МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования
«Самарский государственный социально-педагогический университет»

Кафедра информационно-коммуникационных технологий в образовании

Утверждаю
Проректор по учебно-методической
работе и качеству образования
_____ Н.Н. Кислова

Семенова Н.Н., Тараканова Е.Н.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения промежуточной аттестации по дисциплине
«Методы и средства защиты информации»
Направление подготовки 44.03.05 Педагогическое образование
(с двумя профилями подготовки)

Направленность (профиль): «Начальное образование» и «Организация внеурочной деятельности»

Квалификация выпускника

Бакалавр

Рассмотрено
Протокол от № 1 от 25.08.2020
Заседания кафедры
информационно-коммуникационных
технологий в образовании

Одобрено
Начальник Управления
образовательных программ
_____ Н.А. Доманина

Самара 2020

Пояснительная записка

Фонд оценочных средств (далее – ФОС) для промежуточной аттестации по дисциплине «Детская литература и литературоведение» разработан в соответствии с Федеральным государственным образовательным стандартом высшего образования – бакалавриат по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки), утвержденным приказом Министерства образования и науки Российской Федерации от 22 февраля 2018 г. № 125, основной профессиональной образовательной программой высшего образования «Начальное образование» и «Организация внеурочной деятельности» с учетом требований профессионального стандарта «Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель)», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 18 октября 2013 г. № 544н (зарегистрирован Министерством юстиции Российской Федерации 6 декабря 2013 г., регистрационный № 30550), с изменениями, внесенными приказами Министерства труда и социальной защиты Российской Федерации от 25 декабря 2014 г. № 1115н (зарегистрирован Министерством юстиции Российской Федерации 19 февраля 2015 г., регистрационный № 36091) и от 5 августа 2016 г. № 422н (зарегистрирован Министерством юстиции Российской Федерации 23 августа 2016 г., регистрационный № 43326).

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Цель изучения дисциплины:

обеспечить технологическую и правовую готовность к созданию безопасной информационно-образовательной среды и использованию различных методов и средств защиты информации; профессиональную готовность к реализации образовательных внеурочной деятельности в соответствии с требованиями образовательных стандартов, формированию у обучающихся навыков защиты информации и безопасного использования программных средств при работе с информационными ресурсами.

Задачи изучения дисциплины:

в области педагогической деятельности:

- готовность к формированию у обучающихся знаний в области теоретических основ информационной безопасности, ознакомлению с моделями возможных угроз безопасности информации и современными методами защиты информации и программного обеспечения,

в области проектной деятельности

- освоение правовых основ и способов проектирования профессиональной сетевой среды на основе современных методов и средств защиты информации;

в области исследовательской деятельности:

- постановка и решения исследовательских задач в области современной теории и практике защиты информации.

Область профессиональной деятельности:

01 Образование и наука (в сфере начального общего, основного общего, среднего общего образования, профессионального обучения, профессионального образования, дополнительного образования; в сфере научных исследовании)

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Цикл (раздел) ОП:	Б1.О.11
2.1	**Требования к предварительной подготовке обучающегося:**
Содержание дисциплины базируется на материале:	
Основы информационно-коммуникационных технологий	
Компьютерные сети и Web-программирование	
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
Проектирование программ внеурочной деятельности	
Медиаобразование во внеурочной деятельности	

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

УК-8. Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов

УК-8.1. Обеспечивает безопасные и/или комфортные условия труда на рабочем месте; выявляет и устраняет проблемы, связанные с нарушениями техники безопасности на рабочем месте

Знает:
методы и устройства обеспечения безопасности информации в профессиональной сетевой среде;
нормативно-правовую и законодательную базу, технологические стратегии по обеспечению информационной безопасности при взаимодействии в компьютерных сетях;
Умеет:
выработать политику и реализовать на практике механизмы разграничения прав доступа к массивам информации в информационно-образовательной среде (персональной, коллективной, образовательного учреждения);
Владеет:
навыками применения методов и средств организационно-правовой защиты информации в информационно-образовательной среде (персональной, коллективной, образовательного учреждения);

ОПК-8. Способен осуществлять педагогическую деятельность на основе специальных научных знаний

ОПК-8.1. Знает: историю, теорию, закономерности и принципы построения и функционирования образовательного процесса, роль и место образования в жизни человека и общества, современное состояние научной области, соответствующей преподаваемому предмету; прикладное значение науки; специфические методы научного познания в объеме, обеспечивающем преподавание учебных предметов

Знает:
основные виды угроз информационной безопасности;
понятие и виды компьютерных вирусов, их разрушительные действия; методы защиты от компьютерных вирусов;
актуальные проблемы в области информационной безопасности для проведения учебно-исследовательской деятельности обучающихся;
роль и место, приемы использования содержания обучения в школьном курсе информатики, во внеурочной и учебно-исследовательской деятельности по предмету.

