Министерство науки и высшего образования Российской Федерации

ИВАНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Шуйский филиал ИвГУ

Кафедра математики, информатики и методики обучения

ОДОБРЕНО:

Руководитель программы аспирантуры

_____ А.Н. Привалов
(подпись)

«18» марта 2026 г.

Рабочая программа дисциплины
МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Уровень высшего образования:	Подготовка кадров высшей квалификации
Научная специальность:	2.3.6. Методы и системы защиты информации, информационная безопасность
Направленность образовательной программы:	
Срок освоения образовательной программы и форма обучения:	3 года

Шуя

1. Цели освоения дисциплины

Целью учебной дисциплины является содействие аспирантам в приобретении знаний, умений и навыков в области методов и средств защиты информации и обеспечения информационной безопасности, необходимых в процессе проведения практических работ в рамках диссертационного исследования. В рамках данного курса предполагается изучение современного состояния проблем разработки, совершенствования и применения методов и средств защиты информации в процессе ее сбора, хранения, обработки, передачи и распространения, а также обеспечения информационной безопасности объектов политической, социально-экономической, оборонной, культурной и других сфер деятельности от внешних и внутренних угроз хищения, разрушения и/или модификации информации.

2. Место дисциплины в структуре ОП

Дисциплина «Методы и системы защиты информации, информационная безопасность» является обязательной для изучения и относится к дисциплинам образовательной программы, направленным на подготовку к сдаче кандидатского экзамена.

Успешное освоение данной дисциплины будет способствовать готовности аспирантов к подготовке публикаций и (или) заявок на патенты на изобретения, полезные модели, свидетельства о государственной регистрации программ для электронных вычислительных машин, баз данных, топологий интегральных микросхем, подготовке к прохождению промежуточной аттестации по этапам выполнения научного исследования, сдаче кандидатского экзамена и выполнении диссертационного исследования.

Для освоения данной дисциплины обучающийся должен:

Знать:

– основные варианты использования компьютерных технологий в научных исследованиях и образовательных целях;

Уметь:

– эффективно использовать ресурсы Интернета в образовательных целях, по отношению к проблеме собственного диссертационного исследования;

Владеть:

–современной терминологией в области информационной безопасности.

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины обучающийся должен:

Знать:

– основные организационные и правовые методы обеспечения безопасности информационных систем;

– современные методы защиты локальной и удаленной вычислительных сетей;

– методы анализа безопасности информационных систем с использованием отечественных и зарубежных стандартов в области информационной безопасности;

– методы организации работы коллектива по проведению научных исследований в области информационной безопасности;

– современные методы и средства защиты информации при ее передаче и хранении;

– действующие стандарты в области информационной безопасности;

– критерии, устанавливающие степень соответствия защищаемых объектов стандартам информационной безопасности;

– современные методы исследования сетевого трафика с целью контроля целостности информации, выявления попыток несанкционированного доступа в информационные системы, обнаружения вредоносных программ;

– существующие защищенные протоколы обмена информацией;

– формальные модели политик безопасности, политик управления доступом и информационными потоками в информационных системах.

Уметь:

– формировать требования защиты объектов информатизации и информационных систем;

– разрабатывать и исследовать методы защиты локальной и удаленной вычислительных сетей;

– проводить анализ безопасности информационных систем с использованием отечественных и зарубежных стандартов в области компьютерной безопасности;

– разрабатывать математические модели отдельных средств защиты информации, а также модели безопасности защищаемых информационных систем в целом;

– проводить обоснование и выбор рационального решения по уровню защищенности информационной системы с учетом заданных требований;

– разрабатывать предложения по совершенствованию управления безопасностью информационных систем и сетей;

– адаптировать и обобщать результаты современных исследований;

– обосновывать выбор методов защиты информации при ее передаче и хранении, защищенные протоколы обмена информацией;

– выявлять возможности совершенствования научных методов и алгоритмов исследования свойств сетевого трафика с целью контроля целостности информации, выявления попыток несанкционированного доступа в информационные системы, обнаружения вредоносных программ.

Иметь опыт:

– обоснования оценки степени защищенности объектов информатизации и информационных систем;

– навыками применения организационных и правовых мер для обеспечения безопасности информационных систем;

– навыками применения современных методов защиты локальной и удаленной вычислительных сетей;

– навыками разработки формальных моделей политик безопасности, политик управления доступом и информационным и потоками в информационных системах;

– методами анализа безопасности информационных систем с использованием отечественных и зарубежных стандартов в области информационной безопасности;

– навыками организации работы коллектива по проведению научных исследований в области информационной безопасности;

– методами адаптации и обобщения результатов современных исследований;

– навыками применения существующих защищенных протоколов обмена информацией;

– современными методами исследования сетевого трафика с целью контроля целостности информации, выявления попыток несанкционированного доступа в информационные системы, обнаружения вредоносных программ;

– современными методами и средствами защиты информации при ее передаче и хранении.

4. Объем и содержание дисциплины

Объем дисциплины составляет 4 зачетных единиц (144 академических часов)

4.1. Содержание дисциплины по разделам (темам), соотнесенное с видами и трудоемкостью занятий лекционно-семинарского типа

№	Разделы (темы) дисциплины	Семестр	Виды занятий, их объем (в акад. часах, по очной форме обучения)			Формы текущего контроля успеваемости (по очной форме обучения) Формы промежуточной аттестации
			Занятия лекцион-ного типа	Занятия семинарского типа	Самостоятельная работа обучающихся	
1.	Концепция информационной безопасности	3	4	4 практические	10	Практические задания
2.	Угрозы информации	3	2	2 практические	8	Практические задания
3.	Виды возможных нарушений безопасности информационной системы	3	4	4 практические	8	Практические задания
4.	Информационная безопасность информационных систем	3	4	4 практические	16	Практические задания
5.	Методы и средства защиты компьютерной информации	3	4	4 практические	16	Практические задания
6.	Заключительный. Подведение и анализ промежуточных результатов освоения дисциплины	3	2	2 практические	10	Практические задания
7.	Итого за семестр:		20	20	68	Кандидатский экзамен

4.2. Развернутое описание содержания дисциплины по разделам (темам)

Тема 1 – Концепция информационной безопасности

Актуальность информационной безопасности. Программа «Цифровая экономика» и национальный проект «Информационная безопасность». Национальные интересы РФ в информационной сфере и их обеспечение. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.

Лицензирование и сертификация в области защиты информации. Законодательство в области лицензирования и сертификации. Правила функционирования системы лицензирования.

Основные нормативные руководящие документы. Международные стандарты информационного обмена. Критерии безопасности компьютерных систем. «Оранжевая книга». Руководящие документы Гостехкомиссии.

Тема 2 – Угрозы информации

Информационная безопасность сетей. Информационная безопасность в условиях функционирования в России глобальных сетей. Угрозы информационной безопасности для АСОИ. Способы совершения компьютерных преступлений. Уязвимость сети Интернет. Пользователи и злоумышленники в Интернет. Причины уязвимости сети Интернет. Удаленные атаки на интрасети. Банк данных угроз безопасности информации ФСТЭК России.

Тема 3 – Виды возможных нарушений безопасности информационной системы

Компьютерные преступления. Классификация компьютерных преступлений. Виды противников или «нарушителей». Вредоносные программы. Условия существования вредоносных программ. Хакерские утилиты и прочие вредоносные программы. Спам. Вирусы. Понятия о видах вирусов. Классические компьютерные вирусы. Сетевые черви. Троянские программы.

Тема 4 – Информационная безопасность информационных систем

Теория информационной безопасности информационных систем. Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Криптографические способы защиты информации. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Методы криптографии. Классификация методов криптографического закрытия информации. Шифрование. Симметричные криптосистемы. Криптосистемы с открытым ключом (асимметричные). Характеристики существующих шифров. Кодирование. Стеганография. Электронная цифровая подпись.

Организация информационной безопасности компании. Основные технологии построения защищенных ЭИС. Место информационной безопасности экономических систем в национальной безопасности страны. Организация информационной безопасности компании. Выбор средств информационной безопасности.

Тема 5 – Методы и средства защиты компьютерной информации

Обеспечения информационной безопасности. Методы обеспечения информационной безопасности РФ. Ограничение доступа. Контроль доступа к аппаратуре.

Контроль доступа к информации. Разграничение и контроль доступа к информации. Предоставление привилегий на доступ. Идентификация и установление подлинности объекта (субъекта).

Методы и средства защиты информации. Методы и средства защиты информации от случайных воздействий. Методы защиты информации от аварийных ситуаций. Организационные мероприятия по защите информации. Защита информации от утечки за счет побочного электромагнитного излучения и наводок.

Антивирусное ПО. Признаки заражения компьютера. Источники компьютерных вирусов. Основные правила защиты. Вирусные описания на сайте Dr.Web.

Тема 6 – Заключительный. Подведение и анализ промежуточных результатов освоения дисциплины

5. Образовательные технологии

В программе данного курса предусмотрено использование в учебном процессе активных форм проведения занятий и организации самостоятельной работы. В учебном процессе используются как активные, так и интерактивные формы проведения занятий: дискуссия, метод поиска быстрых решений в группе, мозговой штурм.

Аудиторные занятия проводятся в интерактивной форме с использованием мультимедийного обеспечения (ноутбук, проектор) и технологии проблемного обучения.

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине: технологии смешанного обучения, мультимедиа технологии, облачные технологии, технологии визуализации (инфографика, дашборды).

6. Учебно-методическое обеспечение самостоятельной работы обучающихся

Самостоятельная работа обучающихся по дисциплине осуществляется в следующих формах:

– повторение материала с использованием конспектов лекций;

– изучение и анализ предложенных электронных образовательных ресурсов, содержащих информацию по методам и средствам защиты информации и обеспечения информационной безопасности;

– выполнение заданий, из которых складывается портфолио студента, включающее обязательные и дополнительные (определяемые студентами совместно с преподавателем) материалы.

Задания и результаты их выполнения составляют часть информационного ресурса кафедры математики, информатики и методики обучения и хранятся на сервере кафедры, доступ к ним обеспечен с компьютеров в компьютерном классе.

Полностью весь методический материал по обеспечению самостоятельной работы студентов приводится в приложении 1 к настоящей программе. Доступ к методическим материалам осуществляется при помощи электронной информационно-образовательной среды Шуйского филиала ИвГУ.

7. Характеристика оценочных средств для текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Промежуточная аттестация по дисциплине (экзамен) проводится с использованием рейтинговой оценки.

Промежуточная аттестация студентов предполагает экзамен в форме выполнения тестового задания, примерный вариант которого представлен в Приложении 2.

Критерии оценки:

– оценка «отлично» выставляется аспиранту, если аспирант выполнил тестового задание на 85 или более процентов;

– оценка «хорошо» выставляется аспиранту, если аспирант выполнил тестового задание на 71 или более процентов;

– оценка «удовлетворительно» выставляется аспиранту, если аспирант выполнил тестового задание на 61 или более процентов;

– оценка «неудовлетворительно» выставляется аспиранту, если аспирант выполнил тестовое задание на менее чем 61 процент;

8. Учебно-методическое и информационное обеспечение дисциплины

Основная литература:

1. Аверченков, В. И. Служба защиты информации: организация и управление : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стереотип. - Москва : Издательство «Флинта», 2016. - 186 с. - Библиогр. в кн. - ISBN 978-5-9765-1271-9 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93356

2. Загинайлов, Ю. Н. Основы информационной безопасности: курс визуальных лекций : учебное пособие / Ю.Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. - 105 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3947-4 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=362895

3. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. - 253 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557

4. Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика : учебное пособие / В. Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. : схем., табл.

– ISBN 978-5-4499-0496-6. – DOI 10.23681/571485; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=571485

Дополнительная литература:

1. Аверченков, В. И. Криптографические методы защиты информации : учебное пособие : [16+] / В. И. Аверченков, М. Ю. Рытов, С. А. Шпичак. – 2-е изд., стер. – Москва : ФЛИНТА, 2017. – 201 с. : схем., ил. – ISBN 978-5-9765-2947-2. – Текст : электронный.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=574862

2. Артемов, А.В. Информационная безопасность : курс лекций / А.В. Артемов ; Межрегиональная Академия безопасности и выживания. - Орел : МАБИВ, 2014. - 257 с. : табл., схем. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=428605

3. Голиков, А.М. Защита информации от утечки по техническим каналам : учебное пособие / А.М. Голиков ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). - Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. - 256 с. : схем., табл., ил. - Библиогр.: с. 213. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=480636

4. Ефимова, Л. Л. Информационная безопасность детей: российский и зарубежный опыт / Л. Л. Ефимова, С. А. Кочерга. – Москва : Юнити-Дана, 2017. – 240 с. : схем., табл., ил. – ISBN 978-5-238-02405-9; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=682995

5. Информационная безопасность и защита информации : сборник студенческих работ / отв. ред. А.Ю. Колябин. - М. : Студенческая наука, 2012. - 1322 с. : ил.,табл., схем. - (Вузовская наука в помощь студенту). - ISBN 978-5-00046-137-2 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=227774

6. Ковалев, Д. В. Информационная безопасность : учебное пособие : [16+] / Д. В. Ковалев, Е. А. Богданова ; Южный федеральный университет. – Ростов-на-Дону : Южный федеральный университет, 2016. – 74 с. : схем., табл., ил. – ISBN 978-5-9275-2364-1; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=493175

7. Котова, Л.В. Сборник задач по дисциплине «Методы и средства защиты информации» : учебное пособие / Л.В. Котова ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Московский педагогический государственный университет». - Москва : МПГУ, 2015. - 44 с. : ил. - Библиогр. в кн. - ISBN 978-5-4263-0221-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=469877

8. Моргунов, А. В. Информационная безопасность : учебно-методическое пособие / А. В. Моргунов ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2019. – 83 с. : ил., табл. – ISBN 978-5-7782-3918-0; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=576726

9. Петренко, В.И. Теоретические основы защиты информации : учебное пособие / В.И. Петренко ; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». - Ставрополь : СКФУ, 2015. - 222 с. : ил. - Библиогр.: с. 214-215. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=458204

10. Прохорова, О.В. Информационная безопасность и защита информации : учебник / О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». - Самара : Самарский

государственный архитектурно-строительный университет, 2014. - 113 с. : табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-9585-0603-3 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=438331

11. Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. - 4-е изд., стер. - Москва : Издательство «Флинта», 2016. - 224 с. - (Организация и технология защиты информации). - Библиогр.: с. 192-193. - ISBN 978-5-9765-1274-0 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93351

12. Фефилов, А.Д. Методы и средства защиты информации в сетях / А.Д. Фефилов. - Москва : Лаборатория книги, 2011. - 105 с. : ил., табл. - ISBN 978-5-504-00608-6 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=140796

13. Шунейко, А. А. Информационная безопасность человека : учебное пособие / А. А. Шунейко, И. А. Авдеенко. – Москва : Владос, 2018. – 177 с. : ил. – (Учебник для вузов (бакалавриат)). – ISBN 978-5-906992-91-8; То же [Электронный ресурс]. – URL: http://biblioclub.ru/index.php?page=book&id=573372

Ресурсы информационно-телекоммуникационной сети «Интернет»:
Профессиональные базы данных и информационно-справочные системы:
ЭБС «Университетская библиотека онлайн» www.biblioclub.ru
Национальный цифровой ресурс Руконт - https://rucont.ru/default.aspx
Электронная библиотека ИвГУ http://lib.ivanovo.ac.ru
Электронный каталог НБ ИвГУ http://lib.ivanovo.ac.ru/index.php/ek

Программное обеспечение: операционная система Microsoft Windows, пакет офисных программ Microsoft Office и(или) LibreOffice, интернет-браузер Microsoft Edge и(или) Yandex Browser.

