	0,5			0,5			
10.2.	Атака SYNFlood	1	1	0,5			0,5			
11.	**Тема 10.** Защита трафика на прикладном уровне	**3**	**3**	**1**			**2**			
11.1.	Протоколы защиты данных прикладного уровня	1	1	0,5			0,5			
11.2.	Технологии туннелирования трафика	1	1	0,5			0,5			
11.3.	Атаки на протокол SSL	1	1				1			
12.	**Тема 11.** Анализ защищённости корпоративной сети	**2**	**2**	**1**			**1**			
12.1.	Инвентаризация сетевых ресурсов	1	1	0,5			0,5			
12.2.	Выявление уязвимостей	1	1	0,5			0,5			
13.	**Тема 12.** Обнаружение сетевых атак	**3**	**2**	**1**			**1**		**1**	
13.1.	Технология обнаружения атак	2	1	1					1	

№№ п/п	Наименование учебных модулей, разделов (тем)	Всего учебных часов	Часы занятий с преподавателем	Распределение времени по видам занятий, час					Самостоятельная работа обучающихся	Формы аттестации и контроля знаний
				Лекции	Семинары	Практические занятия	Лабораторные работы	Промежуточная аттестация		
13.2.	Архитектура систем обнаружения атак	1	1				1			
14.	**Тема 13.** Проблемы безопасности служб прикладного уровня	**4**	**3**	**1**			**2**		**1**	
14.1.	Уязвимости протокола DHCP	2	1,5	0,5			1		0,5	
14.2.	Служба DNS с точки зрения безопасности	2	1,5	0,5			1		0,5	
15.	**Тема 14.** Honeynet или сеть-приманка	**2**	**2**	**1**			**1**			
15.1.	Классификация и сценарии использования сетей-приманок	1	1	0,5			0,5			
15.2.	Использование утилиты honeyd	1	1	0,5			0,5			
	Итоговое тестирование	**2**						**2**		Зачёт в форме тестирования
	Итого по Модулю 2:	**48**	**38**	**18**			**20**	**2**	**8**	
	Итого по Курсу:	**96**	**76**	**54**		**2**	**20**	**4**	**16**	

7.6 Сводные данные по бюджету времени

Общий объем времени, отводимого на освоение программы (календарных дней/часов)			Распределение учебного времени (количество часов)					
Всего	Из них		Всего часов учебных занятий	В том числе		Время на самостоятельную работу	Итоговая аттестация	Резерв учебного времени
	Выходные, праздничные дни	Учебное время		Учебные занятия по расписанию	Практика			
14/96	**2**	**12/48**	**96**	**76**	**-**	**16**	**4**	**-**

8. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Срок обучения по программе повышения квалификации, месяцы	1	
Срок обучения по программе повышения квалификации, недели	1	
Виды занятий, предусмотренные программой повышения квалификации	А	И

А – аудиторная и самостоятельная работа

И – Итоговая аттестация

9. РАБОЧАЯ ПРОГРАММА УЧЕБНОГО КУРСА

9.1 Содержание учебных разделов (модулей, тем)

Модуль 1. Безопасность информационных технологий

Раздел 1. Основы безопасности информационных технологий

Актуальность проблемы обеспечения безопасности информационных технологий. Место и роль автоматизированных систем в управлении бизнес-процессами. Основные причины обострения проблемы обеспечения безопасности информационных технологий.

Основные понятия в области безопасности информационных технологий. Что такое безопасность информационных технологий. Информация и информационные отношения. Субъекты информационных отношений, их интересы и безопасность, пути нанесения им ущерба. Основные термины и определения. Конфиденциальность, целостность, доступность. Объекты, цели и задачи защиты автоматизированных систем и циркулирующей в них информации.

Угрозы безопасности информационных технологий. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем. Угрозы безопасности информации, автоматизированных систем и субъектов информационных отношений. Основные источники и пути реализации угроз. Классификация угроз безопасности и каналов проникновения в автоматизированную систему и утечки информации. Основные непреднамеренные и преднамеренные искусственные угрозы. Неформальная модель нарушителя.

Виды мер и основные принципы обеспечения безопасности информационных технологий. Виды мер противодействия угрозам безопасности. Достоинства и недостатки различных видов мер защиты. Основные принципы построения системы обеспечения безопасности информации в автоматизированной системе.

Правовые основы обеспечения безопасности информационных технологий. Законы Российской Федерации и другие нормативные правовые акты, руководящие и нормативно-методические документы, регламентирующие отношения субъектов в информационной сфере и деятельность организаций по защите информации. Защита информации ограниченного доступа, права и обязанности субъектов информационных отношений. Лицензирование деятельности, сертификация средств защиты информации и аттестация объектов информатизации. Требования руководящих документов ФСТЭК России и ФСБ России. Вопросы законности применения средств защиты информации. Ответственность за нарушения в сфере защиты информации.

Государственная система защиты информации. Состав государственной системы защиты информации. Организация защиты информации в системах и средствах информатизации и связи. Контроль состояния защиты информации. Финансирование мероприятий по защите информации.

Основные защитные механизмы, реализуемые в рамках различных мер и

средств защиты. Идентификация и аутентификация пользователей. Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированных систем. Регистрация и оперативное оповещение о событиях безопасности. Криптографические методы защиты информации. Контроль целостности программных и информационных ресурсов. Обнаружение атак. Защита периметра компьютерных сетей. Управление механизмами защиты.

Раздел 2. Обеспечение безопасности информационных технологий

Организационная структура системы обеспечения безопасности информационных технологий. Понятие технологии обеспечения безопасности информации и ресурсов в автоматизированной системе. Цели создания системы обеспечения безопасности информационных технологий. Регламентация действий пользователей и обслуживающего персонала автоматизированной системы. Политика безопасности предприятия. Основные организационные и организационно-технические мероприятия по созданию и обеспечению функционирования комплексной системы защиты информации. Распределение функций по обеспечению безопасности информационных технологий. Система организационно-распорядительных документов по обеспечению безопасности информационных технологий.

Обязанности конечных пользователей и ответственных за обеспечение безопасности информационных технологий в подразделениях. Общие правила обеспечения безопасности информационных технологий при работе сотрудников с ресурсами автоматизированной системы. Обязанности ответственного за обеспечение безопасности информации в подразделении. Ответственность за нарушения. Порядок работы с носителями ключевой информации.

Документы, регламентирующие правила парольной и антивирусной защиты. Инструкции по организации парольной и антивирусной защиты.

Документы, регламентирующие порядок допуска к работе и изменения полномочий пользователей автоматизированной системы. Инструкция по внесению изменений в списки пользователей. Правила именования пользователей. Процедура авторизации сотрудников. Обязанности администраторов штатных и дополнительных средств защиты.