ОПК-9. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности

ОПК-9.1. Знает принципы функционирования, основные характеристики и возможности аппаратных и программных средств современных информационных технологий; тенденции развития сквозных цифровых технологий и профессионально значимые решения на их основе; этические и правовые нормы при работе с

Знает:
основные виды угроз информационной безопасности;
алгоритмы и методы, программные средства и устройства обеспечения безопасности информации в профессиональной сетевой среде;

ОПК-9.2. Умеет применять современные информационно-коммуникационные технологии для решения профессиональных задач с учетом специфики предметной области; осуществлять выбор необходимых для осуществления профессиональной деятельности аппаратных и программных средств, мобильных приложений, средств сетевой коммуникации на основе стандартов и норм, принятых в профессиональной среде и с учетом требований информационной безопасности

Умеет
осуществлять выбор необходимых для защиты информации аппаратных и программных средств, средств сетевой коммуникации на основе стандартов и норм, принятых в профессиональной среде и с учетом требований информационной безопасности

ОПК-9.3. Владеет методами анализа эффективности использования профессионально ориентированных аппаратных и программных средств современных информационных технологий, мобильных приложений, сервисов и ресурсов сети Интернет для сопровождения профессиональной деятельности; технологиями решения актуальных профессиональных задач на их основе

Владеет:
методами анализа эффективности использования аппаратных и программных средств защиты информации и беспечения безопасности ее использования, в том числе в процессе сетевой коммуникации

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Интеракт.
	Раздел 1. Методы и средства обеспечения безопасности информации в профессиональной сетевой среде	8	48	
1.1	Основные понятия информационной безопасности: аппаратные и программные средства обеспечения безопасности /Лек/	8	4	

1.2	Угрозы безопасности информации, их классификация /Лек/	8	2	
1.3	Криптографические методы обеспечения информационной безопасности /Лек/	8	4	
1.4	Основные понятия информационной безопасности: аппаратные и программные средства обеспечения безопасности /Пр/	8	4	2
1.5	Угрозы безопасности информации, их классификация /Пр/	8	4	
1.6	Основные понятия информационной безопасности: аппаратные и программные средства обеспечения безопасности /Ср/	8	8	
1.7	Нормативно-правовое обеспечение информационной безопасности /Ср/	8	6	
1.8	Угрозы безопасности информации /Ср/	8	8	
1.9	Классификация угроз бнзопасности информации /Ср/	8	6	
	Раздел 2. Защита информации в информационно-образовательной среде	8	60	
2.1	Современные программные и аппаратные методы защиты информации. Политика безопасности и механизмы разграничения прав доступа к массивам информации в информационно-образовательной среде. /Лек/	8	4	
2.2	Понятие и классификация «вредоносных программ». Защита от «компьютерных вирусов». /Лек/	8	2	2
2.3	Современные программные и аппаратные методы защиты информации. Политика безопасности и механизмы разграничения прав доступа к массивам информации в информационно-образовательной среде /Пр/	8	4	
2.4	Понятие и классификация «вредоносных программ» /Пр/	8	4	2
2.5	Защита от «компьютерных вирусов» /Пр/	8	4	2
2.6	Программные и аппаратные методы защиты информации (персональной, коллективной, образовательного учреждения) /Пр/	8	6	
2.7	Современные программные и аппаратные методы защиты информации. Политика безопасности и механизмы разграничения прав доступа к массивам информации в информационно-образовательной среде /Ср/	8	8	
2.8	Понятие и классификация «вредоносных программ» /Ср/	8	8	
2.9	Защита от «компьютерных вирусов» /Ср/	8	8	
2.10	Программные и аппаратные методы защиты информации (персональной, коллективной, образовательного учреждения)/Ср/	8	14	

5. Оценочные и методические материалы по дисциплине (модулю)

5.1. Содержание аудиторной работы по дисциплине (модулю)

Раздел 1. Введение в информационную безопасность

Лекция. Основные понятия информационной безопасности: аппаратные и программные средства обеспечения безопасности (4 ч.)

Вопросы:

- Понятие информационной безопасности и защищенной системы.
- Актуальность защиты информационных систем и телекоммуникаций.
- Информационная безопасность в условиях функционирования глобальных сетей.
- Нормативно-правовые и законодательные акты в области информационной безопасности.

Литература:

- Аверченков В. И. , Рытов М. Ю. , Кондрашин Г. В. ,Рудановский М. В. Системы защиты информации в ведущих зарубежных странах: учебное пособие для вузов. М.: ФЛИНТА, 2011. – 224 с. [Электронный ресурс] - Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=93351.

- Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации: учебное пособие. М.-Берлин: Директ-Медиа, 2015. – 253 с. [Электронный ресурс] - Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=276557.
- Прохорова О. В. Информационная безопасность и защита информации: учебник. Самара: СГАСУ, 2014. – 113 с. [Электронный ресурс] - Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=438331.
- Федеральный закон " О персональных данных (с изменениями на 30 декабря 2020 года)" [Электронный ресурс] - Режим доступа: http://docs.cntd.ru/document/901990046
- Федеральный закон " Об информации, информационных технологиях и о защите информации (с изменениями на 29 декабря 2020 года)". [Электронный ресурс] - Режим доступа: http://docs.cntd.ru/document/901990051.
- Федеральный закон "Об электронной подписи (с изменениями на 23 июня 2020 года) (редакция, действующая с 1 января 2021 года)». [Электронный ресурс] - Режим доступа: http://docs.cntd.ru/document/902271495

Лекция. Угрозы безопасности информации, их классификация (2 ч.)
Вопросы:

- Понятие угрозы. Виды противников или «нарушителей». Виды возможных нарушений информационной системы.
- Анализ угроз информационной безопасности.
- Классификация видов угроз информационной безопасности по различным признакам (по природе возникновения, степени преднамеренности и т.п.).
- Свойства информации: конфиденциальность, доступность, целостность.
- Угроза раскрытия параметров системы, угроза нарушения конфиденциальности, угроза нарушения целостности, угроза отказа служб.
- Примеры реализации угроз информационной безопасности.
- Причины, виды и каналы утечки конфиденциальной информации.
- Методы и средства несанкционированного доступа к компьютерным ресурсам и программным средствам.

Литература:

- Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации: учебное пособие. М.-Берлин: Директ-Медиа, 2015. – 253 с. [Электронный ресурс] - Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=276557.
- Прохорова О. В. Информационная безопасность и защита информации: учебник. Самара: СГАСУ, 2014. – 113 с. [Электронный ресурс] - Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=438331.

Лекция. Аппаратные и программные методы защиты информации (персональной, коллективной, образовательного учреждения)(4 ч.)
Вопросы:

- Методы криптографии. Средства криптографической защиты информации (СКЗИ).
- Криптографические преобразования. Шифрование и дешифрование информации.
- Использование криптографических средств для решения задач идентификации и аутентификации.
- Электронная подпись (ЭП), принципы ее формирования и использования.
- Подтверждение подлинности объектов и субъектов информационной системы.
- Контроль целостности информации. Хэш-функции, принципы использования хэш-функций для обеспечения целостности данных.
- Лицензирование и сертификация в области информационной безопасности.
- Критерии безопасности компьютерных систем.

Литература:

- Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации: учебное пособие. М.-Берлин: Директ-Медиа, 2015. – 253 с. [Электронный ресурс] - Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=276557.
- 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
- Прохорова О. В. Информационная безопасность и защита информации: учебник. Самара: СГАСУ, 2014. – 113 с. [Электронный ресурс] - Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=438331.

Практическое занятие. Основные понятия информационной безопасности (4 ч.)
Вопросы и задания:

- Понятие информационной безопасности.
- Нормативно-правовые и законодательные акты России в области информационной безопасности.
- Справочные правовые системы.
- Практическая работа по теме «Политики государств в области информационной безопасности»

Литература:

- Аверченков В. И. , Рытов М. Ю. , Кондрашин Г. В. ,Рудановский М. В. Системы защиты информации в ведущих зарубежных странах: учебное пособие для вузов. М.: ФЛИНТА, 2011. – 224 с. [Электронный ресурс] - Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=93351.
- Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации: учебное пособие. М.-Берлин: Директ-Медиа, 2015. – 253 с. [Электронный ресурс] - Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=276557.
- Прохорова О. В. Информационная безопасность и защита информации: учебник. Самара: СГАСУ, 2014. – 113 с. [Электронный ресурс] - Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=438331.
- Федеральный закон " О персональных данных (с изменениями на 30 декабря 2020 года)" [Электронный ресурс] - Режим доступа: http://docs.cntd.ru/document/901990046
- Федеральный закон " Об информации, информационных технологиях и о защите информации (с изменениями на 29 декабря 2020 года)". [Электронный ресурс] - Режим доступа: http://docs.cntd.ru/document/901990051.
- Федеральный закон "Об электронной подписи (с изменениями на 23 июня 2020 года) (редакция, действующая с 1 января 2021 года)». [Электронный ресурс] - Режим доступа: http://docs.cntd.ru/document/902271495

Практическое занятие. Угрозы безопасности информации, их классификация (4 ч.)
Вопросы и задания:

- Основные виды угроз информационной безопасности.
- Последствия нарушения авторских прав на программное обеспечение и роль соответствующих правоохранительных организаций.
- Практическая работа по теме «Угрозы безопасности информации

Литература:

- Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации: учебное пособие. М.-Берлин: Директ-Медиа, 2015. – 253 с. [Электронный ресурс] - Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=276557.