9. Материально-техническое обеспечение дисциплины

Учебные аудитории:

– для проведения занятий лекционного типа с комплектом специализированной учебной мебели и техническими средствами обучения, служащими для предоставления учебной информации большой аудитории;

– для проведения занятий семинарского типа, консультаций, текущего контроля и промежуточной аттестации с комплектом специализированной учебной мебели и техническими средствами обучения.

Помещение для самостоятельной работы, оснащенное комплектом специализированной учебной мебели, компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в ЭИОС.

Демонстрационное оборудование и учебно-наглядные пособия для занятий лекционного типа, обеспечивающие тематические иллюстрации: электронные пособия (презентации), аудио-визуальные пособия (видеоматериалы), печатные пособия (таблицы, схемы)).

Автор(ы) рабочей программы дисциплины: профессор кафедры математики, информатики и методики обучения, доктор технических наук, профессор Привалов А. Н.

Программа рассмотрена и утверждена на заседании кафедры математики, информатики и методики обучения «02» марта 2022 г., протокол № 8

Программа обновлена
протокол заседания кафедры № 8 от «22» марта 2023 г.
Согласовано:
Руководитель ОП _____ А.Н. Привалов
(подпись)

Программа обновлена
протокол заседания кафедры № 7 от «9» февраля 2024 г.
Согласовано:
Руководитель ОП _____ А.Н. Привалов
(подпись)

Программа обновлена
протокол заседания кафедры № 9 от «20» марта 2025 г.
Согласовано:
Руководитель ОП _____ А.Н. Привалов
(подпись)

Программа обновлена
протокол заседания кафедры № 9 от «18» марта 2026 г.
Согласовано:
Руководитель ОП _____ А.Н. Привалов
(подпись)

Министерство науки и высшего образования Российской Федерации

ИВАНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Шуйский филиал ИвГУ

Кафедра математики, информатики и методики обучения

Приложение 1
к рабочей программе дисциплины

Методические указания
для обучающихся по освоению дисциплины
МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Уровень высшего образования:	Подготовка кадров высшей квалификации
Научная специальность:	2.3.6. Методы и системы защиты информации, информационная безопасность
Направленность образовательной программы:	
Срок освоения образовательной программы:	3 года

Шуя

1. Методические указания к проработке лекционного материала по дисциплине

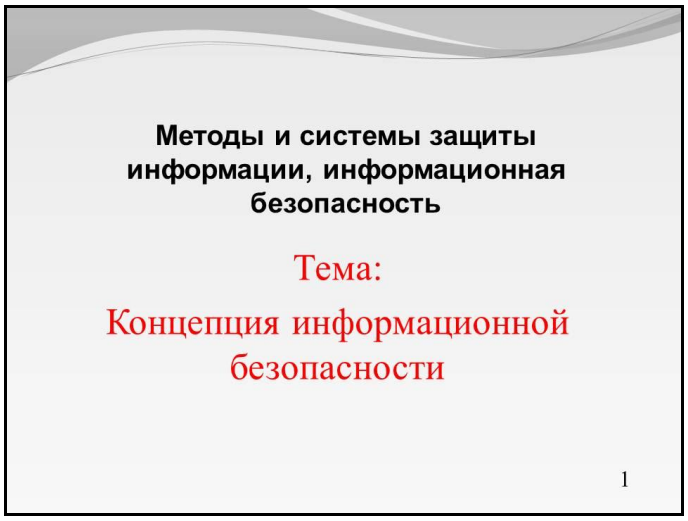
Общий план лекций включает следующие составные элементы:

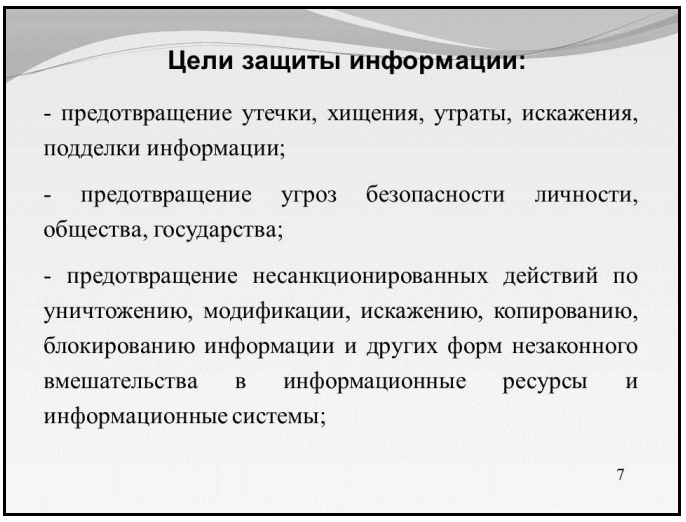
Название этапа	**Содержание**	**Время, мин.**
Вступительная часть	Приветствие. Контроль посещаемости. Постановка темы, цели, основных задач.	4-7
Актуальность и основные понятия	Формулирование проблемы; основные понятия и суть изучаемого вопроса.	8-10
Основная часть	Представление материала лекции в соответствии с программой	60-65
Закрепление полученной информации	Вопрос-ответ, фронтальный опрос, разбор ошибок, допущенных при ответах	5-8
Подведение итогов	Сопоставление результатов лекции с установленной целью и намеченными задачами.	3

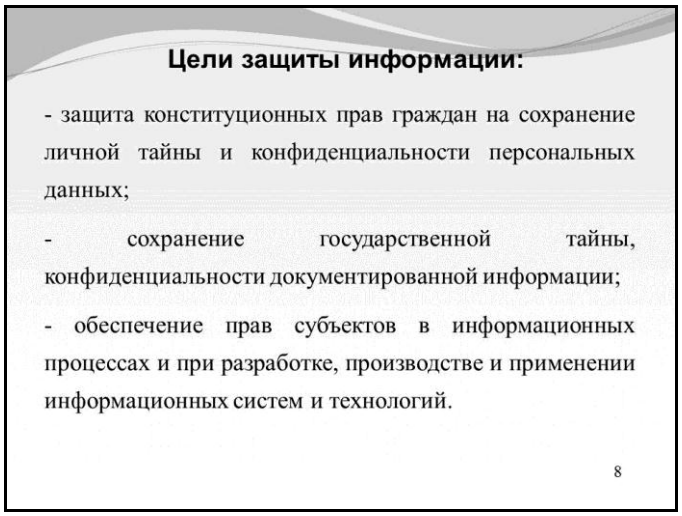
В рамках проведения занятий по дисциплине предполагается чтение следующих лекций:
Лекция 1. Концепция информационной безопасности
Тезисы лекции:

- Актуальность информационной безопасности. Программа «Цифровая экономика» и национальный проект «Информационная безопасность».
- Национальные интересы РФ в информационной сфере и их обеспечение.
- Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
- Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.
- Лицензирование и сертификация в области защиты информации. Законодательство в области лицензирования и сертификации. Правила функционирования системы лицензирования.
- Основные нормативные руководящие документы. Международные стандарты информационного обмена.
- Критерии безопасности компьютерных систем. «Оранжевая книга».
- Руководящие документы Гостехкомиссии.

Слайды презентации к лекции:







Объекты и применяемые меры защиты информации

Правовые меры защиты

Защита информации правовыми методами, включающая разработку законодательных и нормативных правовых документов, применение этих документов, надзор и контроль за их исполнением.

Организационные меры защиты

Меры, предназначенные для организации функционирования ИС, персонала и взаимодействия пользователей с системой. Базовые организационные меры включают:

- формирование политики безопасности;
- организацию доступа в помещения;
- организация доступа сотрудников к информационным ресурсам;
- определение ответственности за нарушение требований информационной безопасности.

9

Применяемые меры защиты информации

- Техническая и программно-аппаратная защита информации:

Защита информации с применением технических, программных, программно-технических средств.

- Физическая защита:

Совокупность средств, препятствующих проникновению потенциального злоумышленника на территорию контролируемой зоны.

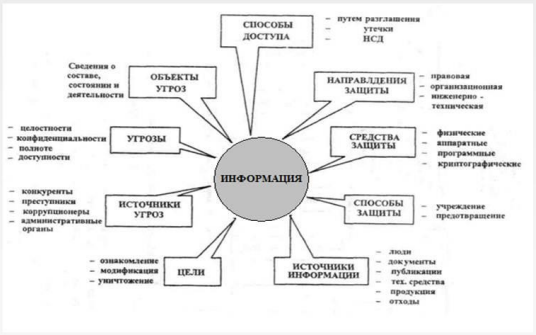
10

Принципы построения системы защиты информации

- *Комплексность;*
- *Своевременность;*
- *Непрерывность;*
- *Активность;*
- *Законность;*
- *Обоснованность;*
- *Экономическая целесообразность и сопоставимость;*
- *Специализация;*
- *Взаимодействие и координация;*
- *Совершенствование;*
- *Централизация управления;*

11

Концептуальная модель компонентов системы защиты информации



12

Правовые основы обеспечения информационной безопасности

- Законы Российской Федерации;
- Указы Президента Российской Федерации;
- Концептуальные документы;
- Постановления правительства Российской Федерации;
- Руководящие документы регуляторов (ФСБ, ФСТЭК, Роскомнадзор и др.);
- Локальные нормативные документы ;
- Инструкции.

13

Правовые основы обеспечения информационной безопасности

- Закон РФ «О безопасности» от 28.12.2010 № 390-ФЗ;
- Закон РФ «О государственной тайне» от 21.07.93 № 5485-1;
- Закон РФ «О коммерческой тайне» от 29.07.2004 № 98-ФЗ;
- Закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ;
- Закон РФ «О лицензировании отдельных видов деятельности» от 04.05.2011 № 99-ФЗ;
- Закон РФ «О техническом регулировании» от 27.12.2002 №184-ФЗ;
- Закон РФ «О стандартизации» от 29.06.2015 № 162-ФЗ;
- Закон РФ «Об электронной подписи» от 06.04.2011 № 63-ФЗ;
- Закон РФ «О связи» от 07.07.2003 № 126-ФЗ;
- Закон РФ «О персональных данных» от 27.07.2006 № 152-ФЗ;
- Закон РФ «О федеральной службе безопасности» от 03.04.95 № 40-ФЗ;
- Закон РФ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ;

14

Правовые основы обеспечения информационной безопасности

Закон РФ «О безопасности» от 28.12.2010 № 390-ФЗ

Закон определяет основные принципы и содержание деятельности по обеспечению безопасности государства, общества, личности, экологической безопасности и иных видов, предусмотренных законодательством Российской Федерации, полномочия и функции федеральных органов государственной власти, субъектов Российской Федерации, местного самоуправления в области безопасности, а также статус Совета Безопасности Российской Федерации.

15

Правовые основы обеспечения информационной безопасности

Закон РФ «О государственной тайне» от 21.07.93 № 5485-1

В законе используются следующие понятия:

Государственная тайна – защищаемые государством сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

Носители сведений, составляющих государственную тайну – материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят отображение виде символов, образов, сигналов, технических решений и процессов;

Система защиты государственной тайны – совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, их носителей, а также мероприятий, проводимых в этих целях;

Государственную тайну составляют сведения:

- в военной области;
- в области экономики, науки и техники;
- в области внешней политики и экономики;
- в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также в области противодействия терроризму и обеспечения безопасности лиц, в отношении которых принято решение о применении мер государственной защиты.

12

Правовые основы обеспечения информационной безопасности

Закон РФ «О коммерческой тайне» от 29.07.2004 № 98-ФЗ

Закон регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны.

Коммерческая тайна – сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в ситу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Ст. 10 настоящего закона устанавливает меры по охране конфиденциальности информации, принимаемые ее обладателем:

- определение перечня информации, составляющей коммерческую тайну;
- ограничение доступа к информации, составляющей коммерческую тайну;
- учет лиц, получивших доступ к информации, составляющей коммерческую тайну;
- регулирование отношений по использованию информации работниками на основании трудовых и гражданско-правовых договоров;
- нанесение на материальные носители, содержащие информацию, составляющей коммерческую тайну грифа «Коммерческая тайна».

17

Правовые основы обеспечения информационной безопасности

Закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ

Закон регулирует отношения, возникающие при:
- поиске, получении, передаче, производство и распространении информации;
- применении информационных технологий;
- обеспечении защиты информации.

Закон не распространяется на отношения при правовой охране интеллектуальной деятельности.

Правовое регулирование основывается на:
- свободе поиска, получения, передачи, производства и распространения информации любым законным способом;
- установление ограничений доступа к информации только федеральными законами;
- открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации;
- обеспечение безопасности Российской Федерации при создании информационных систем и их эксплуатации;
-достоверность информации и своевременность ее представления;

18

Правовые основы обеспечения информационной безопасности

Закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ

Обладатель информации, оператор информационной системы обязаны обеспечить:
- предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- своевременное обнаружение фактов несанкционированного доступа к информации;
- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
- недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- постоянный контроль за обеспечением уровня защищенности информации;

19

Правовые основы обеспечения информационной безопасности

Закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ

Ст. 16 Защита информации

Защита информации представляет собой представляет собой принятие правовых, организационных и технических мер, направленных на:
- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения и иных неправомерных действий в отношении такой информации;
- соблюдение конфиденциальности информации ограниченного доступа;
- реализацию права на доступ к информации.