Документы, регламентирующие порядок изменения конфигурации аппаратно-программных средств автоматизированной системы. Обеспечение и контроль физической целостности и неизменности конфигурации аппаратно-программных средств автоматизированных систем. Регламентация процессов обслуживания и осуществления модификации аппаратных и программных средств. Процедура внесения изменений в конфигурацию аппаратных и программных средств защищенных серверов и рабочих станций. Экстренная модификация (обстоятельства форс-мажор).

Регламентация процессов разработки, испытания, опытной эксплуатации, внедрения и сопровождения задач. Взаимодействие подразделений на этапах проектирования, разработки, испытания и внедрения новых автоматизированных

подсистем.

Определение требований к защите и категорирование ресурсов. Положение о категорировании ресурсов. Проведение информационных обследований и анализ подсистем автоматизированной системы как объекта защиты. Определение градаций важности и соответствующих уровней обеспечения защиты ресурсов. Проведение обследований подсистем, инвентаризация, категорирование и документирование защищаемых ресурсов автоматизированных систем.

Планы защиты и планы обеспечения непрерывной работы и восстановления подсистем автоматизированной системы. Регламентация действий при возникновении кризисных ситуаций.

Основные задачи подразделения обеспечения безопасности информационных технологий. Организация работ по обеспечению безопасности информационных технологий. Организационная структура, основные функции подразделения безопасности.

Концепция безопасности информационных технологий предприятия. Документальное оформление вопросов, отражающих официально принятую систему взглядов на проблему обеспечения безопасности информационных технологий, в качестве методологической основы для формирования и проведения в организации единой политики в области обеспечения информационной безопасности для принятия управленческих решений и разработки практических мер по воплощению данной политики в жизнь.

Раздел 3. Средства защиты информации от несанкционированного доступа

Назначение и возможности средств защиты информации от несанкционированного доступа. Задачи, решаемые средствами защиты информации от несанкционированного доступа.

Рекомендации по выбору средств защиты информации от несанкционированного доступа. Распределение показателей защищенности по классам для автоматизированных систем. Требования руководящих документов ФСТЭК России к средствам защиты информации от несанкционированного доступа. Рекомендации по выбору средств защиты информации от несанкционированного доступа.

Аппаратно-программные средства защиты информации от несанкционированного доступа. Краткий обзор существующих на рынке средств защиты информации от несанкционированного доступа. Существующие средства аппаратной поддержки. Задача защиты от вмешательства посторонних лиц и аппаратные средства аутентификации.

Возможности применения штатных и дополнительных средств защиты информации от несанкционированного доступа. Стратегия безопасности и сертифицированные решения Microsoft. Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной системы. Защита от несанкционированной модификации программ и данных. Защита данных от несанкционированного копирования и перехвата средствами шифрования. Регистрация событий, имеющих отношение к

безопасности. Оперативное оповещение о зарегистрированных попытках несанкционированного доступа. Управление средствами защиты.

Раздел 4. Обеспечение безопасности компьютерных систем и сетей

Проблемы обеспечения безопасности в компьютерных системах и сетях. Типовая корпоративная сеть. Уровни информационной инфраструктуры корпоративной сети. Сетевые угрозы, уязвимости и атаки. Средства защиты сетей.

Назначение, возможности, и основные защитные механизмы межсетевых экранов (МЭ). Назначение и виды МЭ. Основные защитные механизмы, реализуемые МЭ. Основные возможности и варианты размещения МЭ. Достоинства и недостатки МЭ. Основные защитные механизмы: фильтрация пакетов, трансляция сетевых адресов, промежуточная аутентификация, script rejection, проверка почты, виртуальные частные сети, противодействие атакам, нацеленным на нарушение работоспособности сетевых служб, дополнительные функции. Общие рекомендации по применению. Политика безопасности при доступе к сети общего пользования. Демилитаризованная зона. Назначение, особенности и типовая схема «HoneyNet».

Анализ содержимого почтового и Web-трафика (Content Security). Системы анализа содержимого. Компоненты и функционирование систем контроля контента (электронная почта и HTTP-трафик). Политики безопасности, сценарии и варианты применения и реагирования.

Виртуальные частные сети (VPN). Назначение, основные возможности, принципы функционирования и варианты реализации VPN. Структура защищенной корпоративной сети. Варианты, достоинства и недостатки VPN-решений. Общие рекомендации по их применению. Решение на базе ОС Windows. VPN на основе аппаратно-программного комплекса шифрования «Континент». Угрозы, связанные с использованием VPN.

Антивирусные средства защиты. Общие правила применение антивирусных средств в автоматизированных системах. Технологии обнаружения вирусов. Возможные варианты размещение антивирусных средств. Антивирусная защита, как средство нейтрализации угроз.

Обнаружение и устранение уязвимостей. Назначение, возможности, принципы работы и классификация средств анализа защищенности. Место и роль в общей системе обеспечения безопасности. Сравнение возможностей с межсетевыми экранами. Средства обеспечения адаптивной сетевой безопасности. Варианты решений по обеспечению безопасности сети организации. Обзор средств анализа защищенности сетевого уровня и уровня узла. Специализированный анализ защищенности.

Мониторинг событий безопасности. Категории журналов событий. Способы построения, дополнительные компоненты и реализация инфраструктуры управления журналами событий. Технология обнаружения атак. Классификация систем обнаружения атак. Специализированные системы обнаружения атак.

Итоговый зачет (тест).

Модуль 2. Безопасность компьютерных сетей

Раздел 1. Безопасность стека протоколов TCP/IP

Тема 1. Базовые принципы сетевого взаимодействия. Приём, передача данных по сети. Сетевые пакеты. Протоколы, интерфейсы. Уровни сетевого взаимодействия. Модель OSI.

Тема 2. Обзор современных сетевых технологий. Примеры сетей. Физический уровень. Основные сетевые устройства. Технология Ethernet. Сетевые анализаторы.

Тема 3. Обзор современных сетевых протоколов. Архитектура TCP/IP. Документы RFC.

Тема 4. Организация взаимодействия со средой передачи в стеке TCP/IP. Протокол разрешения адресов ARP.

Тема 5. Сетевой уровень в стеке TCP/IP. Протокол IP как основа межсетевого взаимодействия. Маршрутизация. Протокол передачи управляющих сообщений ICMP.

Тема 6. Транспортный уровень в стеке TCP/IP. Протоколы TCP и UDP.

Тема 7. Службы прикладного уровня. Архитектура и принципы работы. Протоколы TELNET, FTP и др.

Тема 8. Электронная почта. Протоколы SMTP и POP3.