Прохорова О. В. Информационная безопасность и защита информации: учебник. Самара: СГАСУ, 2014. – 113 с. [Электронный ресурс] - Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=438331

Раздел 2. Защита информации в информационно-образовательной среде

Лекция. Современные программные и аппаратные методы защиты информации. Политика безопасности и механизмы разграничения прав доступа к массивам информации в информационно-образовательной среде. (4 ч.)
Вопросы:

- Основные задачи обеспечения защиты информации.
- Основные методы и средства защиты информационных систем.
- Классификация способов и средств комплексной защиты информации.
- Понятие политики безопасности информационных систем.
- Разработка и реализация политики безопасности.
- Идентификация и аутентификация. Парольные схемы аутентификации. Токены, смарт-карты, их применение. Использование биометрических данных при аутентификации пользователей.
- Сервисы управления доступом. Механизмы доступа данных в операционных системах, системах управления базами данных. Ролевая модель управления доступом.
- Протоколирование и аудит. Задачи и функции аудита. Структура журналов аудита. Активный аудит, методы активного аудита.

Литература:

- Дистанционный курс «Основы информационной безопасности при работе на компьютере» [Электронный ресурс] - Режим доступа: http://www.intuit.ru/studies/courses/680/536/info
- Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации: учебное пособие. М.-Берлин: Директ-Медиа, 2015. – 253 с. [Электронный ресурс] - Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=276557.
- Прохорова О. В. Информационная безопасность и защита информации: учебник. Самара: СГАСУ, 2014. – 113 с. [Электронный ресурс] - Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=438331.

Лекция. Понятие и классификация «вредоносных программ». Защита от «компьютерных вирусов». (2 ч.)
Вопросы:

- Понятие и основные этапы жизненного цикла «вредоносных программ»; факторы, влияющие на их распространение.
- Объекты внедрения, функции и режимы функционирования вирусов.
- Схемы заражения файлов и загрузчиков. Способы маскировки, используемые вирусами.
- Классификация «вредоносных программ».
- Общая организация защиты от «компьютерных вирусов». Защита от деструктивных действий и размножения вирусов с использованием средств аппаратного и программного контроля.
- Антивирусное программное обеспечение.

- Защита системы электронной почты. Спам, борьба со спамом.
- Технология гарантированного восстановление вычислительной системы после заражения «компьютерными вирусами».

Литература:

- Дистанционный курс «Обеспечение информационной безопасности с помощью антивируса Касперского» [Электронный ресурс] - Режим доступа: http://www.intuit.ru/studies/courses/559/415/info
- Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации: учебное пособие. М.-Берлин: Директ-Медиа, 2015. – 253 с. [Электронный ресурс] - Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=276557.
- Прохорова О. В. Информационная безопасность и защита информации: учебник. Самара: СГАСУ, 2014. – 113 с. [Электронный ресурс] - Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=438331.

Практическое занятие. Программные и аппаратные методы защиты информации. Политика безопасности и механизмы разграничения прав доступа к массивам информации в информационно-образовательной среде (4 ч.)

Вопросы и задания:

- Парольные методы защиты информации. Программные средства для хранения паролей.
- Основные методы и средства защиты информационных систем. Классификация способов и средств комплексной защиты информации.
- Защита Интернет-подключений, функции и назначение межсетевых экранов (брандмауэров).
- Выполнение двух лабораторно-практических работ «Особенности защиты информации в локальных и глобальных компьютерных сетях».

Литература:

- Дистанционный курс «Основы информационной безопасности при работе на компьютере» [Электронный ресурс] - Режим доступа: http://www.intuit.ru/studies/courses/680/536/info
- Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации: учебное пособие. М.-Берлин: Директ-Медиа, 2015. – 253 с. [Электронный ресурс] - Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=276557.
- Прохорова О. В. Информационная безопасность и защита информации: учебник. Самара: СГАСУ, 2014. – 113 с. [Электронный ресурс] - Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=438331.

Практическое занятие. Понятие и классификация «вредоносных программ». (4 ч.)

Вопросы и задания:

- Классификация «вредоносных программ». Общая организация защиты от «вредоносных программ». Защита от деструктивных действий и размножения вирусов с использованием средств аппаратного и программного контроля.
- Антивирусное программное обеспечение.
- Выполнение лабораторно-практической работы «Компьютерные вирусы».

Литература:

- Дистанционный курс «Обеспечение информационной безопасности с помощью антивируса Касперского» [Электронный ресурс] - Режим доступа: http://www.intuit.ru/studies/courses/559/415/info
- Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации: учебное пособие. М.-Берлин: Директ-Медиа, 2015. – 253 с. [Электронный ресурс] - Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=276557.

Прохорова О. В. Информационная безопасность и защита информации: учебник. Самара: СГАСУ, 2014. – 113 с. [Электронный ресурс] - Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=438331

Практическое занятие. Защита от «компьютерных вирусов». (4 ч.)