Ст. 17. Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации

Нарушение требований настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации

20

Правовые основы обеспечения информационной безопасности

Закон РФ «О лицензировании отдельных видов деятельности» от 04.05.2011 № 99-ФЗ

В соответствии с законом лицензированию подлежат следующие виды деятельности:
- разработка, производство, распространение шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств ;
- разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации;
- деятельность по выявлению электронных устройств, предназначенных для негласного получения информации;
- разработка и производство средств защиты конфиденциальной информации;
- деятельность по технической защите конфиденциальной информации;
- производство и реализация защищенной от подделок полиграфической продукции;

21

Правовые основы обеспечения информационной безопасности

Закон РФ «О техническом регулировании» от 27.12.2002 №184-ФЗ;

Закон регулирует отношения, возникающие при:
- разработке, принятии, применении и исполнении обязательных требований к продукции, в том числе зданиям и сооружениям, процессам проектирования, производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации;
- разработке, принятии, применении и исполнении на добровольной основе требований к продукции, процессам проектирования, производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг;

22

Правовые основы обеспечения информационной безопасности

Закон РФ «О техническом регулировании» от 27.12.2002 №184-ФЗ;

Статья 5. Особенности в отношении:
- оборонной продукции (работ, услуг), поставляемой по государственному оборонному заказу; 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;
- продукции (работ, услуг), сведения о которой составляют государственную тайну;

обязательными требованиями наряду с требованиями технических регламентов являются требования, установленные:
- государственными заказчиками;
- федеральными органами исполнительной власти;
- уполномоченными в области обеспечения безопасности, обороны, внешней разведки, противодействия техническим разведкам и технической защиты информации.

Особенности технического регулирования устанавливаются Президентом Российской Федерации и Правительством Российской Федерации.

23

Правовые основы обеспечения информационной безопасности

Закон РФ «О стандартизации» от 29.06.2015 № 162-ФЗ;

Стандартизация направлена на достижение цели обеспечения обороны страны и безопасности государства.

Статья 6.
Порядок стандартизации в отношении оборонной продукции (товаров, работ, услуг) по государственному оборонному заказу, продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, продукции, сведения о которой составляют государственную тайну, а также процессов и иных объектов стандартизации, связанных с такой продукцией, устанавливается **Правительством Российской Федерации**.

24

Правовые основы обеспечения информационной безопасности

Закон РФ «Об электронной подписи» от 06.04.2011 № 63-ФЗ;

1. Видами электронных подписей, отношения в области использования которых регулируются настоящим Федеральным законом, являются:
- простая электронная подпись;
- усиленная электронная подпись.
Различаются усиленная неквалифицированная электронная подпись и усиленная квалифицированная электронная подпись.

2. Простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

22

Правовые основы обеспечения информационной безопасности

Закон РФ «Об электронной подписи» от 06.04.2011 № 63-ФЗ;

3. Неквалифицированной электронной подписью является электронная подпись, которая:
- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- создается с использованием средств электронной подписи.

4. Квалифицированной электронной подписью является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:
- ключ проверки электронной подписи указан в квалифицированном сертификате;
- для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

26

Правовые основы обеспечения информационной безопасности

Закон РФ «О персональных данных» от 27.07.2006 № 152-ФЗ;

Закон регулирует деятельность физических и юридических лиц по обработке и использованию персональных данных.

В законе определяются требования и правила по защите персональных данных ко всем организациям, государственным и частным компаниям, которые хранят, обрабатывают и собирают персональные данные своих сотрудников, посетителей или клиентов.

Закон обязывает операторов персональных данных уведомлять об обработке персональных данных субъекта, получать его письменное разрешение и уведомлять об уничтожении персональных данных при прекращении отношений.

27

Правовые основы обеспечения информационной безопасности

Закон РФ «О персональных данных» от 27.07.2006 № 152-ФЗ;

Действие настоящего Федерального закона не распространяется на отношения, возникающие при:

- обработке персональных данных физическими лицами исключительно для личных и семейных нужд;
- организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов;
- обработке персональных данных, отнесенных к сведениям, составляющим государственную тайну;
- предоставлении уполномоченными органами информации о деятельности судов в Российской Федерации.

28

Правовые основы обеспечения информационной безопасности

Закон РФ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ;

Действие настоящего Федерального закона распространяется на государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы (объекты КИИ), информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сферах:

здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

29

Правовые основы обеспечения информационной безопасности

Закон РФ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ;

Критическая информационная инфраструктура (КИИ) – совокупность всех объектов КИИ и используемых ими сетей электросвязи;

Объекты КИИ подразделяются на значимые (три категории) и незначимые;

Субъекты КИИ сами определяют категории значимости своих объектов. Критерии для категорирования значимых объектов КИИ определяются постановлением Правительства.

Регулирование и надзор осуществляет ФСТЭК (федеральная служба по техническому и экспортному контролю), ФСБ (федеральная служба безопасности), Минкомсвязь, Банк России;

30

Правовые основы обеспечения информационной безопасности

Закон РФ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ;

Субъект КИИ обязан:

- обеспечивать выполнение порядка, технических условий установки и эксплуатации технических средств ГосСОПКА (Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак), если они устанавливаются на объектах КИИ;
- соблюдать требования по обеспечению безопасности и выполнять предписания регуляторов об устранении выявленных нарушений;
- оказывать содействие должностным лицам ФСТЭК, ФСБ и прочим регуляторам в деятельности, связанной с предупреждением, обнаружением и ликвидацией последствий инцидентов;
- незамедлительно информировать регуляторов об инцидентах нарушения информационной безопасности.

31

Правовые основы обеспечения информационной безопасности

Закон РФ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ;

Ответственность за невыполнение обязанностей:

- невыполнение требований по обеспечению безопасности КИИ («нарушение правил эксплуатации») – до 6 лет лишения свободы (до 8 лет в случае «группы лиц по предварительному сговору»);
- невыполнение требований по обеспечению безопасности КИИ в случае инцидента с тяжкими последствиями или угрозой таких последствий – до 10 лет лишения свободы.

32

Правовые основы обеспечения информационной безопасности

Указы Президента РФ

- **«Стратегия национальной безопасности Российской Федерации» от 31.12.2015 № 683;**

«О некоторых вопросах информационной безопасности Российской Федерации» от 22.05.2015 № 260;

- **Доктрина информационной безопасности, утвержденная Указом Президента Российской Федерации от 5 декабря 2016 г. № 646**

- **Стратегия развития информационной общества в Российской Федерации на 2017 -2030 от 9 мая 2017 г. N 203**

- «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» от 17.03.2008 №351;

- «О Федеральной службе по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия» от 12.03.2007 №320;

33

Правовые основы обеспечения информационной безопасности

Указы Президента РФ

- «Вопросы Федеральной службы по техническому и экспортному контролю» от 16.08.2004 №1013;

- «Вопросы Федеральной службы безопасности Российской Федерации» от 11.08.2003 №960;

- «Об утверждении перечня сведений, отнесенных к государственной тайне» от 30.11.1995 № 1203;

- «Об утверждении перечня сведений конфиденциального характера» от 06.03.1997 № 188;

- «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации» от 03.04.1995 № 334;

- «Об основах государственной политики в сфере информатизации» от 20.01.1994 № 1701;

34

Правовые основы обеспечения информационной безопасности

Стратегия национальной безопасности Российской Федерации» от 31.12.2015 № 683;

обеспечение национальной безопасности - реализация органами государственной власти и органами местного самоуправления во взаимодействии с институтами гражданского общества политических, военных, организационных, социально-экономических, информационных, правовых и иных мер, направленных на противодействие угрозам национальной безопасности и удовлетворение национальных интересов;

система обеспечения национальной безопасности - совокупность осуществляющих реализацию государственной политики в сфере обеспечения национальной безопасности органов государственной власти и органов местного самоуправления и находящихся в их распоряжении инструментов

35

Правовые основы обеспечения информационной безопасности

«Стратегия национальной безопасности Российской Федерации» от 31.12.2015 № 683;

Обеспечение национальных интересов осуществляется посредством реализации следующих стратегических национальных приоритетов:
- оборона страны;
- государственная и общественная безопасность;
- повышение качества жизни российских граждан;
- экономический рост;
- наука, технологии и образование;
- здравоохранение;
- культура;
- экология живых систем и рациональное природопользование;
- стратегическая стабильность и равноправное стратегическое партнерство.

36

Правовые основы обеспечения информационной безопасности

«Доктрина информационной безопасности» от 5 декабря 2016 г. № 646

Основные информационные угрозы национальной безопасности России:

- стремление «отдельных государств» использовать технологическое превосходство для доминирования в информационном пространстве;

- наращивание зарубежными странами возможностей по оказанию «информационно-психологического воздействия» на российское население с целью внутриполитической дестабилизации и подрыва суверенитета РФ;

- увеличение в зарубежных СМИ числа материалов, содержащих «предвзятую оценку государственной политики РФ», дискриминация российских средств массовой информации за рубежом нормативам.

37

Правовые основы обеспечения информационной безопасности

«Доктрина информационной безопасности» от 5 декабря 2016 г. № 646

- технологическое отставание РФ в сфере информационных технологий, высокий уровень зависимости от зарубежной компонентной базы и программного обеспечения, недостаточная эффективность отечественных научных исследований;

- рост киберпреступности, в первую очередь в кредитно-финансовой сфере.

38

Правовые основы обеспечения информационной безопасности

«Доктрина информационной безопасности» от 5 декабря 2016 г. № 646

Доктрина предусматривает пять основных сфер, в которых необходимо обеспечение информационной безопасности РФ:

- оборона;
- государственная безопасность;
- экономика;
- наука, технологии и образование;
- стратегическая стабильность.

39

Правовые основы обеспечения информационной безопасности

«Доктрина информационной безопасности» от 5 декабря 2016 г. № 646

Основные направления противостояния информационным угрозам:

- нейтрализация информационно-психологического воздействия, «направленного на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества» (оборона);
- повышение защищенности критически важной информационной инфраструктуры, противодействие экстремизму и размыванию «традиционных российских духовно-нравственных ценностей» (госбезопасность);

40

Правовые основы обеспечения информационной безопасности

«Доктрина информационной безопасности» от 5 декабря 2016 г. № 646

Основные направления противостояния информационным угрозам:

- инновационное развитие электронной промышленности, импортозамещение (экономика);
- разработка перспективных технологий (наука);
- развитие национальной системы управления российским сегментом интернета (стратегическая стабильность).

.

41

Правовые основы обеспечения информационной безопасности

«О некоторых вопросах информационной безопасности Российской Федерации» от 22.05.2015 № 260;

В целях противодействия угрозам информационной безопасности Российской Федерации при использовании информационно-телекоммуникационной сети "Интернет" на территории Российской Федерации предусмотрены следующие мероприятия:
Преобразование сегмента международной компьютерной сети "Интернет" для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, находящийся в ведении Федеральной службы охраны Российской Федерации, в российский государственный сегмент информационно-телекоммуникационной сети "Интернет«, являющийся элементом российской части сети "Интернет»

42

Правовые основы обеспечения информационной безопасности

«О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» от 17.03.2008 №351;

В целях обеспечения информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей, позволяющих осуществлять передачу информации через государственную границу Российской Федерации, в том числе при использовании международной компьютерной сети «Интернет» предусмотрены следующие мероприятия:

- подключение информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие **государственную тайну**, либо информации, обладателями которой являются государственные органы и которая содержит сведения, составляющие **служебную тайну**, к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу Российской Федерации, в том числе к международной компьютерной сети "Интернет" ***не допускается;***

43

Правовые основы обеспечения информационной безопасности

«О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» от 17.03.2008 №351;

- При необходимости подключения информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие **государственную тайну**, либо информации, обладателями которой являются государственные органы и которая содержит сведения, составляющие **служебную тайну**, к информационно-телекоммуникационным сетям международного информационного обмена *такое подключение производится только с использованием специально предназначенных для этого средств защиты информации, в том числе шифровальных (криптографических) средств, прошедших в установленном законодательством Российской Федерации порядке сертификацию в Федеральной службе безопасности Российской Федерации и (или) получивших подтверждение соответствия в Федеральной службе по техническому и экспортному контролю.*

44

Правовые основы обеспечения информационной безопасности

«Вопросы Федеральной службы по техническому и экспортному контролю» от 16.08.2004 №1013;

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) является федеральным органом исполнительной власти и осуществляет реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности **по вопросам**:

1) обеспечения безопасности (некриптографическими методами) информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере, в том числе в функционирующих в составе критически важных объектов Российской Федерации информационных системах и телекоммуникационных сетях, деструктивные информационные воздействия на которые могут привести к значительным негативным последствиям;

2) противодействия иностранным техническим разведкам на территории Российской Федерации;

45

Правовые основы обеспечения информационной безопасности

«Вопросы Федеральной службы по техническому и экспортному контролю» от 16.08.2004 №1013;

3) обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации;

4) защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;

5) осуществления экспортного контроля.

46

Правовые основы обеспечения информационной безопасности

«Вопросы Федеральной службы безопасности Российской Федерации» от 11.08.2003 №960;

Одними из основных задач ФСБ России являются:

- обеспечение в пределах своих полномочий защиты сведений, составляющих государственную тайну, и противодействия иностранным организациям, осуществляющим техническую разведку;

- формирование и реализация в пределах своих полномочий государственной и научно-технической политики в области обеспечения информационной безопасности;

- организация в пределах своих полномочий обеспечения криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, а также систем шифрованной, засекреченной и иных видов специальной связи в Российской Федерации и ее учреждениях за рубежом.

47

Правовые основы обеспечения информационной безопасности

«Об утверждении перечня сведений, отнесенных к государственной тайне» от 30.11.1995 № 1203;

К сведениям, отнесенных к государственной тайне относятся:

- сведения в военной области;

- сведения в области экономики, науки и техник;

- сведения в области внешней политики и экономики;

- сведения в области разведывательной, контрразведывательной и оперативно-разыскной деятельности, в области противодействия терроризму и обеспечения безопасности лиц, в отношении которых принято решение о применении мер государственной защиты;

48

Правовые основы обеспечения информационной безопасности

«Об утверждении перечня сведений конфиденциального характера» от 06.03.1997 № 188;

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

2. Сведения, составляющие тайну следствия и судопроизводства, сведения о лицах, в отношении которых принято решение о применении мер государственной защиты, а также сведения о мерах государственной защиты указанных лиц, если законодательством Российской Федерации такие сведения не отнесены к сведениям, составляющим государственную тайну.