Раздел 2. Безопасность компьютерных сетей на основе стека протоколов TCP/IP

Тема 1. Типовая IP-сеть организации. Уровни информационной инфраструктуры корпоративной сети. Концепция глубокоэшелонированной защиты. Угрозы, уязвимости и атаки. Варианты классификации уязвимостей и атак. Обзор механизмов защиты компьютерных систем. Базовые принципы сетевого взаимодействия Архитектура TCP/IP. Краткая характеристика протоколов.

Тема 2. Безопасность физического и канального уровней. Сетевые анализаторы и «снифферы». Методы обнаружения «снифферов». Проблемы аутентификации на основе MAC-адресов. Уязвимости сетевого оборудования.

Тема 3. Проблемы безопасности протокола разрешения адресов ARP. Варианты атак с использованием уязвимостей протокола ARP. ARP Spoofing. Особенности работы механизма разрешения MAC-адресов в различных операционных системах. Меры защиты от атак на протокол ARP, утилита arpwatch. Обнаружение сетевых анализаторов с помощью протокола ARP, утилита Cain.

Тема 4. Стандарт 802.1x. Безопасность на уровне порта. Протокол EAP. Этапы построения сетевой инфраструктуры, удовлетворяющей требованиям стандарта 802.1x.

Тема 5. Безопасность сетевого уровня модели OSI. Протоколы IP и ICMP. Address Spoofing и его использование. Атаки с использованием протокола ICMP. Уязвимости механизма фрагментации.

Тема 6. Защита периметра сети. Межсетевые экраны и их разновидности.

Пакетные фильтры, технология Stateful Inspection. Пакетный фильтр iptables на базе ОС Linux. Посредники и системы анализа содержимого. Изучение базовых возможностей межсетевого экрана CheckPoint NGX. Защита от атаки Address Spoofing.

Тема 7. Виртуальные частные сети. Определение VPN. Разновидности VPN-технологий. Реализации VPN-технологий. Топологии VPN. Схемы использования технологий VPN. Краткие сведения об IPsec. Симметричные и асимметричные схемы и алгоритмы защиты. Протокол L2TP. Протокол PPTP. Сертифицированные решения для построения VPN.

Тема 8. Проблемы безопасности протокола IP версии 6. Краткое описание протокола. Проблемы безопасности. Итоговые рекомендации.

Тема 9. Безопасность транспортного уровня модели OSI. Протоколы TCP и UDP. Распределённые DoS-атаки и меры защиты от них. DoS-умножение. Сканирование портов, утилита nmap. Атаки SYNFlood и LAND. Подмена участника TCP-соединения. Разрыв TCP-соединения с помощью протокола ICMP.

Тема 10. Анализ защищённости корпоративной сети как превентивный механизм защиты. Классификация сканеров безопасности. Принципы анализа защищённости на сетевом уровне. Возможности и варианты использования сетевых сканеров безопасности. Работа с программой Internet Scanner.

Тема 11. Защита трафика на прикладном уровне. Протоколы SSL/TLS, SSH. Теория и практика атак «человек посередине».

Тема 12. Обнаружение сетевых атак. Архитектура систем обнаружения атак. Классификация систем обнаружения атак. Анализ сигнатур. Виды сигнатур. Примеры систем обнаружения атак. Система обнаружения атак Snort.

Тема 13. Общие проблемы безопасности служб прикладного уровня. Уязвимости протокола DHCP. Обнаружение ложного DHCP-сервера. Изучение механизма DNSSpoofing.

Тема 14. Honeynet или сеть-приманка для изучения поведения нарушителей. Принципы организации Honeynet. Классификация сетей-приманок, практические реализации. Утилита honeyd, проект HoneyNet. Сценарии использования сетей-приманок (обнаружение сетевых червей, контроль распространении спама и т. д.). Риски, связанные с использованием сетей-приманок.

Итоговый зачет (тест).

9.2 Лабораторный практикум

№№ п/п	№ (наименование) модуля (раздела, темы)	Наименование лабораторной работы	Количество отводимого времени (час.)
1.	**Тема 2.** Безопасность физического и канального уровней	Изменение MAC-адреса устройства в ОС Windows	0,5
2.	**Тема 2.** Безопасность физического и канального уровней	Изучение трафика атаки с помощью программы Wireshark	0,5
3.	**Тема 3.** Проблемы безопасности протокола разрешения адресов ARP	Уязвимости протокола ARP	0,5
4.	**Тема 3.** Проблемы безопасности протокола разрешения адресов ARP	Мониторинг трафика ARP	0,5
5.	**Тема 4.** Стандарт 802.1x. Безопасность на уровне порта	Подключение клиентов к сети с аутентификацией на уровне порта	1
6.	**Тема 5.** Безопасность сетевого уровня модели OSI	Атаки на протоколы IP и ICMP	1
7.	**Тема 6.** Защита периметра сети	Пакетный фильтр в ОС Linux	1
8.	**Тема 6.** Защита периметра сети	Изучение базовых возможностей многофункциональных межсетевых экранов	1
9.	**Тема 7.** Виртуальные частные сети	Настройка IPsec средствами Windows	1
10.	**Тема 7.** Виртуальные частные сети	Организация удалённого доступа на базе протоколов PPTP и L2TP	1
11.	**Тема 9.** Безопасность транспортного уровня модели OSI	Подмена участника TCP соединения	0,5
12.	**Тема 9.** Безопасность транспортного уровня модели OSI	Защита от атаки SYNFlood	0,5
13.	**Тема 10.** Защита трафика на прикладном уровне	Туннелирование трафика MS RDP при помощи SSH	1
14.	**Тема 10.** Защита трафика на	Атака SSL Strip	1

	прикладном уровне		
15.	**Тема 11.** Анализ защищённости корпоративной сети	Инвентаризация сетевых ресурсов с использованием утилиты nmap	0,5
16.	**Тема 11.** Анализ защищённости корпоративной сети	Выявление уязвимостей	0,5
17.	**Тема 12.** Обнаружение сетевых атак	Настройка систем обнаружения атак	1
18.	**Тема 13.** Проблемы безопасности служб прикладного уровня	Обнаружение неавторизованного сервера DHCP	1
19.	**Тема 13.** Проблемы безопасности служб прикладного уровня	Изучение механизма DNS Spoofing	1
20.	**Тема 14.** Honeynet или сеть-приманка	Настройка honeyd	1

9.3 Семинары

Семинары программой не предусмотрены.

9.4 Практические занятия

№№ п/п	№ раздела учебной дисциплины	Тематика практического занятия	Количество отводимого времени (час.)
1.	3	Возможности штатных средств защиты от НСД в операционных системах	1
2.	4	Варианты применения антивирусных средств защиты	1

9.5 Примерная тематика курсовых работ

9.6 Учебно-методическое и информационное обеспечение

Каждый обучающийся (слушатель) перед началом занятий по Программе получает в постоянное пользование:

- оригинальное учебное пособие (руководство слушателя курса в печатном виде и возможность удалённого доступа к его электронному варианту на сервере СДО Учебного центра);
- справочные и вспомогательные материалы по изучаемым вопросам в

электронном виде в системе дистанционного обучения.