Вопросы и задания:

- Классификация «компьютерных вирусов». Общая организация защиты от «компьютерных вирусов». Защита от деструктивных действий и размножения вирусов с использованием средств аппаратного и программного контроля.
- Антивирусное программное обеспечение.
- Выполнение лабораторно-практической работы «Антивирусные средства защиты».

Литература:

- Дистанционный курс «Обеспечение информационной безопасности с помощью антивируса Касперского» [Электронный ресурс] - Режим доступа: http://www.intuit.ru/studies/courses/559/415/info
- Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации: учебное пособие. М.-Берлин: Директ-Медиа, 2015. – 253 с. [Электронный ресурс] - Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=276557.

Прохорова О. В. Информационная безопасность и защита информации: учебник. Самара: СГАСУ, 2014. – 113 с. [Электронный ресурс] - Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=438331

Практическое занятие. Криптографические методы обеспечения информационной безопасности. (6 ч.)

Вопросы и задания:

- Средства криптографической защиты информации (СКЗИ). Криптографические преобразования. Шифрование и дешифрование информации. Использование криптографических средств для решения задач идентификации и аутентификации.
- Выполнение трех лабораторно-практических работ «Базовые принципы криптографической защиты информации».

Литература:

- Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации: учебное пособие. М.-Берлин: Директ-Медиа, 2015. – 253 с. [Электронный ресурс] - Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=276557.
- 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
- Прохорова О. В. Информационная безопасность и защита информации: учебник. Самара: СГАСУ, 2014. – 113 с. [Электронный ресурс] - Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=438331.

5.2. Содержание самостоятельной работы по дисциплине (модулю)

Содержание обязательной самостоятельной работы по дисциплине

№ п/п	Темы дисциплины	Содержание самостоятельной работы студентов	Продукты деятельности
1.	Основные понятия информационной безопасности. Нормативно-правовое обеспечение информационной безопасности	Домашняя работа поисково-аналитического характера по теме «Основные понятия информационной безопасности. Нормативно-правовое обеспечение информационной безопасности».	Глог по теме «Информационная безопасность в РФ» (с помощью сервиса glogster.com)
2.	Угрозы безопасности информации, их классификация	Самостоятельное структурирование учебного материала по существующим угрозам безопасности информации.	Составление Google-таблицы с: o классификаций угроз безопасности информации по различным признакам, o классификацией компьютерных преступлений, o и др.
3.	Понятие и классификация «вредоносных программ». Защита от «компьютерных вирусов».	Классификация «вредоносных программ» и антивирусных программных средств.	Составление ментальной карты (кластера, фишбоун и др.) по теме.
4.	Криптографические методы информационной безопасности	Самостоятельное изучение законодательных и нормативно-правовых актов в сфере электронной подписи, цифровых сертификатов, лицензирования деятельности удостоверяющих центров.	Коллективный Google-документ, отражающий состояние нормативно-правовой базы по изучаемой теме в РФ.
5.	Современные пограммные и аппаратные методы защиты информации. Политика безопасности и механизмы разграничения прав доступа к массивам информации в информационно-образовательной среде.	Упорядочивание, приведение в единую систему знаний о современных методах защиты информации. Выявление причинно-следственных связей.	Создание Google-сайта по выбранной теме.

Содержание самостоятельной работы по дисциплине на выбор студента

№ п/п	Темы дисциплины	Содержание самостоятельной работы студентов	Продукты деятельности
1.	Основные понятия информационной	Домашняя работа поисково-аналитического характера по теме	Составление словаря терминов в области информационной

	безопасности. Нормативно-правовое обеспечение информационной безопасности	«Информационная безопасность: концептуальные, практические, системотехнические, экономические, правовые, криптологические, математические, психологические, физические, программные и информационные основы».	безопасности и перечня нормативных документов по информационной безопасности (Google-документ).
2.	Программные и аппаратные методы обеспечения безопасности информации, их классификация	Подготовка мультимедийной презентации об источниках угроз информационной безопасности и способах совершения компьютерных преступлений	Мультимедийная презентация. Публичное выступление
3.	Понятие и классификация «компьютерных вирусов». Защита от «компьютерных вирусов».	Подготовка мультимедийной презентации о классификации и схемах функционирования компьютерных вирусов или антивирусных программных средствах	Презентация MS Power Point
4.	Современные пограммные и аппаратные методы защиты информации. Политика безопасности и механизмы разграничения прав доступа к массивам информации в информационно-образовательной среде.	Эссе рефлексивного характера по одной из проблем курса: «Как я лично понимаю термин *информационная безопасность*?», «Защита информации: основные подходы», «Использование методов социальной инженерии для получения доступа к информации», «Особенности парольной защиты информации»	Публикация в Google-группе
5.	Криптографические методы информационной безопасности	Создание индивидуального блога с обзором правовых и технологических аспектов электронной цифровой подписи и электронных сертификатов.	Блог
6.	Все темы	Составление аннотированного каталога Интернет-ресурсов по теме (по выбору студента)	Аннотированный каталог (Google-документ)

5.3.Образовательные технологии

При организации изучения дисциплины будут использованы следующие образовательные технологии: информационно-коммуникационные технологии, технология организации самостоятельной работы, технология рефлексивного обучения, технология модульного обучения, технология игрового обучения, технологии групповой дискуссии, интерактивные технологии, технология проблемного обучения, технология организации учебно-исследовательской деятельности, технология проектного обучения, технология развития критического мышления.