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

49

Правовые основы обеспечения информационной безопасности

«Об утверждении перечня сведений конфиденциального характера» от 06.03.1997 № 188;

4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).

5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

7. Сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц.

50

Правовые основы обеспечения информационной безопасности

Постановления Правительства РФ:

- «Об утверждении правил организации и осуществления федерального государственного контроля за обеспечением защиты государственной тайны» от 22.12.2012 №1376;

- «Об утверждении требований к защите персональных данных при обработке в информационных системах персональных данных» от 01.11.2012 № 1119

- «О видах электронной подписи, использование которых допускается при обращении за получением государственных и муниципальных услуг» от 25.06.2012 № 634;

- «О лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных и телекоммуникационных систем …» от 16.04.2012

51

Правовые основы обеспечения информационной безопасности

Постановления Правительства РФ:

- «О лицензировании деятельности по разработке и(или) производству средств защиты конфиденциальной информации» от 03.03.2012 № 171;

- «О лицензировании деятельности по технической защите конфиденциальной информации» от 03.02.2012 № 79;

- «Об организации лицензировании отдельных видов деятельности» от 21.11.2011 № 957;

- «О единой системе межведомственного электронного взаимодействия» от 08.09.2010 № 697;

- «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой…. » от 21.04.2010 № 266;

52

Правовые основы обеспечения информационной безопасности

Постановления Правительства РФ:

- «Об утверждении Инструкции о порядке доступа должностных лиц и граждан Российской Федерации к государственной тайне» от 06.02.2010 № 63;

«Об утверждении единого перечня продукции, подлежащей обязательной сертификации, и единого перечня продукции, подтверждение соответствия которой осуществляется в форме принятия декларации о соответствии» » от 01.12.2009 № 982;

- «Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям» от 18.05.2009 № 424;

- «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» от 16.03.2009 № 228;

- «Об утверждении Положения о лицензировании внешнеэкономических операций с товарами, информацией, работами, услугами, результатами интеллектуальной деятельности (правами на них), в отношении которых установлен экспортный контроль» от 15.09.208 № 691;

53

Правовые основы обеспечения информационной безопасности

Постановления Правительства РФ:

- «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008 № 687;

- «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных» от 06.07.2008 № 512;

- «О порядке проведения проверки наличия в заявках на выдачу патента на изобретение или полезную модель, созданные в Российской Федерации, сведений, составляющих государственную тайну» от 24.12.2007 №928;

- «О государственной аккредитации организаций, осуществляющих деятельность в области информационных технологий» от 06.11.2007 №758;

54

Правовые основы обеспечения информационной безопасности

Постановления Правительства РФ:

- «О Федеральном агентстве по техническому регулированию и метрологии» от 17.06.2004 №294;

- «Об утверждении Положения о создании и деятельности экспертных комиссий по техническому регулированию» от 21.08.2003 №513;

- «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну…» от 15.04.95 № 333;

- «Положение о сертификации средств защиты информации» от 26.06.1995 № 608;

- «Об утверждении правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» от 04.09.1995 № 870;

- «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» от 03.11.1994 №1233.

55

Структура государственной системы защиты информации



56

Структура государственной системы защиты информации

В состав системы обеспечения информационной безопасности Российской Федерации также входят:

- Федеральная служба по техническому и экспортному контролю (ФСТЭК России);
- Федеральная служба безопасности Российской Федерации (ФСБ России);
- Служба внешней разведки Российской Федерации (СВР России);
- Министерство обороны Российской Федерации (Минобороны России);
- Министерство внутренних дел Российской Федерации (МВД России);
- Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

57

Структура государственной системы защиты информации

Федеральная служба по техническому и экспортному контролю (ФСТЭК России)

- организует деятельность государственной системы противодействия техническим разведкам и технической защиты информации и руководит ею.
- является органом защиты *государственной тайны*, наделенным полномочиями по распоряжению сведениями, составляющими *государственную тайну*.
- Руководство деятельностью ФСТЭК России осуществляет Президент Российской Федерации.
- ФСТЭК России подведомственна Минобороны России. ФСТЭК России и ее территориальные органы входят в состав государственных органов обеспечения безопасности.

58

Структура государственной системы защиты информации

Основными задачами ФСТЭК России являются:

- Организация деятельности государственной системы противодействия техническим разведкам и технической защиты информации на федеральном, межрегиональном, региональном, отраслевом и объектовом уровнях, а также руководство указанной государственной системой.
- Осуществление самостоятельного нормативно-правового регулирования вопросов организации защиты информации.
- Противодействие добыванию информации техническими средствами разведки, техническая защита информации.
- Осуществление центральным аппаратом ФСТЭК России организационно-технического обеспечения деятельности Межведомственной комиссии по защите *государственной тайны* и Комиссии по экспортному контролю Российской Федерации

59

Структура государственной системы защиты информации

Как преемник деятельности Гостехкомиссиии России ФСТЭК наделена следующими полномочиями:

- организация и проведение лицензирования деятельности по осуществлению мероприятий и/или оказанию услуг в области защиты *государственной тайны* (в части, касающейся противодействия техническим разведкам и/или технической защиты информации);
- создание *средств защиты информации*, содержащей сведения, составляющие *государственную тайну*;
- техническая защита конфиденциальной информации;
- разработка и/или производство средств защиты конфиденциальной информации, а также *лицензирование* иных видов деятельности в соответствии с законодательством Российской Федерации.

Решения ФСТЭК России являются обязательными для исполнения всеми органами государственной власти и местного самоуправления, государственными и негосударственными предприятиями, учреждениями, организациями, должностными лицами и гражданами

60

Структура государственной системы защиты информации

Федеральная служба безопасности Российской Федерации (ФСБ России):

-ФСБ России является федеральным органом исполнительной власти.

- Руководит ФСБ Президент.

- При ФСБ России действует Академия криптографии Российской Федерации.

- Основные цели, задачи и функции ФСБ описаны в "Положении о Федеральной службе безопасности Российской Федерации и ее структуре".

- ФСБ определяет порядок осуществления в пределах своих полномочий контроля за организацией и функционированием криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, систем шифрованной, засекреченной и иных видов специальной связи.

61

Структура государственной системы защиты информации

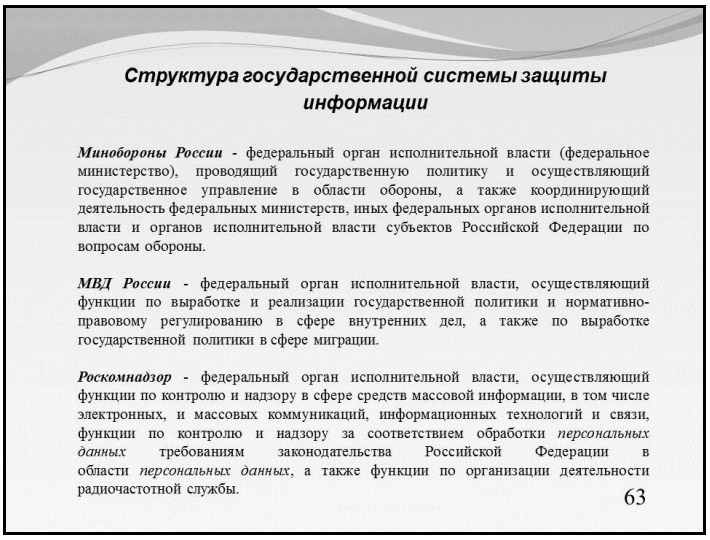
Федеральная служба безопасности Российской Федерации (ФСБ России):

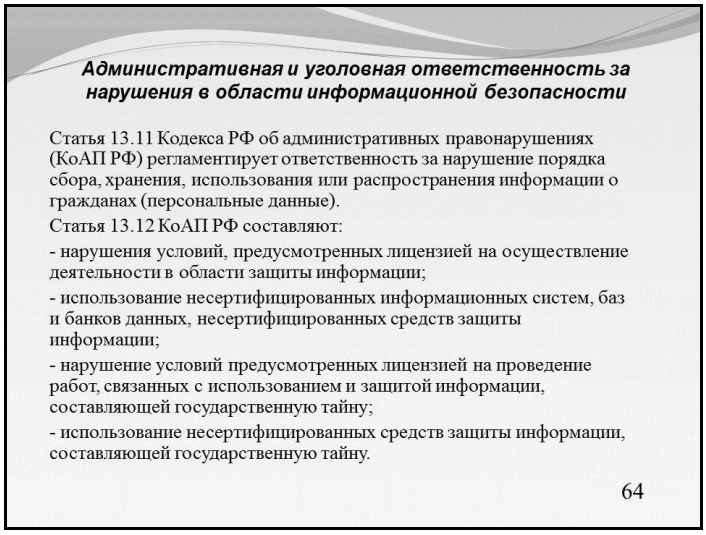
-ФСБ осуществляет и организует в соответствии с федеральным законодательством *сертификацию средств защиты информации*, систем и комплексов *телекоммуникаций*, технических средств, используемых для выявления электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах;

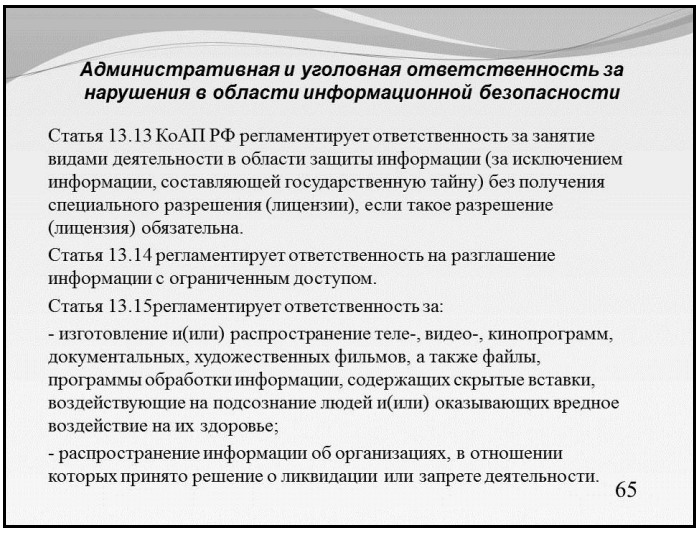
- определяет основные направления деятельности органов федеральной службы безопасности в этих областях;

- осуществляет и организует в соответствии с федеральным законодательством *лицензирование* отдельных видов деятельности.

62







Литература: Аверченков, В. И. Служба защиты информации: организация и управление : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стереотип. - Москва :

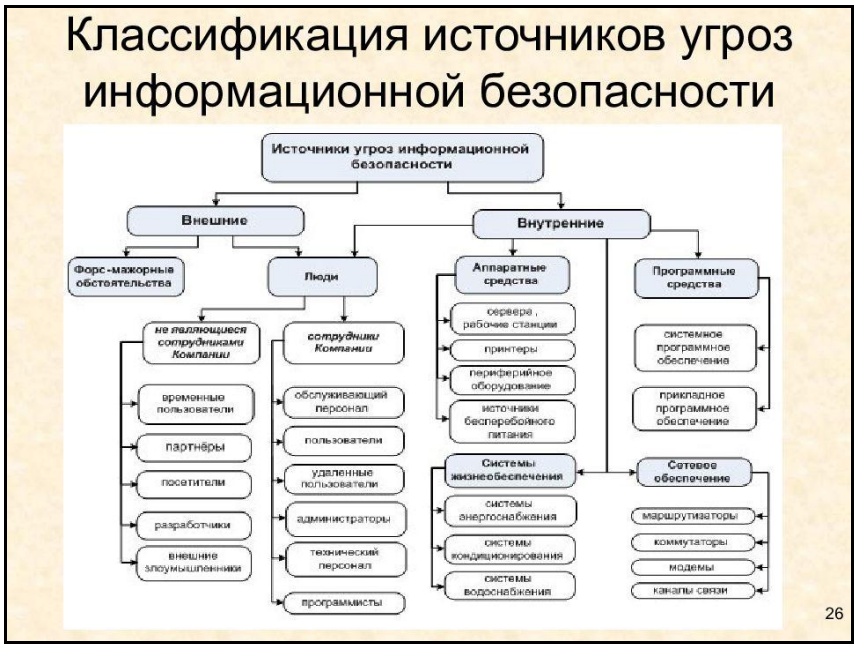
Издательство «Флинта», 2016. - 186 с. - Библиогр. в кн. - ISBN 978-5-9765-1271-9 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93356

Лекция 2. Угрозы информации

Тезисы лекции:

- Информационная безопасность сетей.
- Информационная безопасность в условиях функционирования в России глобальных сетей.
- Угрозы информационной безопасности для АСОИ.
- Способы совершения компьютерных преступлений.
- Уязвимость сети Интернет.
- Пользователи и злоумышленники в Интернет.
- Причины уязвимости сети Интернет.
- Удаленные атаки на интрасети.
- Банк данных угроз безопасности информации ФСТЭК России.