Обеспеченность слушателей учебной литературой – 100%.

а) основная литература:

1. Безопасность информационных технологий. Руководство слушателя курса БТ01. - М.: УЦ Информзащита, 2016. – 350 с.

2. Безопасность компьютерных сетей. Руководство слушателя курса БТ03.- М.: УЦ Информзащита, 2016. – 426 с.

3. Основы TCP/IP. Руководство слушателя курса БТ05. - М.: УЦ Информзащита, 2012. – 108 с.

б) дополнительная литература:

4. «Конституция Российской Федерации», принята всенародным голосованием 12 декабря 1993г.

5. «О Декларации прав и свобод человека и гражданина», Постановление Верховного Совета РСФСР от 22.11.1991 № 1920-1.

6. «Доктрина информационной безопасности Российской Федерации», утверждена Указом Президента РФ 5 декабря 2016г. № 646.

Кодексы:

7. «Уголовный кодекс Российской Федерации», принят Федеральным законом от 13 июня 1996г. № 63-ФЗ.

8. «Кодекс Российской Федерации об административных правонарушениях», принят Федеральным законом от 30 декабря 2001г. №195-ФЗ.

9. «Гражданский кодекс Российской Федерации (часть первая)», принят Федеральным законом от 30 ноября 1994г. №51-ФЗ.

10. «Гражданский кодекс Российской Федерации (часть вторая)», принят Федеральным законом от 26 января 1996г. №14-ФЗ.

11. «Гражданский кодекс Российской Федерации (часть третья)», принят Федеральным законом от 26 ноября 2001г. №146-ФЗ.

12. «Гражданский кодекс Российской Федерации (часть четвертая)», принят Федеральным законом от 18 декабря 2006г. №230-ФЗ.

13. «Трудовой кодекс Российской Федерации», принят Федеральным законом от 30 декабря 2001 г. № 197-ФЗ.

Федеральные законы:

14. Федеральный Закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

15. Федеральный Закон от 19 декабря 2005г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».

16. Федеральный Закон от 27 июля 2006г. № 152-ФЗ «О персональных данных».

17. Федеральный Закон от 29 июля 2004г. № 98-ФЗ «О коммерческой тайне».

18. Федеральный закон от 2 декабря 1990г. № 395-1 «О банках и банковской

деятельности».

19. Федеральный закон от 4 мая 2011г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

20. Федеральный закон от 6 апреля 2011г. № 63-ФЗ «Об электронной подписи».

21. Федеральный закон от 27 декабря 2002г. № 184-ФЗ «О техническом регулировании».

22. Закон Российской Федерации от 21 июля 1993г. № 5485-1 «О государственной тайне».

23. Федеральный закон от 28 декабря 2010г. № 390-ФЗ «О безопасности».

24. Федеральный закон от 3 апреля 1995г. № 40-ФЗ «О Федеральной службе безопасности».

25. Федеральный закон от 7 июля 2003г. № 126-ФЗ «О связи».

26. Федеральный закон от 27 июля 2004г. № 79-ФЗ «О государственной гражданской службе Российской Федерации».

27. Федеральный закон от 2 марта 2007г. № 25-ФЗ «О муниципальной службе в Российской Федерации».

Указы Президента Российской Федерации:

28. Указ Президента Российской Федерации от 31 декабря 2015 года N 683 «О Стратегии национальной безопасности Российской Федерации».

29. Указ Президента Российской Федерации от 6 марта 1997г. № 188 «Об утверждении перечня сведений конфиденциального характера».

30. Указ Президента Российской Федерации от 30 мая 2005г. № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела».

31. Указ Президента Российской Федерации от 3 апреля 1995г. № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации».

32. Указ Президента Российской Федерации от 17 марта 2008г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

33. Указ Президента Российской Федерации от 16 августа 2004г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» (Выписка).

Постановления Правительства Российской Федерации:

34. Постановление Правительства РСФСР от 5 декабря 1991г. № 35 «О перечне сведений, которые не могут составлять коммерческую тайну».

35. Постановление Правительства Российской Федерации от 16 марта 2009г. № 228 «О федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций».

36. Постановление Правительства Российской Федерации от 15 сентября 2008г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

37. Постановление Правительства Российской Федерации от 1 ноября 2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

38. Постановление Правительства Российской Федерации от 6 июля 2008г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

39. Постановление Правительства Российской Федерации от 4 марта 2010г. № 125 «О перечне персональных данных, записываемых на электронные носители информации, содержащиеся в основных документах, удостоверяющих личность гражданина Российской Федерации, по которым граждане Российской Федерации осуществляют выезд из Российской Федерации и въезд в Российскую Федерацию».

40. Постановление Правительства Российской Федерации от 16 апреля 2012г. № 313 «Об утверждении Положения о лицензирования 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)».

41. Постановление Правительства Российской Федерации от 3 марта 2012 г. N 171 «о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации».

42. Постановление Правительства Российской Федерации от 3 февраля 2012г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».

43. Постановление Совета Министров – Правительства Российской Федерации от 15 сентября 1993г. № 912-51 «Об утверждении Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам» (Извлечения).

44. Постановление Правительства Российской Федерации от 18 мая 2009г. № 424 «Об особенностях подключения федеральных государственных информационных систем

к информационно-телекоммуникационным сетям».

45. Постановление Правительства Российской Федерации от 26 июня 1995г. № 608 «О сертификации средств защиты информации».

46. Постановление Правительства Российской Федерации от 21.04.2010 № 266 «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, предназначенной для эксплуатации в загранучреждениях Российской Федерации, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения, об особенностях аккредитации органов по сертификации и испытательных лабораторий (центров), выполняющих работы по подтверждению соответствия указанной продукции (работ, услуг), и о внесении изменения в Положение о сертификации средств защиты информации».

47. Постановление Правительства Российской Федерации от 3 ноября 1994г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

48. Постановление Правительства Российской Федерации от 21 марта 2012г. №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным Законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

Нормативные документы ФСТЭК России:

49. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена Заместителем директора ФСТЭК России 14 февраля 2008г.

50. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка)», утверждена Заместителем директора ФСТЭК России 15 февраля 2008г.

51. «Методические рекомендации по технической защите информации, составляющей коммерческую тайну», утверждены Заместителем директора ФСТЭК России 25 декабря 2006г.

52. «Пособие по организации технической защиты информации, составляющей коммерческую тайну», утверждены Заместителем директора ФСТЭК России 25 декабря 2006г.