5.4. Текущий контроль, промежуточный контроль и промежуточная аттестация

Балльно-рейтинговая карта дисциплины оформлена как приложение к рабочей программе дисциплины.
Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине оформлен отдельным документом.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы,	Заглавие, ссылка на электронную библиотечную систему	Издательство, год
Л1.1	Аверченков В. И. , Рытов М. Ю. , Кондрашин Г. В. , Рудановский М. В.	Системы защиты информации в ведущих зарубежных странах: учебное пособие для вузов. http://biblioclub.ru/index.php?page=book_view_red&book_id=93351	М.: ФЛИНТА, 2011
Л1.2	Загинайлов Ю. Н.	Теория информационной безопасности и методология защиты информации: учебное пособие. http://biblioclub.ru/index.php?page=book_view_red&book_id=276557	М.-Берлин: Директ-Медиа, 2015

Л1.3	Прохорова О. В.	Информационная безопасность и защита информации: учебник. http://biblioclub.ru/index.php?page=book_view_red&book_id=438331	Самара: СГАСУ, 2014.
6.1.2. Дополнительная литература			
	Авторы,	Заглавие, ссылка на электронную библиотечную систему	Издательство, год
Л2.1	Голиков А.М.	Защита информации в инфокоммуникационных системах и сетях : учебное пособие http://biblioclub.ru/index.php?page=book&id=480637	Томск : Томский государственный университет систем управления и радиоэлектроники, 2015
Л2.2	И.В. Ефремов, В.А. Солопова	Информационные технологии в сфере безопасности: практикум : учебное пособие http://biblioclub.ru/index.php?page=book&id=259178	Оренбург: ОГУ, 2013
Л2.3	Л.В. Котова	Сборник задач по дисциплине «Методы и средства защиты информации» : учебное пособие : http://biblioclub.ru/index.php?page=book&id=363040	Санкт-Петербург : Издательство Политехнического университета, 2014

6.2 Перечень программного обеспечения
- Acrobat Reader DC
- Dr.Web Desktop Security Suite, Dr.Web Server Security Suite
- GIMP
- Microsoft Office 365 Pro Plus - subscription license (12 month) (Пакет программ Word, Excel, Access, PowerPoint, Outlook, OneNote, Publisher, Teams, OneDrive, Yammer, Stream, SharePoint Online)
- Microsoft Windows 10 Education
- XnView
- Архиватор 7-Zip
- 1С:ИТС ПРОФ ВУЗ
- Программная система для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат.ВУЗ»
6.3 Перечень информационных справочных систем
- Elsevier (база данных «Freedom Collection» и коллекции электронных книг «Freedom Collection eBook collection», национальная подписка на полнотекстовые ресурсы)
- SCOPUS издательства Elsevier
- SpringerNature (национальная подписка на полнотекстовые ресурсы)
- БД «Polpred.com. Обзор СМИ»
- УИС РОССИЯ
- ЭБС «E-LIBRARY.RU»
- ЭБС «ЛАНЬ»
- ЭБС «РУКОНТ» (Контекстум)
- ЭБС «Университетская библиотека онлайн»
- ЭБС «ЮРАЙТ» (Коллекция Легендарные книги)
- ЭБС «IPR BOOKS»

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	Наименование специального помещения: помещение для самостоятельной работы, Читальный зал. Оснащенность: ПК-4шт., Принтер-1шт., Телефон-1шт., Письменный стол-4 шт., Парта-2 шт.
7.2	Наименование специального помещения: учебная аудитория для проведения лекционного типа, практических занятий, курсового проектирования (выполнения курсовых работ), групповых консультаций, индивидуальных консультаций, текущего контроля, промежуточной аттестации, Учебная аудитория. Оснащенность: Меловая доска-1шт., Комплект учебной мебели, ноутбук, проекционное оборудование (мультимедийный проектор и экран).

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Работа над теоретическим материалом происходит кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю.

Проработка рабочей программы дисциплины, уделяя особое внимание целям и задачам, структуре и содержанию дисциплины. Конспектирование источников, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, работа с информационными источниками в разных форматах.