Иллюстративный материал к лекции:



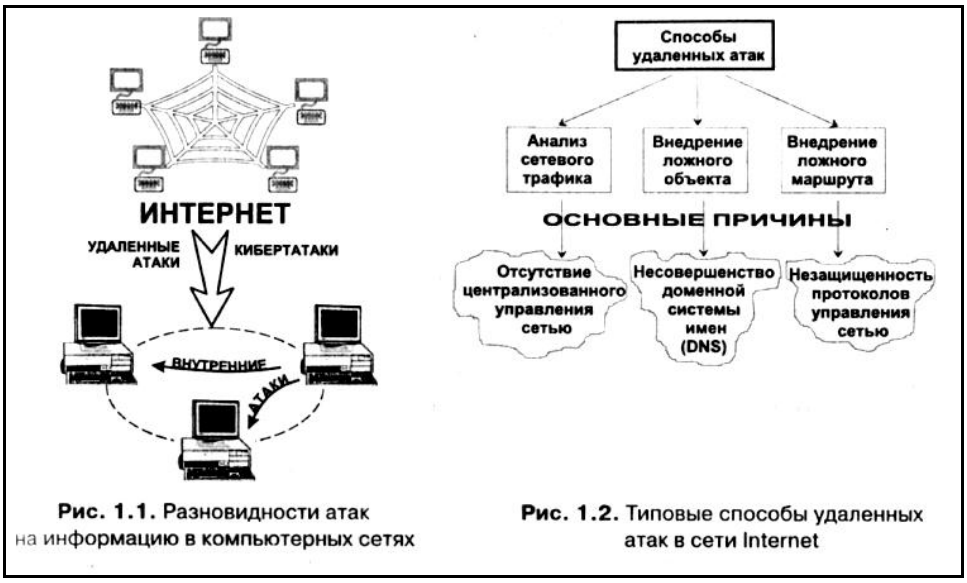


Рис. 1.1. Разновидности атак на информацию в компьютерных сетях

Рис. 1.2. Типовые способы удаленных атак в сети Internet





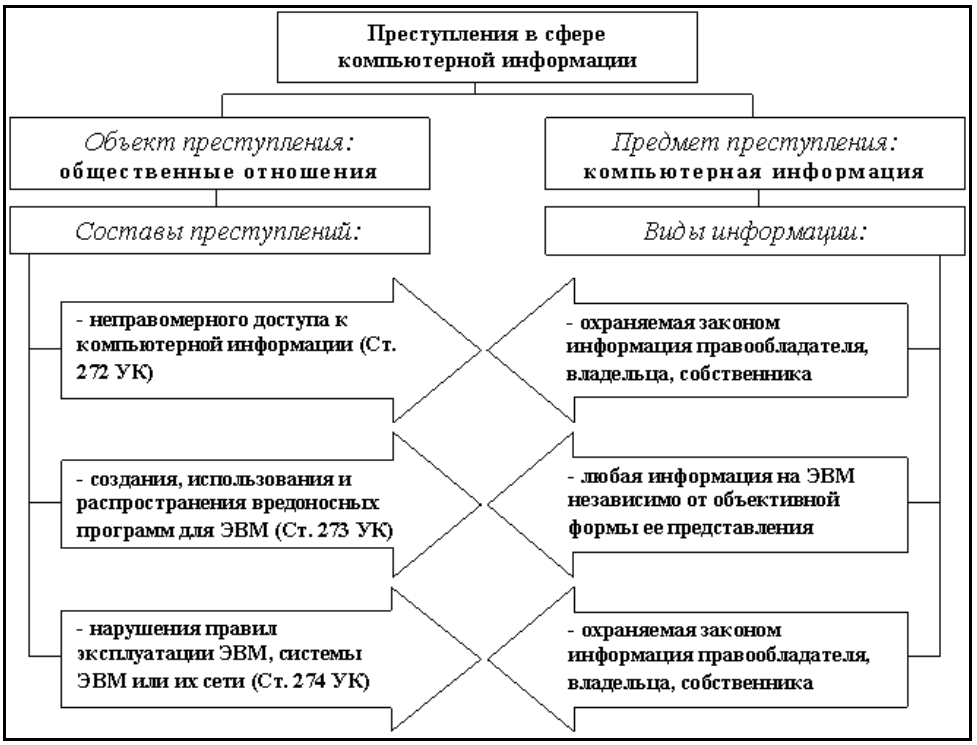
Литература: Загинайлов, Ю. Н. Основы информационной безопасности: курс визуальных лекций : учебное пособие / Ю.Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. - 105 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3947-4 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=362895

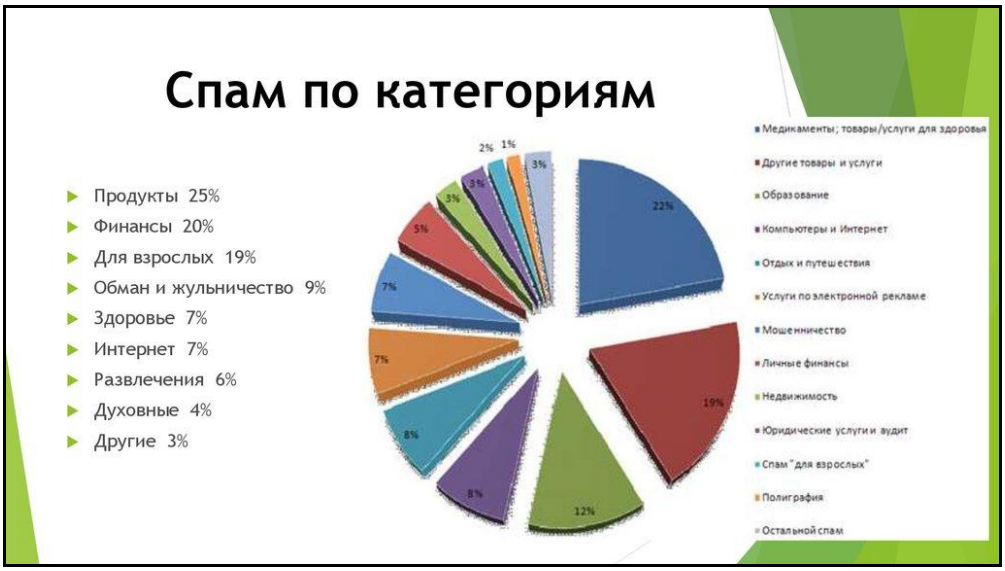
Лекция 3. Виды возможных нарушений безопасности информационной системы
Тезисы лекции:

- Компьютерные преступления.
- Классификация компьютерных преступлений.
- Виды противников или «нарушителей».
- Вредоносные программы.
- Условия существования вредоносных программ.
- Хакерские утилиты и прочие вредоносные программы.
- Спам.
- Вирусы.
- Понятия о видах вирусов.
- Классические компьютерные вирусы.
- Сетевые черви.
- Троянские программы.

Иллюстративный материал к лекции:







Литература: Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика : учебное пособие / В. Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. : схем., табл. – ISBN 978-5-4499-0496-6. – DOI 10.23681/571485; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=571485

Лекция 4. Информационная безопасность информационных систем

Тезисы лекции:

- Теория информационной безопасности информационных систем.
- Основные положения теории информационной безопасности информационных систем.
- Модели безопасности и их применение.
- Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Криптографические способы защиты информации.
- Анализ способов нарушений информационной безопасности.
- Использование защищенных компьютерных систем.
- Методы криптографии.
- Классификация методов криптографического закрытия информации.
- Шифрование.
- Симметричные криптосистемы.
- Криптосистемы с открытым ключом (асимметричные).
- Характеристики существующих шифров.
- Кодирование.
- Стеганография.
- Электронная цифровая подпись.
- Организация информационной безопасности компании.
- Основные технологии построения защищенных ЭИС.
- Место информационной безопасности экономических систем в национальной безопасности страны.
- Организация информационной безопасности компании.
- Выбор средств информационной безопасности.

Слайды презентации к лекции:

Информационная безопасность информационных систем

Криптография. Шифрование

Криптография

(от греч. κρυπτός — скрытый и γράφω — пишу)

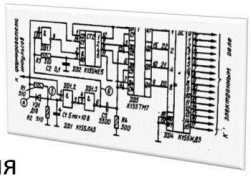
Криптография - наука о методах обеспечения конфиденциальности и аутентичности (целостности и подлинности авторства) информации.

КЛЮЧ

Ключ — параметр шифра, определяющий выбор конкретного преобразования данного текста.



В современных шифрах алгоритм шифрования известен, и криптографическая стойкость шифра целиком определяется секретностью ключа (Принцип Керкгоффса).



Шифрование —применения криптографического преобразования открытого текста на основе алгоритма и ключа шифрованный текст.

Расшифровывание — процесс нормального применение криптографического преобразования шифрованного текста в открытый.

Виды текста

Открытый (исходный) текст — данные передаваемые без использования криптографии.

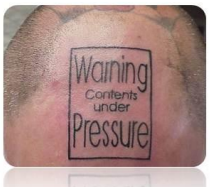
Закрытый (шифрованный) текст — данные, полученные после применения криптосистемы с указанным ключом.

Первые примеры криптогрфии

татуировка

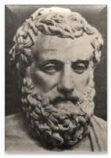
Геродот (484 до н. э. – 425 до н. э.) Татуировка, сделанная на обритой голове раба, скрытая под отросшими волосами.







Скитала (шифр Древней Спарты)



Впервые скитала упоминается греческим поэтом Архилохом.

Скитала — это деревянный цилиндр.

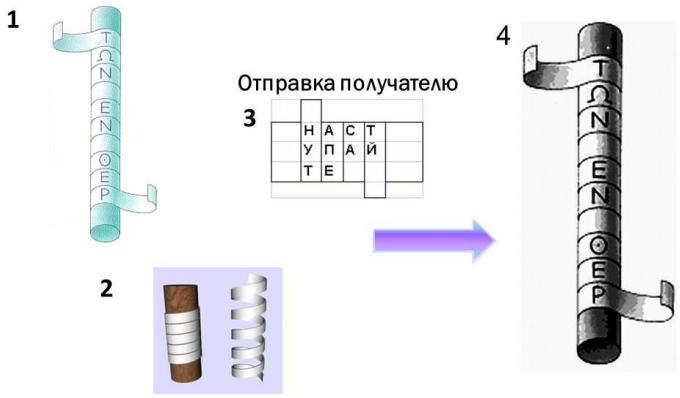
(от греч. Σκυτάλη – жезл)

Для криптосвязи требуется два цилиндра (одна скитала у того, кто будет отправляет сообщение, другая — у адресата.

Диаметр обоих должен быть строго одинаковым.



Принцип шифрования



библия

Книга пророка Иеремии (22,23): "...а царь *Сессаха* выпьет после них."

На языке оригинала мы имеем слово *Вавилон*.



Атбаш

Исходный текст:
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Зашифрованный текст:
ZYXWVUTSRQPONMLKJIHGFEDCBA

диск с шифротекстом Альберти

Леон Баттиста Альберти
(1404-1472)
«Трактат о шифрах»



Первая буква шифруется по первому шифроалфавиту, вторая по второму и т.д.



решетка Кардану

Джероламо Кардано (1501-1576)



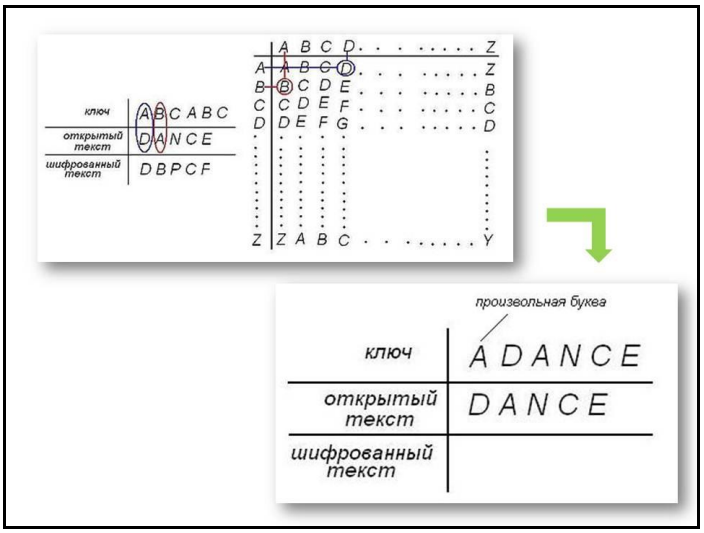
«YOU KILL AT ONCE»

«I LOVE YOU. I HAVE YOU DEEP UNDER MY SKIN. MY LOVE LASTS FOREVER IN HYPERSPACE».

I		L	O	V	E		Y	O	U					
I		H	A	V	E		Y	O	U					
D	E	E	P		U	N	D	E	R					
M	Y		S	K	I	N		M	Y					
L	O	V	E		L	A	S	T	S					
F	O	R	E	V	E	R		I	N					
H	Y	P	E	R	S	P	A	C	E					


Петр и Модест Чайковс
Замена каждой гласной русского языка на другую гласную, каждой согласной - на другую согласную:
«шыр-пир ю пяпюжгы зэлэмьгый гесрыг»
вместо:
«жил-был у бабушки серенький козлик».


Шифр Виженера
Ключ - ABC
ключ A B C A B C
открытый текст D A N C E
шифрованный текст


ключ A B C A B C
открытый текст D A N C E
шифрованный текст D B P C F
произвольная буква
ключ A D A N C E
открытый текст D A N C E
шифрованный текст

Литература о криптографии

- **«Трактат о шифрах»,** Габриэль де Лавинд
- **«Энциклопедия всех наук»,** Шехаба Калкашанди (методы засекречивания содержания переписки)
- **«Интеллидженс сервис»,** Оливер Кромвель (раздел по дешифровке)
- **«Военная криптография»,** Огюст Кергоффс

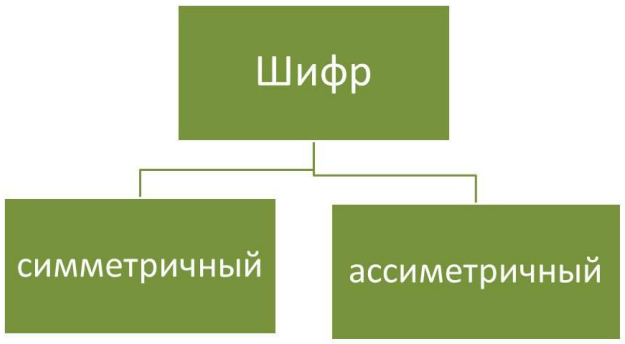
…

Шифр

(от араб. صِفْر ,ṣifr «ноль», фр. chiffre «цифра»; родственно слову цифра)

Шифр — совокупность алгоритмов криптографических преобразований.





классические виды шифрования простая замена

а б в г д е … я

1 2 3 4 5 6 … 33

Или:

A b c d t f …

! @ # $ % *…

Пример:

33 9 29 12 16 9 15 1 15 10 6

ЯЗЫКОЗНАНИЕ

Перестановочный вид

Буквы сообщения переставляются:

«помоги мне» → *«опомиг нме»*

«приду во вторник» *«рпдиу ов твроинк»*

Замещающий вид

Замены каждой буквы следующей за ней в алфавите:

«очень быстро» → *«пшжоы вътусп»*

“good bye” *”hppe czf”*

Шифр цезаря

Н → о п Р с …

Юлий Цезарь использовал шифр со смещением 3 при связи со своими полководцами во время военных кампаний.