53. «Положение о сертификации средств защиты информации по требованиям безопасности информации», утверждено приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 27 октября 1995г. № 199.

54. «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утверждены приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 30 августа 2002г. № 282.

55. «Положение по аттестации объектов информатизации по требованиям безопасности информации», утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994г.

56. «Сборник временных методик оценки защищённости конфиденциальной информации, обрабатываемой техническими средствами и системами», утверждены приказом председателя Государственной технической комиссии при Президенте Российской Федерации, 2001г.

57. «Сборник руководящих документов по защите информации от НСД», утверждены приказом председателя Государственной технической комиссии при Президенте Российской Федерации, 1998г.

58. «Методические документы по обеспечению безопасности информации в ключевых системах информационной инфраструктуры», утверждены Заместителем директора ФСТЭК России 18 мая 2007г. и 19 ноября 2007г.

59. «Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения», утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

60. «Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации», утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

61. «Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

62. «Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

63. «Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники», утвержден решением председателя Гостехкомиссии России от 30 марта 1992г.

64. «Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации», утвержден решением председателя Гостехкомиссии России от 25 июля 1997г.

65. «Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования», утвержден решением председателя Гостехкомиссии России от 25 июля 1997г.

66. «Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей», утвержден приказом председателя Гостехкомиссии России от 4 июня 1999 г. № 114.

67. «Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 1, Часть 2, Часть3», утвержден приказом председателя Гостехкомиссии России от 19 июня 2002 г. №187.

68. «Руководящий документ. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности», Гостехкомиссия России, 2003г.

69. «Руководящий документ. Безопасность информационных технологий. Руководство по регистрации профилей защиты», Гостехкомиссия России, 2003г.

70. «Руководящий документ. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты», Гостехкомиссия России, 2003г.

71. «Руководство по разработке профилей защиты и заданий по безопасности», Гостехкомиссия России, 2003г.

72. «Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры», утверждены заместителем директора ФСТЭК России 18 мая 2007г.

73. «Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры», утверждены заместителем директора ФСТЭК России 19 ноября 2007 г.

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

75. Приказ ФСТЭК России от 11 февраля 2013 г. N 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

76. Приказ ФСТЭК России от 14 марта 2014 г. N 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

77. «Методический документ. Меры защиты информации в государственных информационных системах». Утвержден ФСТЭК России 11 февраля 2014.

Нормативные документы ФСБ России:

78. Приказ ФСБ от 10 июля 2014 года № 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».

79. «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утвержденные руководством 8 Центра ФСБ России (№ 149/7/2/6-432 от 31.03.2015).

80. Приказ ФСБ Российской Федерации от 9 февраля 2005г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

81. Приказ ФАПСИ Российской Федерации от 13 июня 2001г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащих сведений, составляющих государственную тайну», зарегистрирован в Министерстве юстиции Российской Федерации 6 августа 2001 г. № 2848.

Стандарты:

82. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Москва, Стандартинформ, 2007, 11с.

83. ГОСТ Р 50739-95. «Средства вычислительной техники. Защита от НСД к информации. Общие технические требования». Москва, Стандартинформ, 2006, 8 с.

84. ГОСТ Р ИСО/МЭК 15408-1-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель" (утв. и введен в действие Приказом Росстандарта от 15.11.2012 N 814-ст). Москва, Стандартинформ, 2014, 56 с.

85. ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. ... Часть 2. Функциональные компоненты безопасности. Москва, Стандартинформ, 161 с.

86. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности. Москва, Стандартинформ, 150 с.

87. ГОСТ 28147-89. «Системы обработки информации. Защита криптографическая.

Алгоритм криптографического преобразования». Москва, ИПК Изд-во стандартов, 1989, 28 с.

88. ГОСТ Р 34.10-2012. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи». Москва, Стандартинформ, 2012, 33 с.

89. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования». Москва, Стандартинформ, 2012, 35 с.

90. ГОСТ 29099-91. «Сети вычислительные локальные. Термины и определения». Москва, ИПК Изд-во стандартов, 1991, 27 с.

91. ГОСТ Р ИСО/МЭК 27002-2012. «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. Москва, Стандартинформ, 2014. 106 с.

92. ГОСТ Р ИСО/МЭК 27006-2008. Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности. Москва, Стандартинформ, 2009, 40 с.

93. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Москва, Стандартинформ, 2014, 18 с.

94. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие положения. Москва, Госстандарт России, 2000, 14 с.

95. ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания». Москва, ИПК Изд-во стандартов, 1990, 6 с.

96. ГОСТ 34.602-89. «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы». Москва, Стандартинформ, 2009, 12 с.

97. ГОСТ 34.603-92 «Информационная технология. Виды испытаний автоматизированных систем». Москва, Стандартинформ, 2009, 6 с.

Учебные пособия:

98. Баранова Е. К. Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А.В., 3-е изд.- М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016.- 322 с.

99. Жук А. П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.

100.Партыка Т. Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов, – 5-е изд., перераб. и доп. - М.: Форум, НИЦ ИНФРА-М, 2016.- 432с.

101.Основы информационной безопасности: Учебное пособие / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2006. – 544 с.

102. Домарев В.В. Безопасность информационных технологий. Методология

создания систем защиты. Киев, ООО «ТИД ДС», 2001, 688 с.

103. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. Москва, Горячая линия - Телеком, 2000.

104. Петренко С.А., Курбатов В.А. Политики информационной безопасности. Москва, Компания АйТи, 2006, 400 с.

105. Петренко С.А., Петренко А.А. Аудит безопасности IntraNet. Москва, ДМК Пресс, 2002, 187 с.

106. Скот Бармен. Разработка правил информационной безопасности. Вильямс, 2002, 208 с.

107. Смит Р.Э. Аутентификация: от паролей до открытых ключей. Вильямс, 2002, 432 с.

108. Шнайер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Москва, Издательство ТРИУМФ, 2002, 816 с.

109. Безопасность компьютерных сетей. Руководство слушателя курса БТ03.- М.: УЦ Информзащита, 2016. – 426 с.

110. Основы TCP/IP. Руководство слушателя курса БТ05. Москва, УЦ Информзащита, 2012,108 с.

111. Безопасность ОС Windows 7/8.1/10/2012R2. Руководство слушателя курса БТ30.- М.: УЦ Информзащита, 2016. – 700 с.

112. Безопасность ОС Windows 7/8.1/10/2012R2. Приложение к Руководству слушателя курса БТ30 - Практикум. - М.: УЦ Информзащита, 2016. – 752 с.

113. Порядок применения системы защиты Secret Net (сетевая версия). Руководство слушателя курса Т005. Москва, УЦ Информзащита, 2016, 245 с.