Также в процессе изучения дисциплины методические рекомендации могут быть изданы отдельным документом

Приложение

Балльно-рейтинговая карта дисциплины «Методы и средства защиты информации»

Курс 4 Семестр 8

Вид контроля		Минимальное количество баллов	Максимальное количество баллов
Введение в информационную безопасность			
Текущий контроль по разделу:			
1	Аудиторная работа	8	10
2	Самостоятельная работа (специальные обязательные формы)	8	10
3	Самостоятельная работа (специальные формы на выбор студента)	4	8
Контрольное мероприятие по разделу		4	12
Промежуточный контроль		**24**	**40**
Защита информации в информационно-образовательной среде			
Текущий контроль по разделу:			
1	Аудиторная работа	8	18
2	Самостоятельная работа (специальные обязательные формы)	10	20
3	Самостоятельная работа (специальные формы на выбор студента)	8	14
Контрольное мероприятие по разделу		6	8
Промежуточный контроль		**32**	**60**
Промежуточная аттестация			
	Итого:	**56**	**100**

Виды контроля		Перечень или примеры заданий, критерии оценки и количество баллов	Темы для изучения и образовательные результаты
Текущий контроль по разделу «Введение в информационную безопасность»			
1	Аудиторная работа (10 баллов)	Выполнение лабораторно-практических работ «Особенности защиты информации в локальных и глобальных компьютерных сетях». *Выполнение лабораторной работы – 4 балла * 2 работы=8.* Отчёт о выполнении лабораторной работы. *Критерии:* *отчёт содержит полную информацию по изучаемым вопросам;* *студент чётко и ясно объясняет методы защиты;* *студент демонстрирует знания программных средств защиты информации при работе в компьютерных сетях;* *студент демонстрирует навыки организации защиты при работе в компьютерных сетях.*	**Тема 3.** Современные методы защиты информации. Политика безопасности и механизмы разграничения прав доступа к массивам информации в информационно-образовательной среде. Парольные методы защиты информации. Программные средства для хранения паролей. Основные методы и средства защиты информационных систем. Классификация способов и средств комплексной защиты информации. Защита Интернет-подключений, функции и назначение межсетевых экранов (брандмауэров). **Знает**: методы и устройства обеспечения безопасности информации в профессиональной сетевой среде; основные виды угроз информационной безопасности; алгоритмы и методы, программные средства и устройства обеспечения безопасности

		Каждый критерий – 0,25 балла	информации в профессиональной сетевой среде; **Умеет:** защищать информацию с использованием паролей, противостоять методам социальной инженерии; осуществлять выбор необходимых для защиты информации аппаратных и программных средств, средств сетевой коммуникации на основе стандартов и норм, принятых в профессиональной среде и с учетом требований информационной безопасности применять методы защиты данных в процессе решения практических задач получения, хранения, обработки и передачи информации; **Владеет:** методами анализа эффективности использования аппаратных и программных средств защиты информации и беспечения безопасности ее использования, в том числе в процессе сетевой коммуникации навыками применения методов защиты данных в процессе решения практических задач получения, хранения, обработки и передачи информации. навыками применения методов и средств организационно-правовой защиты информации; навыками применения методов и средств инженерно-технической защиты;
		Выполнение лабораторно-практических работ «Компьютерные вирусы», «Антивирусные средства защиты». *Критерии: выполнение лабораторной работы – 2 балла * 2 работы =4* Отчёт о выполнении лабораторной работы. *Критерии:* *отчёт содержит полные ответы на контрольные вопросы;* *студент чётко и ясно объясняет алгоритм действий пользователя при заражении компьютера вирусами;* *студент демонстрирует знания способов профилактики заражения компьютера вирусами, многообразия антивирусных средств, их возможностей и особенностей приобретения, установки и использования;* *студент демонстрирует навыки работы с антивирусной программой.* *Каждый критерий – 0,5 балла*	**Тема 4.** Понятие и классификация «компьютерных вирусов». Защита от «компьютерных вирусов». Классификация «компьютерных вирусов». Общая организация защиты от «компьютерных вирусов». Защита от деструктивных действий и размножения вирусов с использованием средств аппаратного и программного контроля. Антивирусное программное обеспечение. **Знает:** понятие и виды компьютерных вирусов, их разрушительные действия; методы защиты от компьютерных вирусов; **Умеет:** прогнозировать действие вирусов и атак, направленных на вызов отказа в обслуживании; объяснить угрозы безопасности из-за компьютерных вирусов и атак, направленных на инициирование отказов в обслуживании; **Владеет:** навыками работы с антивирусным программным обеспечением.
		Выполнение лабораторно-практических работ «Принципы криптографической защиты информации». *Критерии: выполнение лабораторной работы – 2 балла * 3 работы =6* Отчёт о выполнении лабораторных работ в MS Excel. *Критерии:* *отчёт содержит полные ответы на контрольные вопросы;*	**Тема 5.** Криптографические методы информационной безопасности. Средства криптографической защиты информации (СКЗИ). Криптографические преобразования. Шифрование и дешифрование информации. Использование криптографических средств для решения задач идентификации и аутентификации. **Знает:** основные виды угроз информационной безопасности; алгоритмы и методы, программные средства и устройства обеспечения безопасности информации в профессиональной сетевой среде;