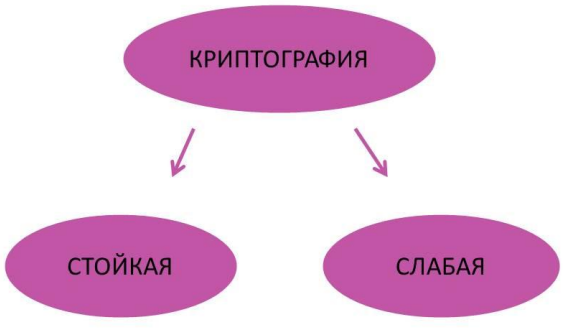


Криптография и другие науки

До XX века криптография имела дело только с языковедческими образцами.

Сейчас:

- использование математики
- часть инженерного дела
- применение в криптографии квантовой физики



Криптографическая атака

Криптографическая атака – результаты криптоанализа конкретного шифра.



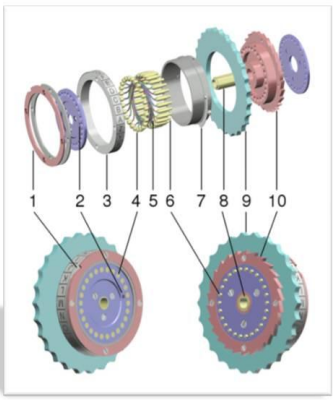
Роторная криптомашина Enigma

Первая шифровальная машина.

Использовалась германскими войсками с конца 1920-х годов до конца Второй мировой войны.

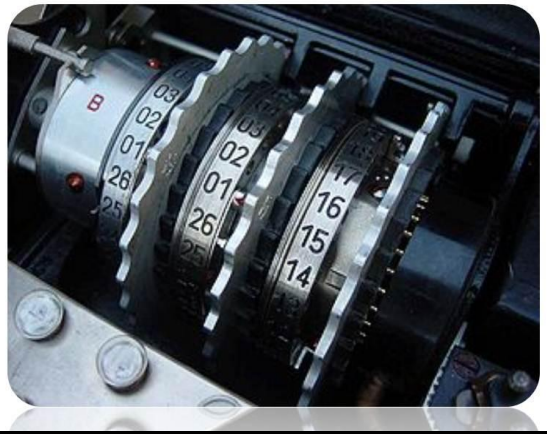


Ротор в разобранном виде



1. кольцо с выемками
2. маркирующая точка
3. для контакта «А»
4. алфавитное кольцо
5. залужённые контакты
6. электропроводка
7. штыревые контакты
8. пружинный рычаг для
9. настройки кольца
10. втулка
11. пальцевое кольцо
12. храповое колесо

Роторы Энигмы в собранном состоянии



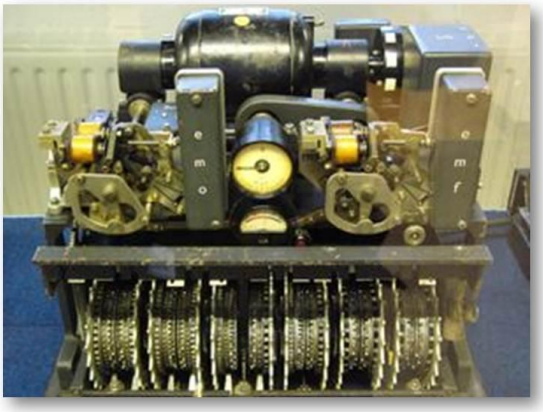
Примеры шифрования Энигмы

E = PRMLUL − 1M − 1R − 1P − 1

E = P(ρiRρ − i)(ρjMρ − j)(ρkLρ − k)U(ρkL − 1ρ − k)(ρjM − 1ρ − j)(ρiR − 1ρ − i)P − 1



Немецкая криптомашина Lorenz



Криптоанализ

Криптоанализ – наука о методах получения исходного значения зашифрованной информации, не имея доступа к секретной информации (ключу), необходимой для этого.

(Уильям Ф. Фридман, 1920)



Криптоаналитик — человек, создающий и применяющий методы криптоанализа.



криптология

Криптология – наука, занимающаяся методами шифрования и дешифрования.



современная криптография

Включает в себя:

- асимметричные криптосистемы
- системы электронной цифровой подписи (ЭЦП) хеш-функции
- управление ключами
- получение скрытой информации
- квантовую криптографию

Современная криптография

Распространенные алгоритмы:

- симметричные DES, Twofish, IDEA, и др.;
- асимметричные RSA и Elgamal
- хэш-функций MD4, MD5, ГОСТ Р 34.11-94.

RSA

RSA (буквенная аббревиатура от фамилий Rivest, Shamir и Adleman) — криптографический алгоритм с открытым ключом.

Схема RSA

A - отправитель

B - получатель

M - сообщение



Алгоритм:

- Взять *открытый ключ* (e, n) стороны A
- Взять открытый текст M
- Передать шифрованное сообщение:

$$P_A(M) = M^e \mod n \qquad (1)$$

Алгоритм:

- Принять зашифрованное сообщение C
- Применить свой *секретный ключ* (d, n) для расшифровки

$$S_A(C) = C^d \mod n \qquad (2)$$

СОВРЕМЕННЫЕ СРЕДСТВА ШИФРОВАНИЯ

Симпатические черни́ла — это чернила, записи которыми становятся видимыми только при определенных условиях.





микроточки

Микроточка — изображение, уменьшенное до такой степени, что невозможно обнаружить.



Фотокамера «Mark IV» для получения микроточек.



Список производителей, использующих микроточки:







- Audi
- BMW в Австралии
- Mitsubishi Ralliart
- Porsche
- Subaru
- Техмашимпорт (Techmashimport) в России
- Toyota

Цифровые водяные знаки

Цифровой водяной знак - это специальная метка, встраиваемая в цифровой контент с целью защиты авторских прав.



Актуальность шифрования сегодня

- широкое использование World Wide Web
- появление современных сверхмощных компьютеров



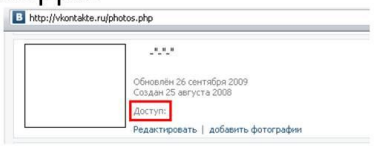


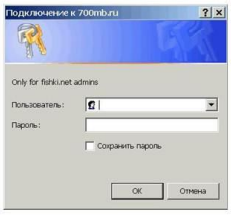
- расширилась сфера применения компьютерных сетей
- возможность дискредитации шифровых систем еще вчера считавшихся совершенно безопасными



Средства защиты информации сегодня









Литература: Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. -

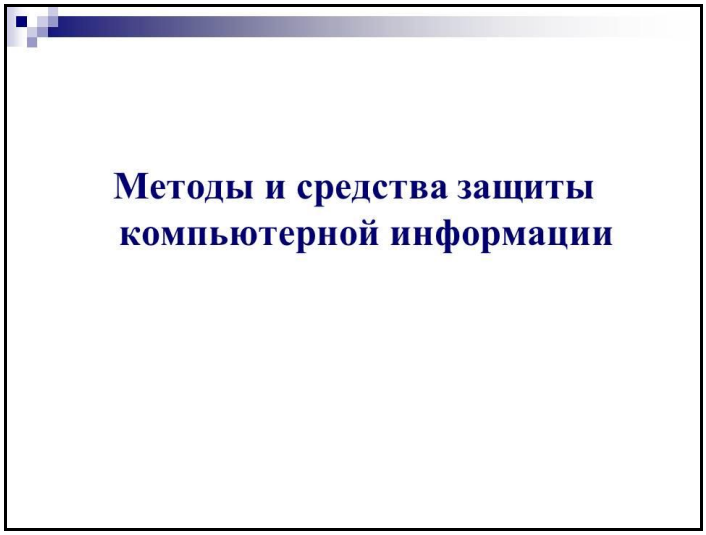
253 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557

Лекция 5. Методы и средства защиты компьютерной информации

Тезисы лекции:

- Обеспечения информационной безопасности. Методы обеспечения информационной безопасности РФ.
- Ограничение доступа. Контроль доступа к аппаратуре. Контроль доступа к информации. Разграничение и контроль доступа к информации.
- Предоставление привилегий на доступ.
- Идентификация и установление подлинности объекта (субъекта).
- Методы и средства защиты информации. Методы и средства защиты информации от случайных воздействий. Методы защиты информации от аварийных ситуаций.
- Организационные мероприятия по защите информации.
- Защита информации от утечки за счет побочного электромагнитного излучения и наводок.
- Антивирусное ПО.
- Признаки заражения компьютера. Источники компьютерных вирусов.
- Основные правила защиты.
- Вирусные описания на сайте Dr.Web.

Слайды презентации к лекции:



Цели изучения темы

- изучить методы разграничения доступа пользователей и процессов к ресурсам защищенной информационной системы.
- изучить сущность и механизм реализации "регистрации" и "аудита" в целях повышения защищенности информационных систем.

- После выполнения идентификации и аутентификации подсистема защиты устанавливает полномочия (совокупность прав) субъекта для последующего контроля санкционированного использования объектов информационной системы.
- Обычно полномочия субъекта представляются: **списком ресурсов**, доступным пользователю и **правами по доступу** к каждому ресурсу из списка.

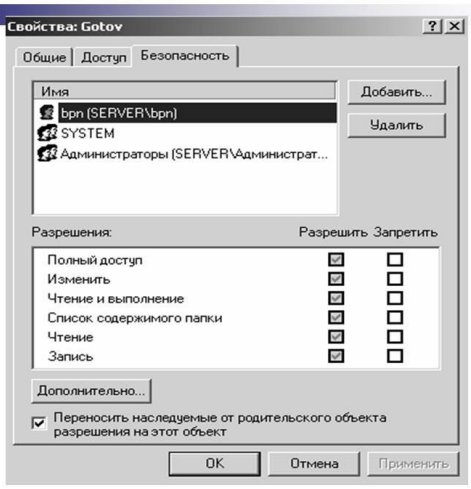
Существуют следующие методы разграничения доступа:

- Разграничение доступа по спискам.
- Использование матрицы установления полномочий.
- Разграничение доступа по уровням секретности и категориям.
- Парольное разграничение доступа.

При разграничении доступа по спискам задаются соответствия: каждому пользователю – список ресурсов и прав доступа к ним или каждому ресурсу – список пользователей и их прав доступа к данному ресурсу.

Списки позволяют установить права с точностью до пользователя. Здесь нетрудно добавить права или явным образом запретить доступ. Списки используются в подсистемах безопасности операционных систем и систем управления базами данных.

Пример (операционная система Windows 2000) разграничения доступа по спискам для одного объекта показан на рисунке.



Мандатное и дискретное управление доступом

В ГОСТе Р 50739-95 **"Средства вычислительной техники. Защита от несанкционированного доступа к информации"** и в документах Гостехкомиссии РФ определены два вида (принципа) разграничения доступа:

- дискретное управление доступом;
- мандатное управление доступом.

- **Дискретное управление** доступом представляет собой разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту. Данный вид организуется на базе методов разграничения по спискам или с помощью матрицы.
- **Мандатное управление доступом** основано на сопоставлении меток конфиденциальности информации, содержащейся в объектах (файлы, папки, рисунки) и официального разрешения (допуска) субъекта к информации соответствующего уровня конфиденциальности.

При внимательном рассмотрении можно заметить, что дискретное управление доступом есть ничто иное, как произвольное управление доступом (по "Оранжевой книге США"), а мандатное управление реализует принудительное управление доступом.

Определение и содержание регистрации и аудита информационных систем

Регистрация является еще одним механизмом обеспечения защищенности информационной системы. Этот механизм основан на подотчетности системы обеспечения безопасности, фиксирует все события, касающиеся безопасности, такие как:

- вход и выход субъектов доступа;
- запуск и завершение программ;
- выдача печатных документов;
- попытки доступа к защищаемым ресурсам;
- изменение полномочий субъектов доступа;
- изменение статуса объектов доступа и т. д.

Реализация механизмов регистрации и аудита позволяет решать следующие задачи обеспечения информационной безопасности:

- обеспечение подотчетности пользователей и администраторов;
- обеспечение возможности реконструкции последовательности событий;
- обнаружение попыток нарушений информационной безопасности;
- предоставление информации для выявления и анализа проблем.

Практическими средствами регистрации и аудита являются:

- различные системные утилиты и прикладные программы;
- регистрационный (системный или контрольный) журнал.

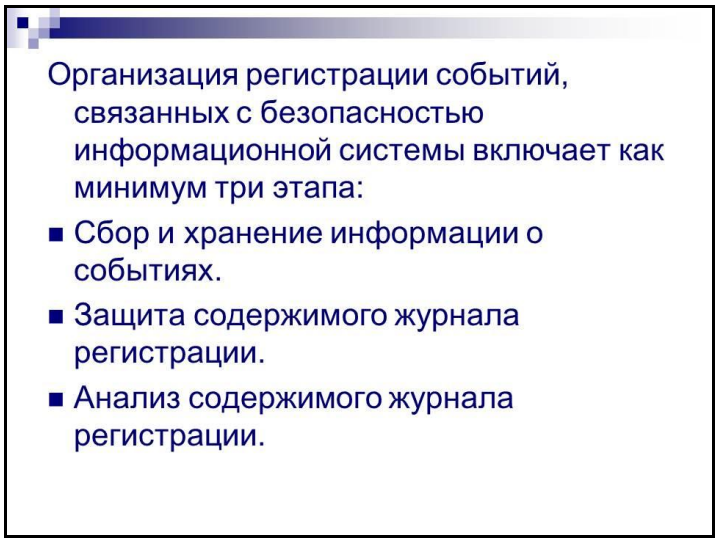
Регистрационный журнал – это хронологически упорядоченная совокупность записей результатов деятельности субъектов системы, достаточная для восстановления, просмотра и анализа последовательности действий, окружающих или приводящих к выполнению операций, процедур или совершению событий при транзакции с целью контроля конечного результата.