114. Порядок применения системы защиты Secret Net (автономный вариант). Руководство слушателя курса Т005АВ. Москва, УЦ Информзащита, 2016, 138 с.

115. Реализация режима коммерческой тайны на предприятии. Руководство слушателя курса КП30. Москва, УЦ Информзащита, 2015, 85 с.

116. Организация конфиденциального делопроизводства. Руководство слушателя курса КП31. Москва, УЦ Информзащита, 2015, 218 с.

117. Защита персональных данных. Руководство слушателя курса КП32. Москва, УЦ Информзащита, 2016, 94 с.

Статьи:

118. Станскова У.М. Правовой анализ локальных нормативных актов работодателя по защите информации ограниченного доступа. Трудовое право в России и за рубежом, 2011, № 2.

119. Волков П.П. Экспертный анализ методов защиты информации от утечки по техническим каналам. Эксперт-криминалист, 2009, № 4.

120. Воротников В.Л. О правовой защите компьютерной информации. Администратор суда, 2009, № 2.

121. Забегайло Л.А., Назарова И.А. Актуальные вопросы охраны коммерческой

тайны в отношениях с органами государства. Современное право, 2011, № 7.

122. Савчишкин Д.Б. Административная ответственность как средство обеспечения информационной безопасности. Административное и муниципальное право, 2011, № 6.

123. Маркарьян Р.В. Об основных направлениях совершенствования законодательства о развитии Интернета в Российской Федерации. Международное публичное и частное право, 2011, № 4.

124. Кузнецова Т.В. Организация работы с персональными данными. Трудовое право, 2011, № 5.

125. Терещенко Л.К. О соблюдении баланса интересов при установлении мер защиты персональных данных. Журнал российского права, 2011, №5.

126. Будаковский Д.С. Способы совершения преступлений в сфере компьютерной информации. Российский следователь, 2011, №4.

127. Воронцова С.В. Киберпреступность: проблемы квалификации преступных деяний. Российская юстиция, 2011, №2.

128. Загузов Г.В. Административно-правовые средства обеспечения информационной безопасности и защиты информации в Российской Федерации. Административное и муниципальное право, 2010, №5.

129. Палехова Е.А. Конфиденциальная информация и институт персональных данных в банковской деятельности. Предпринимательское право, 2010, №3.

130. Дэвид Гринфилд Новые Калиостро LAN / Журнал сетевых решений, Июль-Август 2002.

131. Олифер В. Г., Олифер Н. А. Новые технологии и оборудование IP-сетей. – СПб.:БХВ – Санкт-Петербург, 2000. – 512 с.: ил.

132. Кульгин М. Технологии корпоративных сетей. Энциклопедия – СПб.: Издательство “Питер”, 1999. – 704 с.; ил.

133. Salim Douba Networking UNIX. – Indiana: SAMS Publishing 1995. – 476 с.

134. Б.Ю.Анин Анализаторы протоколов. Системы безопасности связи и телекоммуникаций №31 2000.

135. Ресурсы Microsoft Windows NT Workstation 4.0: пер с англ. – СПб.: BHV – Санкт-Петербург, 1998. - 800 с., ил.

136. Журнал «Сети», №02/2000 Павел ИВАНОВ IPSec: защита сетевого уровня.

137. Артёмов Д. В., Погульский Г. В., Альперович М. М. Microsoft SQL Server для профессионалов: установка, управление, эксплуатация, оптимизация. – М.: Издательский отдел «Русская Редакция» ТОО «Channel Traiding Ltd.». – 1999. – 576 с.: ил.

138. Г. Карпов DNS Методы обеспечения безопасности корпоративной службы доменных имён. BYTE/Россия, октябрь 1999.

139. Д. Давидович, П. Викси Защита DNS. LAN / Журнал сетевых решений, февраль 2000.

140. К. Пьянзин Классификация межсетевых экранов LAN / Журнал сетевых

решений Февраль1999.

141. Д. Форристал, Г. Шипли Сканеры для обнаружения изъянов в корпоративной сети. Сети и системы связи № 7 (71) 15 июня 2001.

142. Лукацкий А. В. Обнаружение атак. – СПб.: БХВ-Петербург, 2001. – 624 с.: ил.

143. К. Касперски Техника сетевых атак. – Издательство «СОЛОН-Р», 2001 г.

144. Стюарт Макклуре, Джоел Скембрей, Джордж Куртц Секреты хакеров. Проблемы и решения сетевой защиты. – Издательство «Лори», 2001

145. А. Борзенко Беспроводные сети BYTE/Россия, август 2001.

146. Олег Артемьев, Владислав Мяснянкин Опасные деревья в сетевых лесах LAN/Журнал сетевых решений, Январь 2002

147. http://www.ietf.org/rfc/rfc4987.txt

148. Mariusz Burdach “Hardening the TCP/IP stack to SYN attacks“ http://www.securityfocus.com/infocus/1729

149. Detection of promiscuous nodes using arp-packets http://securityfriday.com/promiscuous_detection_01.pdf

150. http://project.honeynet.org/alliance/requirements.html

151. http://www.securitylab.ru/contest/264659.php

152. Security Assessment of the Internet Protocol Version 4 (http://www.ietf.org/rfc/rfc6274.txt)

153. ГОСТ 29099-91. «Сети вычислительные локальные. Термины и определения».

154. «Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации», утвержден решением председателя Гостехкомиссии России от 25 июля 1997г.

155. Приказ ФСТЭК России от 9 февраля 2016 г. № 9 (зарегистрирован Минюстом России 25 марта 2016 г., регистрационный N 41564) «Требования к межсетевым экранам» вступают в силу с 1 декабря 2016 г.

в) программное обеспечение:

156. Хакерские инструменты: Cain, Nmap, Netcat и др.

г) базы данных, информационно-справочные и поисковые системы:

157. www.fstec.ru

158. http://www.fsb.ru

159. www.gost.ru

160. Электронный ресурс Internet Security Glossary, Version 2. Режим доступа: http://www.ietf.org/rfc/rfc4949.txt.

161. Система дистанционного обучения (СДО) Учебного центра «Информзащита». Режим доступа: https://sdo.itsecurity.ru/view_doc.html?mode=default

162. Сайт Учебного центра «Информзащита». Режим доступа: http://itsecurity.ru/

9.7 Материально-техническое обеспечение учебного курса

Аудиторные занятия по дисциплине (модулю, курсу) включают лекции с демонстрацией презентаций на экране и практические работы (семинары) под руководством преподавателя.