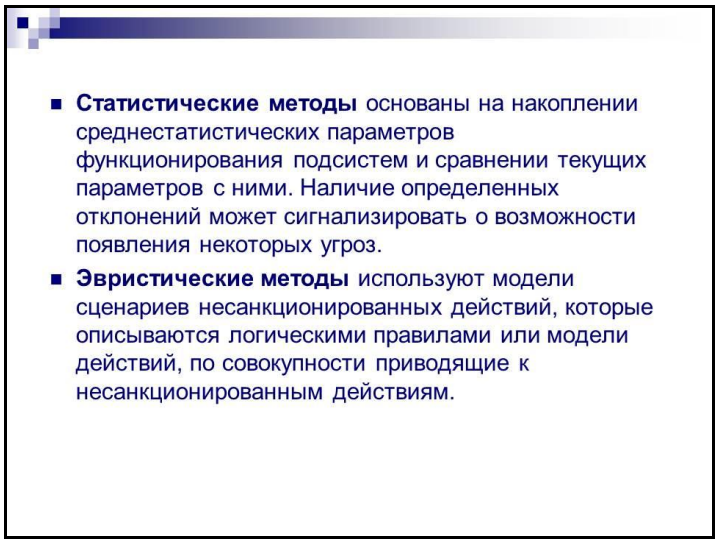
Фрагмент журнала безопасности подсистемы регистрации и аудита операционной системы показан на рисунке

Безопасность 13 событий

Тип	Дата	Время	Источник	Категория	Событие	Пользователь	Компьютер
Аудит успехов	26.04.2004	5:35:02	Security	Доступ к объектам	562	admin	GHJ
Аудит успехов	26.04.2004	5:35:02	Security	Доступ к объектам	562	admin	GHJ
Аудит успехов	26.04.2004	5:35:02	Security	Учетные записи	643	admin	GHJ
Аудит успехов	26.04.2004	5:35:02	Security	Доступ к объектам	560	admin	GHJ
Аудит успехов	26.04.2004	5:35:02	Security	Доступ к объектам	560	admin	GHJ
Аудит успехов	26.04.2004	5:34:49	Security	Доступ к объектам	562	admin	GHJ

Этапы регистрации и методы аудита событий информационной системы





Литература: Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика : учебное пособие / В. Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. : схем., табл. – ISBN 978-5-4499-0496-6. – DOI 10.23681/571485; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=571485

Лекция 6. Итоговая лекция. Подведение и анализ промежуточных результатов освоения дисциплины

Итоговая лекция завершает изучение дисциплины, обобщает пройденное за весь период. При ее подготовке учитываются пробелы в знаниях аспирантов, выявленные на практических занятиях и при оценке самостоятельной работы. Аспиранты получают установку на их устранение и на дальнейшее совершенствование своей подготовки в данной области. На лекции подводятся итоги изучения дисциплины, показывается ее значение в профессиональной сфере и формировании научного мировоззрения, обсуждается вопрос о подведении итогов изучения дисциплины – прохождения тестирования и сдаче кандидатского экзамена по специальности.

2. Методические указания по подготовке к занятиям семинарского типа

2.1. Планы и (или) методические рекомендации к практическим занятиям

В рамках проведения занятий по дисциплине предполагается организация следующих практических занятий:

Практическое занятие 1. Концепция информационной безопасности

Тематика: Лицензирование и сертификация в области защиты информации.

Текст задания №1 «Лицензирование деятельности по защите информации»

Контрольные вопросы для изучения:

1) Основные понятия: лицензия, лицензируемые виды деятельности, соискатель лицензии, лицензиат.

2) Законодательная основа лицензирования в современной России.

3) Лицензионные требования и условия применительно к видам деятельности по обеспечению информационной безопасности.

4) Лицензирующие органы, процедуры их взаимодействия с соискателями лицензий и лицензиатами; нормативные сроки; реестр лицензий.

Практические задания:

1) Составить перечень видов деятельности, требующих для исполнения лицензии по современному законодательству РФ (5…7 направлений).

2) Определить, какие органы исполнительной власти выдают лицензии на право осуществления образовательной деятельности? а какие – на право владения огнестрельным оружием?

3) Разработать план-график действий для гипотетической организации – соискателя лицензии на осуществление одного из видов лицензируемой деятельности в области защиты информации. Сопоставить ориентировочные затраты денежных и материальных ресурсов, продолжительность и кадровое обеспечение отдельных этапов лицензирования.

Текст задания №2 «Сертификация средств защиты информации»

Контрольные вопросы для изучения:

1) Основные понятия: сертификация, сертификат соответствия, система сертификации (сертифицирующих органов).

2) Законодательная основа осуществления сертификации средств защиты информации в современной России.

3) Федеральные органы сертификации, профильные органы сертификации, испытательные лаборатории, разработчики / производители / продавцы – процедуры их взаимодействия и нормативные сроки отдельных этапов сертификации.

4) Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00.

Практические задания:

1) Изучить ознакомительный материал «Примерный перечень действий по сертификации средств защиты информации», представленный в Приложении 3.

2) Подготовить FAQ по сертификации на основании изученного материала, включающий развёрнутые и адаптированные ответы на следующие вопросы:

а) Кто выступает инициатором сертификации?

б) Может ли сертификация проводится в плановом порядке (по заранее утвержденному графику)?

в) Куда направляется Заявка на проведение сертификации?

г) Может ли Заявитель выбирать исполнителя сертификационных испытаний?

д) Кто оплачивает расходы на проведение сертификации?

е) Каков максимальный срок получения Решения по Заявке на сертификацию?

ж) Кому направляются экземпляры Решения?

з) Что входит в комплект документов при заключении Договора между Заявителем и Испытательной Лабораторией?

и) На основании чего Испытательная лаборатория устанавливает стоимость сертификационных испытаний?

к) Кто составляет программу сертификационных испытаний?

л) Кто настраивает оборудование (например, испытательный стенд) для сертификационных испытаний?

м) Может ли Заявитель оперативно (в ходе испытаний) вносить улучшения в конструкцию и/или комплектацию сертифицируемой продукции?

н) Какие документы составляются по результатам сертификационных испытаний?

о) Кому направляются результаты испытаний?

п) Кто исполняет экспертизу результатов испытаний и какие документы появляются «на выходе» этого процесса?

р) Кто принимает решение о выдаче сертификата соответствия?

3) Изучить Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00 (доступен на официальном сайте ФСТЭК) и определить:

а) Сколько всего сертификатов внесено в Госреестр в настоящее время?

б) Когда были выданы первый и последний (на данный момент) сертификаты? какие объекты были сертифицированы первым и последним?

в) Какие антивирусные средства сертифицированы? отдаётся ли предпочтение какому-то конкретному разработчику антивирусов?

г) Какие продукты корпорации Microsoft получили сертификаты?

д) Какая из испытательных лабораторий является чемпионом по количеству обследованных объектов сертификации?

Шкала оценивания:

Оценка «отлично» за практическую работу выставляется, если оба задания выполнены не меньше, чем на 85%.

Оценка «хорошо» за практическую работу выставляется, если оба задания выполнены не меньше, чем на 71%.

Оценка «удовлетворительно» за практическую работу выставляется, если оба задания выполнены не меньше, чем на 61%.

Оценка «неудовлетворительно» за практическую работу выставляется, если любое из заданий выполнено меньше, чем на 61%.

Практическое занятие 2. Угрозы информации

Тематика: Угрозы информационной безопасности для АСОИ.

Цель работы: Ознакомиться с алгоритмами оценки риска информационной безопасности.

Краткие теоретические сведения:



Риск ИБ – потенциальная возможность использования определенной угрозой уязвимостей актива или группы активов для причинения вреда организации.

Уязвимость - слабость в системе защиты, делающая возможной реализацию угрозы.

Угроза ИБ - совокупность условий и факторов, которые могут стать причиной нарушений целостности, доступности, конфиденциальности информации.

Информационный актив – это материальный или нематериальный объект, который:
- является информацией или содержит информацию,
- служит для обработки, хранения или передачи информации,
- имеет ценность для организации.

Текст задания: Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология (ИТ). «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий» Ознакомьтесь с Приложениями C, D и E ГОСТа. Выберите три различных информационных актива организации (см. вариант). Из Приложения D ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов. Пользуясь ОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости. Пользуясь одним из методов (см. вариант) предложенных в ОСТа произведите оценку рисков информационной безопасности. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

Содержание отчета:
1. Титульный лист
2. Содержание
3. Задание
4. Обоснование выбора информационных активов организации
5. Оценка ценности информационных активов
6. Уязвимости системы защиты информации
7. Угрозы ИБ
8. Оценка рисков
9. Выводы

Варианты:

Номер варианта	Организация	Метод оценки риска (см. Приложение Е ГОСТа)
1	Отделение коммерческого банка	1
2	Поликлиника	2
3	Колледж	3
4	Офис страховой компании	4
5	Рекрутинговое агентство	1
6	Интернет-магазин	2
7	Центр оказания государственных услуг	3
8	Отделение полиции	4
9	Аудиторская компания	1
10	Дизайнерская фирма	2
11	Офис интернет-провайдера	3
12	Офис адвоката	4
13	Компания по разработке ПО для сторонних организаций	1
14	Агентство недвижимости	2
15	Туристическое агентство	3
16	Офис благотворительного фонда	4
17	Издательство	1
18	Консалтинговая фирма	2
19	Рекламное агентство	3
20	Отделение налоговой службы	4
21	Офис нотариуса	1
22	Бюро перевода (документов)	2
23	Научно проектное предприятие	3
24	Брачное агентство	4
25	Редакция газеты	1
26	Гостиница	2
27	Праздничное агентство	3
28	Городской архив	4
29	Диспетчерская служба такси	1
30	Железнодорожная касса	2

Шкала оценивания:

Оценка «отлично» за практическую работу выставляется, если работа выполнена полностью правильно и самостоятельно, а аспирант способен уверенно отвечать на вопросы преподавателя о проделанной работе;

Оценка «хорошо» выставляется, если работа выполнена в целом корректна, но имеются неточности в ответах на вопросе преподавателя или некоторые действия выполнены неоптимально;

Оценка «удовлетворительно» выставляется, когда работа не может быть завершена аспирантом самостоятельно, без помощи преподавателя.

Оценка «неудовлетворительно» выставляется, если работа не была выполнена.

Практическое занятие 3. Виды возможных нарушений безопасности информационной системы

Тематика: Классификация компьютерных преступлений.

Решение ситуационных задач по теме: «Информационные преступления в сфере компьютерной информации и меры защиты от них»

Алгоритм решения задачи включает в себя следующую последовательность действий:

1. Ответ на поставленный вопрос;
2. Законодательная (нормативная) база;
3. Обоснование решения со ссылкой на соответствующие законодательные предписания и фактические обстоятельства дела (фабулу).

В качестве образца предлагается решение задачи:

Студент заочного отделения Шатурин решил использовать компьютер из компьютерного класса университета для оформления контрольных и курсовых работ. Без разрешения деканата факультета он проник в класс и стал работать на компьютере. Из-за крайне поверхностных знаний и навы-ков работы на компьютере произошли сбои в работе машины, что привело в дальнейшем к отключению модема - одного из элементов компьютерной системы.

Подлежит ли уголовной ответственности Шатурин? Дайте анализ состава преступления, предусмотренного ст.274 УК РФ. Что понимается под информационно-телекоммуникационными сетями и оконечным оборудованием в смысле ст. 274 УК РФ? Какие виды оконечного оборудования возможны? Относится ли к оконечному оборудованию телефонный модем?

Фрагмент ответа: В деянии Шатурина можно усмотреть признаки состава преступления, предусмотренные ст. 274 УК РФ «нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей». законодательная база для решения задачи – ст. 274 УК РФ, примечания к ст. 272 УК РФ.

Родовым объектом данного преступления являются общественная безопасность и общественный порядок; видовым – отношения в сфере компьютерной безопасности. Непосредственный объект – это отношения, обеспечивающие правила эксплуатации хранения, обработки, передачи компьютерной информации и информационно-телекоммуникационных сетей.

Объективная сторона преступления сконструирована в качестве материального состава. Обязательные условия наступления уголовной ответственности – причинение крупного ущерба. В деянии Шатурина усматриваются отдельные признаки объективной стороны деяния, в частности, нарушения правил эксплуатации информационно-телекоммуникационных сетей. Он также обладает признаками субъекта данного преступления – вменяем и достиг 16 лет. Субъективная сторона преступления характеризуется виной как в форме умысла, так и неосторожности.

Однако, вопрос об уголовной ответственности Шатурина зависит от того, в каком размере был причинен ущерб его деянием, так как состав преступления является материальным. Согласно примечанию к ст. 22 УК РФ крупным ущербом в статьях данной главы признается ущерб сумма которого превышает один миллион рублей. Таким образом, Шатурин будет подлежать уголовной ответственности по ч. 1 ст. 274 УК РФ, если его деянием причинен ущерб на сумму свыше одного миллиона рублей.

Ситуации для самостоятельного решения:

1. Аспирант университета Хохлов, 23-ти лет, занимался исследовательской работой по компьютерной "вирусологии". Целью работы было выяснение масштаба глобальной сетевой инфраструктуры. В результате ошибки в механизме размножения вирусы, так называемые "сетевые черви", проникли в университетскую компьютерную сеть и уничтожили информацию, содержащуюся в компьютерах факультетов и подразделений. В результате этого были полностью уничтожены списки сотрудников университета, расчеты бухгалтерии по зарплате, повреждены материалы научно-исследовательской работы, в том числе "пропали" две кандидатские и одна докторская диссертации.

Решите вопрос о правомерности действий Хохлова. В чем заключается субъективная сторона преступлений в сфере компьютерной информации?

2. Левченко и другие граждане Российской Федерации вступили в сговор на похищение денежных средств в крупных размерах, принадлежащих "City Bank of America", расположенного в г. Нью-Йорке. Образовав устойчивую преступную группу, они в период с конца июня по сентябрь 2012 г., используя электронную компьютерную систему телекоммуникационной связи "Интернет" и преодолев при этом несколько рубежей многоконтурной защиты от несанкционированного доступа с помощью персонального компьютера стандартной конфигурации из офиса предприятия, находящегося в г. Санкт-Пе-тербурге, вводили в систему управления наличными фондами указанного банка ложные сведения. В результате этих операций было осуществлено не менее 40 переводов денежных средств на общую сумму 10 млн 700 тыс. 952 доллара США со счетов клиентов названного банка на счета лиц, входящих в состав преступной группы, проживающих в шести странах: США, Великобритании, Израиле, Швейцарии, ФРГ, России.

Дайте уголовно-правовую оценку действиям Левченко и других членов орга-низованной группы.

3. Оператор ЭВМ одного из государственных учреждений Утевский, используя многочисленные дискеты с информацией, получаемые от сотрудников других организаций, не всегда проверял их на наличие "вирусов", доверяясь заверениям поставщиков о том, что "вирусов" нет. В результате этого в компьютер Утевского, а затем и в компьютерную сеть учреждения попал комбинированный вирус, что привело к утрате информации, содержащей государственную тайну, и поставило под угрозу срыва запуск одного из космических объектов.

Дайте юридический анализ действий Утевского. Что следует понимать под тяжкими последствиями нарушении правил эксплуатации информационно-телекоммуникационных сетей?

4. Савченко осуществлял рассылку подложных электронных писем с целью завладения персональной информацией клиентов «Ситибанка». Рассылка представляла собой электронное письмо с сообщением о переводе 100 долларов США на личный счет клиента и содержала просьбу зайти в систему Интернет-бакинта «CitibankOnline» для подтверждения перевода. В случае следования по указанной ссылке происходило попадание на сайт, созданный Савченко, и очень похожий на стартовый экран «CitibankOnline». Десять человек ввели номер кредитной карты и пин-код для того, чтобы войти в систему. Воспользовавшись полученной таким образом информацией, Савченко совершил завладение денежными средствами Павлова и Костенко, находящимися в Ситибанке, в сумме 15 и 20 тысяч долларов соответственно.

Квалифицируйте содеянное Савченко.

5. Гуляшов, студент факультета вычислительной математики, организовывал сетевые атаки, заключающиеся в получении обманным путем доступа в сеть посредством имитации соединения. Таким образом он получил доступ к информации о счетах пользователей интернета и номерах некоторых кредитных карт и пин-кодов. Полученную информацию Гуляшов передавал Сорокиной за вознаграждение, которая использовала ее для хищения денежных средств.

Что такое фишинг, спуфинг и фарминг? Признаки какого явления усматриваются в деянии Гуляшова? (фишинга, спуфинга или фарминга). Квалифицируйте содеянное Гуляшовым и Сорокиной.

6. ГУВД Московской области было возбуждено уголовное дело по факту совершение неправомерного доступа в охраняемой законом компьютерной информации в кассовых аппаратах одного из индивидуальных предпринимателей г.Павловский Посад Лебедева. Следствие квалифицировало действие Лебедева по ч.2 ст.272 УК РФ, т.е. изменение информации в контрольно-кассовых аппаратах, при которых записанная в них сумма выручки за смену искусственно занижалась. Информация, содержащаяся в контрольно-кассовых аппаратах, признана следствием разновидностью компьютерной информации. Адвокат Лебедева настаивал на изменении квалификации.

Дайте юридическую оценку содеянного. Что следует понимать под компьтерной информацией?

7. Программист Мохов был признан судом виновным в деяниях, предусмотренных ч.3. ст.273 УК РФ и ч.1 ст.165 УК РФ. С ноября по апрель Мохов рассылал клиентам пяти городским Интернет-провайдерам «Троянские» программы и получал логины с паролями, которыми пользовался для доступа в Интернет. Всего было доказано наличие 12 подобных эпизодов, в течение которых Мохов пользовался услугами Интернета без оплаты.

Правильно ли суд квалифицировал содеянное? В каких случаях возможна квалификация по совокупности деяний, предусмотренных ст.272-274 УК РФ с иными составами преступлений? Что следует понимать под тяжкими последствиями, применительно к составу преступления, предусмотренного ст.273 УК РФ?

8. Панченко и Будин, работали в компьютерной форме, распространяли «Троянские» программы и получали доступ к паролям пользователей компьютеров. Следствие квалифицировало распространение вирусных программ по ч.1 ст.273 УК РФ, а доступ к чужим паролям по ч.1. ст.272 УК РФ.

Дайте анализ объективных и субъективных признаков данных составов преступлений. Решите вопрос о квалификации содеянного.

Шкала оценивания:

Оценка «отлично» за практическую работу выставляется, если все ситуации разобраны полностью правильно и самостоятельно, а аспирант способен уверенно отвечать на вопросы преподавателя о проделанной работе;

Оценка «хорошо» выставляется, если работа выполнена в целом корректна, но имеются неточности в ответах на вопросе преподавателя;

Оценка «удовлетворительно» выставляется, когда работа не может быть завершена аспирантом самостоятельно, без помощи преподавателя.

Оценка «неудовлетворительно» выставляется, если работа не была выполнена.

Практическое занятие 4. Информационная безопасность информационных систем

Тематика: Криптографические способы защиты информации.

Текст задания №1: Выполните следующие задания:

1. Вычислить символ Лежандра (5/160465489).
2. Найти индекс совпадения Фридмана для предложенного текста преподаваетелем.
3. Зашифровать сообщение с помощью двойного шифра Хилла, использующего матрицы размеров 2 и 3.
4. Написать программу выработки имитовставки.
5. Написать программу зашифрования с помощью шифра Плейфейра.
6. Прочитать предложенное преподавателем сообщение, зашифрованное шифром Виженера.

Текст задания №2: Используя возможности поисковых систем, найдите ответы на следующие вопросы:

1. В чем заключаются достоинства и недостатки систем поточного шифрования по сравнению с блочными?
2. Как определяются энтропия и избыточность языка?
3. Сравнить достоинства и недостатки шифров DES, AES и ГОСТ-28147-89
4. Для каких целей применяются хеш-функции? Как строятся криптографические хеш-функции?
5. Описать возможные схемы получения псевдослучайной последовательности.

Шкала оценивания:

Оценка «отлично» за практическую работу выставляется, если представлено полное и правильное решение всех задач из текста задания №2 и ответы на вопросы из текста задания №1;

Оценка «хорошо» выставляется, если представлено полное и правильное решение всех задач из текста задания №2, но в ответах на вопросы из текста задания №1 присутствует небольшое количество ошибок и/или неточностей (полностью правильный и полный ответ дан не менее, чем на 60% вопросов);

Оценка «удовлетворительно» выставляется, когда аспирантом было выполнено 60% заданий из текста задания №2 и дан полный и правильный ответ на 60% вопросов из текста задания №1.

Оценка «неудовлетворительно» выставляется, если работа выполнена менее, чем на 60% по любому из двух текстов заданий.

Практическое занятие 5. Методы и средства защиты компьютерной информации

Тематика: Антивирусное ПО.

Текст задания №1: На сайте ФСТЭК России представлен Государственный реестр сертифицированных средств защиты информации: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00

Найдите в нем названия антивирусных программ от двух различных производителей и представьте в качестве ответа на данное задание.

Текст задания №2: Используя возможности поисковых систем, найдите ответы на следующие вопросы:

1. Что такое EICAR-Test-File?
2. Существует ли в мире и в РФ уголовная ответственность за создание и распространение компьютерных вирусов?

3. Что такое полиморфный вирус? Почему этот тип вирусов считается наиболее опасным?
4. Опишите схему функционирования загрузочно-файловых вирусов.
5. Каковы отличия вирусов-репликаторов, стелс-вирусов, мутантов и «троянских» программ?
6. Как используются утилиты скрытого администрирования и их деструктивные возможности?
7. В чем состоят особенности CRC-сканеров?
8. В чем состоят особенности эвристических сканеров?

Шкала оценивания:

Оценка «отлично» за практическую работу выставляется, если на все вопросы дан полный, обоснованный и правильный ответ;

Оценка «хорошо» выставляется, если аспирант ошибся при ответе на один вопрос;

Оценка «удовлетворительно» выставляется, если аспирант ошибся при ответе на два вопроса.

Оценка «неудовлетворительно» выставляется, если аспирант допустил больше двух ошибок.

Практическое занятие 6. Заключительное занятие. Подведение и анализ промежуточных результатов освоения дисциплины

При подготовке материалов для заключительного практического занятия, преподаватель учитывает недостаточную степень развития навыков аспирантов, определенную в ходе практических занятий и при оценке самостоятельной работы. На практическом занятии обсуждаются итоги проведения занятий по дисциплине, проверяется полнота и качество собранного аспирантом портфолио материалов и результатов выполнения заданий по дисциплине. Обсуждаются вопросы для подготовки к сдаче кандидатского экзамена по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность. Оцениваются индивидуальные достижения, полученные аспирантов в ходе внеурочной работы (сертификаты олимпиад, конкурсов, грантов, написание тезисов/статей в сборники конференций различного уровня).

3. Методические указания по выполнению других видов самостоятельной работы по дисциплине

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К СДАЧЕ КАНДИДАТСКОГО ЭКЗАМЕНА ПО СПЕЦИАЛЬНОСТИ

1. Нормативно-правовые документы в области защиты и информации и информационной безопасности;
2. Требования к защите информации в автоматизированных системах управления;
3. Сущность проблемы обеспечения информационной безопасности предприятий с развитой инфраструктурой;
4. Организационно-правовые меры обеспечения сохранности информации в автоматизированных системах;
5. Основные задачи обеспечения безопасности информации в автоматизированных системах;
6. Защищенная информационная система и система защиты информации;
7. Принципы построения систем комплексной защиты информации в автоматизированных

системах управления и в информационно-вычислительных сетях;
8. Программно-технические методы и средства защиты информации;
9. Программно-аппаратные методы и средства ограничения доступа к ресурсам вычислительных сетей;
10. Мандатная модель доступа: сущность и особенности практической реализации;
11. Ролевая модель доступа: сущность и особенности практической реализации;
12. Типы несанкционированного доступа и условия работы средств защиты;
13. Способы защиты от локального несанкционированного доступа и от удаленного несанкционированного доступа (НСД);
14. Контроль целостности и системные вопросы защиты программ и данных.
15. Сущность системного подхода к проектированию программно-аппаратных средств защиты информации в автоматизированных системах управления и в информационно-вычислительных сетях;
16. Классификация угроз информации;
17. Математические модели угроз и процессов комплексной защиты информации.
18. Требования к математическим моделям, используемым в задачах формализованного анализа систем защиты информации;
19. Постановка задачи синтеза оптимального механизма комплексной защиты информации;
20. Методология анализа систем комплексной защиты информации. Аналитические, вероятностные и имитационные модели процессов защиты информации.
21. Методы идентификации и проверки подлинности пользователей компьютерных систем;
22. Проблема аутентификации данных и электронная цифровая подпись;
23. Режим функционирования межсетевых экранов и их основные компоненты;
24. Основные схемы сетевой защиты на базе межсетевых экранов;
25. Применение межсетевых экранов для организации виртуальных корпоративных сетей;
26. Сравнительный анализ *существующих аппаратно-программных* средств криптографической защиты компьютерной информации серии КРИПТОН.
27. Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов).
28. Понятие разрушающего программного воздействия; модели взаимодействия прикладной программы и программной закладки;
29. Компьютерные вирусы как особый класс разрушающих программных воздействий; защита от разрушающих программных воздействий; понятие изолированной программной среды.
30. Особенности комплексной защиты процесса обработки информации в компьютерных системах на основе стохастической интеллектуальной информационной технологии (ИИТ).
31. Метод верификации программного обеспечения для контроля корректности, реализуемости и защиты от закладок;
32. Метод защиты от НСД и разрушающих программных воздействий процесса хранения, обработки информации;
33. Анализ рисков информационной безопасности в автоматизированных системах и информационно-вычислительных сетях;
34. Проблема управления информационной безопасностью в автоматизированных системах управления и в распределённых вычислительных сетях.
35. Адаптация механизмов защиты информации в автоматизированных системах управления.
36. Внешний аудит информационной безопасности организации: сущность, задачи и этапы;
37. Задача управления рисками информационной безопасности (на примере АСУ);
38. Внутренний аудит информационной безопасности организации: сущность, задачи и этапы;
39. Актуальность темы и научная новизна диссертационного исследования.

40. Характеристика предметной области исследования;
41. Гипотеза исследования; Методологические основы диссертационного исследования.
42. Характеристика объекта диссертационного исследования;
43. Научная задача и цель диссертационного исследования.

По представленным вопросам предполагается выполнение аспирантом конспектов или повторение материала с использованием конспектов лекций.

4. Примеры контрольных заданий (оценочных средств), используемых при текущем контроле успеваемости и промежуточной аттестации по дисциплине

Демоверсия итогового тестирования:

1. При какой атаке цель выводится из строя путем отправки ей огромного количества запросов от множества других систем?

а) ping sweep;
б) фальсификация;
в) DoS-атака;
г) DDoS-атака (правильный ответ);

2. Какие из нижеуказанных мер эффективны в борьбе с киберпреступниками?

а) Замена операционных систем;
б) Внедрение систем раннего оповещения (правильный ответ);
в) Обмен результатами анализа киберугроз (правильный ответ);
г) Наем хакеров;
д) Отключение сети;

3. При какой атаке компьютер выводится из строя за счет переполнения памяти или перегрузки центрального процессора?

а) DDoS-атака;
б) APT;
в) исчерпание ресурсов;
г) алгоритмическая атака (правильный ответ);

4. Назовите три принципа проектирования, благодаря которым достигается высокая доступность.

а) исключение единых точек отказа (правильный ответ);
б) обеспечение конфиденциальности;
в) выявление отказов по мере их возникновения (правильный ответ);
г) проверка данных на согласованность;
д) шифрование;
е) обеспечение надежного механизма переключения на резервные ресурсы (правильный ответ);

5. Как называется механизм передачи информации с одного устройства на другое с помощью съемного носителя?

а) беспроводная связь;
б) перенос данных вручную (правильный ответ);
в) инфракрасный порт;
г) локальная сеть;
д) проводная связь;
е) пакет;

6. Как называется защищенная виртуальная сеть, существующая внутри общедоступной сети?

а) IDS;
б) IPS;
в) Межсетевой экран;
г) MPLS;
д) NAC;
е) VPN (правильный ответ);

7. Назовите две наиболее распространенные хеш-функции.

а) ECC;
б) Blowfish;
в) SHA (правильный ответ);
г) RC4;
д) MD5 (правильный ответ);
е) RSA;

8. Какой механизм можно применить в организации в качестве средства защиты от непреднамеренного изменения информации авторизованными пользователями?

а) хэширование;
б) резервное копирование;
в) шифрование;
г) управление версиями (правильный ответ);
д) SHA-1.

Автор(ы)-составитель(и): *Привалов А.Н.*, профессор кафедры математики, информатики и методики обучения, доктор технических наук, профессор