Наименование специализированных аудиторий, кабинетов, лабораторий	**Вид занятий**	**Наименование оборудования, программного обеспечения**
1	2	3
Лаборатория для изучения дисциплин по теме «Управление информационной безопасностью»	Лекции, практические занятия (семинары)	Для преподавателя компьютер, мультимедийный проектор, экран, оборудование для on-line трансляции (вебинара) Для слушателей (на каждого, не менее) компьютер: Процессор Core 2 Quad 2.50GHz Память 2 Gb Жесткий диск 500.0 Gb DVD-ROM Доступ в сеть интернет (сеть, броузер) Доступ к СДО (системе тестирования) Рассматриваемые аппаратно-программные средства защиты
Лаборатория для изучения дисциплин по теме «Безопасность компьютерных сетей»	Лекции, практические и лабораторные занятия	Для преподавателя компьютер, мультимедийный проектор, экран, оборудование для on-line трансляции Для слушателей (на каждого, не менее) компьютер: Процессор Core 2 Quad 2.50GHz Память 4 GBt Жесткий диск 500.0 Gb DVD-ROM Изучаемые аппаратно-программные средства защиты Доступ к виртуальным лабораторным стендам в ЦОД, к СДО и системе тестирования Доступ в сеть интернет
Виртуальная лаборатория в центре обработки данных	Практические и лабораторные занятия на виртуальных машинах	ЦОД в составе трёх серверов HP ProLiant DL360p Gen8 с двумя внешними файловыми хранилищами и коммутатора Juniper EX3300-24P. Программная платформа vSphere и высокоскоростные каналы доступа в Интернет.

Необходимое оснащение класса. Столы, стулья по количеству обучаемых, оборудование кондиционирования и вентиляции воздуха.

Для преподавателя: компьютер, мультимедийный проектор, экран, оборудование для on-line трансляции (вебинара).

В период очного обучения, каждому слушателю предоставляется компьютер с возможностью выхода в интернет, в том числе для доступа в «личный кабинет», где находится раздаточный материал по курсу (в электронном виде), а также к СДО Учебного центра для прохождения тестирования.

Тестирование слушателей в целях контроля усвоения материала по дисциплине (модулю, курсу), реализуется в системе дистанционного тестирования на базе сервера управления обучением и тестированием Учебного центра.

При использовании дистанционных образовательных технологий (онлайн-вебинаров) к компьютерам слушателей предъявляются такие же требования, как и компьютерам в аудитории.

9.8 Методические рекомендации по организации изучения учебного курса

Используются традиционные образовательные технологии на основе объяснительно-иллюстративного метода обучения, в форме информационной лекции и практических занятий в компьютерных классах.

Формирование профессиональных компетенций обеспечивается использованием в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой.

9.9 Оценочные материалы

Оценочные материалы по Модулю 2 Программы включают следующие основные вопросы, выносимые на аттестацию (тестирование):

Основные понятия ИБ

Безопасность - это: …

Какой принцип лежит в основе эффективного применения защитного механизма «разграничение доступа субъектов к объектам»?

Какой из перечисленных способов управления рисками является альтернативой для трёх остальных (исключает их)?

Дайте определение понятию "Конфиденциальность"

Дайте определение понятию "Доступность"

Дайте определение понятию "Целостность"

Укажите основную причину отсутствия практических методик количественной оценки рисков, связанных с использованием информационных технологий?

В каком случае правильно перечислены все основные причины возникновения антропогенных угроз (угроз «человеческого фактора») в АИС?

В каком случае более точно сформулировано определение угрозы безопасности информации в соответствии с ГОСТ Р 51275?

Безопасность информации - это (по СТР-К) состояние защищенности информации,…

Что такое риск?

Как "безопасность" связана с "бизнесом"?

В каком случае точно указаны три основных свойства ресурсов АИС, которые необходимо обеспечивать (защищать) для обеспечения безопасности (защиты интересов) субъектов информационных отношений?

Какова главная (конечная) цель защиты автоматизированной информационной системы (АИС) Компании?

Какой принцип является основополагающим (краеугольным) для обеспечения безопасности (управления рисками)?

Правовые вопросы

Если класс защиты АИС установлен как 1В по РД ФСТЭК (Гостехкомиссии) России, то сертифицированные средства защиты (СВТ) каких классов в ней должны использоваться?

Как называется Глава 28 Уголовного Кодекса РФ?

Какой международный стандарт определяет Общие критерии оценки безопасности (защищённости) информационных технологий (Evaluation criteria for IT Security)?

Каким нормативным актом утвержден Перечень сведений конфиденциального характера?

В каком кодексе предусмотрена ответственность за «незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну»?

Что именно лицензируется в области защиты информации?

Какие статьи Уголовного Кодекса РФ определяют ответственность за преступления в сфере компьютерной информации?

Если на нескольких компьютерах сети планируется обработка конфиденциальной информации, то какому минимально возможному диапазону классов защиты по требованиям ФСТЭК (по РД Гостехкомиссии) России должна соответствовать данная АИС?

Аттестация АИС по требованиям безопасности информации ФСТЭК России проводится: …

В каком кодексе предусмотрена ответственность за «Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)»?

В каком случае правильно сформулировано определение «персональных данных»?

В соответствии с требованиями ФСТЭК (Руководящими документами Гостехкомиссии) России мандатный (полномочный, меточный) принцип контроля доступа должен быть реализован в СВТ: …

Для кого аттестация АИС по требованиям безопасности информации ФСТЭК (Гостехкомиссии) России является обязательной?

Действие Федерального закона №152-ФЗ «О персональных данных» не распространяется на отношения, возникающие при: …

Если на нескольких компьютерах многопользовательской АИС планируется обработка информации с грифом «С», то по какому классу защиты (по требованиям ФСТЭК) должна быть аттестована данная система?

В какой статье Уголовного Кодекса РФ определяется ответственность за создание, использование и распространение вредоносных программ для ЭВМ?

Обладатель информации, оператор информационной системы обязан обеспечить: ...

Организационные вопросы

Какой стандарт определяет требования к управлению инцидентами информационной безопасности (Information security incident management)?

На каких этапах жизненного цикла АИС специалисты подразделения обеспечения информационной безопасности должны принимать обязательное участие в её защите?

Когда и кому разрешено передавать свой пароль для входа в систему (пароль своей учётной записи в АИС)?

Какой правовой акт является базовым для определения требований к режиму защиты информации, содержащей конфиденциальные сведения?

Кто такой "обладатель информации"?

Следует ли согласовывать с начальником службы безопасности прием новых сотрудников в штат организации?

Какой стандарт определяет требования к системе управления информационной безопасностью («Information security management systems – Requirements»)?

Кто отвечает за сохранность и резервное копирование данных, хранимых на стационарных и портативных компьютерах (рабочих местах) конечных пользователей?

Кто входит в состав комплексной системы обеспечения информационной безопасности АИС предприятия?

Кто имеет право разрешать или ограничивать доступ к информации (согласно ФЗ от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите

информации»)?

В каком случае необходимо хранить пароль пользователя для входа в систему в записанном виде (в запечатанном конверте, в сейфе у уполномоченного лица) на случай его непредвиденного отсутствия на рабочем месте?

Как правильно трактуется название (назначение) раздела стандарта ISO/IEC 27002-2005 «Personal security»?

На осуществление какого из перечисленных ниже видов деятельности в соответствии с федеральным законодательством лицензии не требуется?

Обеспечение безопасности информационных технологий есть процесс: …

Защитные механизмы

Какой из перечисленных паролей является наиболее стойким (сложным для подбора и угадывания)?

Какая модель разграничения доступа субъектов к объектам NTFS (NT File System) и AD (Active Directory) используется в Windows 2000/XP/2003?

Сколько секретных ключей используется при взаимном обмене зашифрованными (ассиметричным алгоритмом) и подписанными сообщениями двух пользователей электронной почты?

Что такое Single Sign-On (SSO) ?

При каком способе управления разграничением доступа к ресурсам пользователю присваивается уровень допуска?

В каком из приведенных вариантов аутентификация является многофакторной?

Что является наиболее серьезной проблемой парольной аутентификации пользователей на серверах?

Сетевая безопасность

Что такое демилитаризованная зона (DMZ, в применении к компьютерным сетям)?

Что такое СПАМ (SPAM)?

Какой протокол НЕ используется для построения виртуальных частных сетей (VPN)?

Можно ли отразить атаку (блокировать трафик атаки) типа «WinNuk» при помощи перечисленных ниже средств защиты? (IDS - Intrusion Detection System, IPS - Intrusion Prevention System, VLAN - Virtual Local Network)

Какой вариант построения VPN используется при защищённом удалённом доступе к сети Компании с мобильного компьютера (ноутбука) ?

Какой вариант сетевой трансляции адресов и портов используется на межсетевом

экране (МЭ) с одним внешним адресом для обеспечения возможности выхода пользователей из внутренней корпоративной сети в Интернет?

Какая причина затрудняет использование в компании сетевых сканеров безопасности?

К какому уровню информационной инфраструктуры корпоративной сети относится уязвимость Microsoft Internet Explorer, приводящая к возможности создания/модификации файлов на жестком диске компьютера?

Какая из перечисленных ниже задач может быть решена сетевым сканером безопасности?

Какую дополнительную критичную информацию может получить злоумышленник в результате сканирования портов?

Нужен ли в вашей системе межсетевой экран, если у вас на входном сегменте сети уже применяется средство обнаружения (предотвращения) атак (средство противодействия вторжениям, IDS/IPS)?

В чём состоит главный недостаток пакетных фильтров (разновидности межсетевых экранов)?

Какой утилитой администратор может проверить наличие обновлений на компьютере пользователя, работающего под управлением ОС Windows XP?

Какие данные анализируются сетевой системой обнаружения атак (Network Intrusion Detection System, NIDS)?

Какой протокол, используемый в Windows, наиболее защищен от подбора пароля, перехваченного при передаче по сети злоумышленником?

«Виртуальная частная сеть» (Virtual Private Network, VPN) – это технология передачи информации через...

Реагирование на инциденты

Какой способ реагирования на выявление в компании факта продажи сотрудником информации, составляющей коммерческую тайну компании, третьим лицам несет наименьшие репутационные риски?

С какого возраста предусмотрена уголовная ответственность за преступления в сфере компьютерной информации?

Имеют ли результаты расследования нарушений информационной безопасности доказательную силу по уголовному делу?

Имеет ли право служба безопасности Компании при расследовании инцидентов в сфере информационной безопасности использовать методы оперативно-розыскной деятельности (наблюдение, прослушивание помещений, оперативный эксперимент и т.п.)?

Коммерческая тайна

Информация составляет служебную или коммерческую тайну в случае: …

Какие меры должен принять работодатель, прежде чем допустить работника к работе с информацией, составляющей коммерческую тайну?

Что такое «коммерческая тайна» (в соответствии с ФЗ «О коммерческой тайне»)?

Информация, составляющая коммерческую тайну, предоставляется обладателем в органы государственной власти и местного самоуправления:…

Режим коммерческой тайны считается установленным после: …

Конфиденциальное делопроизводство

Что такое «конфиденциальный документ»?

Что такое «конфиденциальная информация»?

Что такое «гриф конфиденциальности»?

Что такое «носители конфиденциальной информации»?

Что такое «конфиденциальное делопроизводство»?

Кто такой обладатель информации?

Что такое «документированная информация»?

Кто имеет право разрешать или ограничивать доступ к информации?

Оценочные материалы по Модулю 2 Программы включают следующие основные вопросы, выносимые на аттестацию (тестирование):

Какой из механизмов реализации сетевых атак наиболее сложен с точки зрения обнаружения?

Какие параметры TCP-соединения должны быть известны нарушителю для подмены участника?

Какие способы можно использовать для защиты от атаки SYNFlood?

Какие меры защиты можно использовать для предотвращения негативного влияния неавторизованного сервера DHCP?

В каком случае более точно сформулировано назначение протокола Internet Key Exchange (IKE)?

В чём заключается слабость подстановочных шифров?

На каком участке используется механизм инкапсуляции «EAP over LAN» или EAPOL?

В каком случае более точно перечислены типы проверок, используемых в сетевых сканерах безопасности?

Какие алгоритмы используются для обеспечения целостности передаваемых данных?

В чём разница между пакетным фильтром с контролем состояния ("stateful") и "классическим" посредником сеансового уровня?

Какой из механизмов реализации сетевых атак не подразумевает использования какой-либо уязвимости?

При получении нескольких ответов на ARP-запрос какой из них используется для добавления записи в ARP-таблицу узла?

Как может быть использовано нарушителем сообщение "ICMP Redirect"?

В каком случае более точно названы типы агентов сканирования, используемых в современных системах управления уязвимостями?

В каком случае правильно перечислены режимы работы IPsec?

В каком случае более точно названы источники данных, используемые в системах обнаружения атак?

Какие угрозы связаны с использованием протокола DHCP?

В чём разница между пакетным фильтром и пакетным фильтром с контролем состояния ("stateful")?

В каком случае наиболее правильно перечислены "векторы атак" на сервис DNS?

В каком случае правильно перечислены протоколы, входящие в набор IPsec?

В каком случае более точно названы характеристики модуля слежения, используемого в системах обнаружения сетевых атак?

Можно ли использовать ARP-запрос для добавления записи в ARP-таблицу удалённого узла?

Какой способ можно использовать для защиты от атаки "ICMP Redirect"?

10. Перечень сведений, составляющих государственную тайну, используемых в учебном процессе

В учебном процессе по данной программе повышения квалификации сведения, составляющие государственную тайну, не рассматриваются.