		студент чётко и ясно объясняет изучаемый алгоритм (метод) шифрования; *студент демонстрирует примеры выполненных практических заданий в MS Excel.* *Каждый критерий оценивается в 1 балл*	возможности и ограничения широко распространенных криптографических методов; понятия криптография, криптоанализ, криптостойкость; понятия шифрование и цифровая подпись, требования к алгоритму шифрования. **Умеет:** объяснить принципы симметричного и асимметричного шифрования; особенности криптографических стандартов. **Владеет:** основами технологии криптографической защиты информации.
2	Самостоятельная работа (обязательные формы) (10 баллов)	**Домашняя работа поисково-аналитического характера по теме «Основные понятия информационной безопасности. Нормативно-правовое обеспечение информационной безопасности» (6 баллов)** Содержание представленной информации осмысленно и интерпретировано в соответствии с поставленной задачей Результат представлен в лаконичной форме, удобной для восприятия. Визуализированы результаты работы (составлен глог по теме «Информационная безопасность в РФ» например, с помощью сервиса glogster.com); *Каждый критерий оценивается по следующему правилу: 0 баллов - критерий не выполнен; 1 балл – выполнен частично; 2 балла – выполнен полностью*	Тема 1. Основные понятия информационной безопасности. Знает: нормативно-правовую и законодательную базу по обеспечению информационной безопасности; Умеет: детализировать и интерпретировать нормативно-правовую информацию в области информационной безопасности; Владеет: • навыками информационного анализа информации по теме.
		Практическая работа по теме «Угрозы безопасности информации. Компьютерные преступления» (4 балла) Составлена google-таблица с (2 балла): классификаций угроз безопасности информации по различным признакам, классификацией компьютерных преступлений,и др. Материал структурирован, информация полная, адекватная и актуальная (1 балл); Оформление задания соответствует требованиям (1 балл).	Тема 2. Угрозы безопасности информации, их классификация. Знает: основные виды компьютерных преступлений; последствия нарушения авторских прав на программное обеспечение и роль соответствующих правоохранительных организаций; Умеет: осуществлять выбор необходимых для защиты информации аппаратных и программных средств, средств сетевой коммуникации на основе стандартов и норм, принятых в профессиональной среде и с учетом требований информационной безопасности; приводить примеры реализации угроз информационной безопасности; Владеет: навыками определения причин, видов и каналов утечки конфиденциальной информации методами анализа эффективности использования аппаратных и программных средств защиты информации и беспечения безопасности ее использования, в том числе в процессе сетевой коммуникации

3	Самостоятельная работа (на выбор студента) (8 баллов)	Домашняя работа поисково-аналитического характера по теме «Информационная безопасность: концептуальные, практические, системотехнические, экономические, правовые, криптологические, математические, психологические, физические, программные и информационные основы». Составление словаря терминов в области информационной безопасности и перечня нормативных документов по информационной безопасности (Google-документ) (4 балла). • Наполнение терминологического словаря (2 балла); • Корректность цитирования источников (1 балл); • Грамотность содержания и оформления (1 балл).	Тема 1. Основные понятия информационной безопасности. Знает: основные понятия информационной безопасности; нормативно-правовую и законодательную базу по обеспечению информационной безопасности; основные виды угроз информационной безопасности; алгоритмы и методы, программные средства и устройства обеспечения безопасности информации в профессиональной сетевой среде; Умеет: детализировать и интерпретировать нормативно-правовую информацию в области информационной безопасности; Владеет: навыками информационного анализа информации по теме.
		Подготовка мультимедийной презентации и сообщения об источниках угроз информационной безопасности и способах совершения компьютерных преступлений (4 балла) • Информационная (содержательная) насыщенность продукта; • Авторская интерпретация содержания; • Уровень структуризации информации; • Адекватный выбор выразительных средств; • Выбор адекватного сервиса для представления презентации; • Корректность цитирования источников; • Реализация технологических возможностей сервиса • Размещение на серверах www.slideshare.net,www.slideboom.com; создание Google-презентаций; использование сервиса www.prezy.com и т.п. *Каждый критерий оценивается в 0,5 балла*	Тема 2. Угрозы безопасности информации, их классификация Знает: основные виды компьютерных преступлений; последствия нарушения авторских прав на программное обеспечение и роль соответствующих правоохранительных организаций; Умеет: приводить примеры реализации угроз информационной безопасности; Владеет: навыками определения причин, видов и каналов утечки конфиденциальной информации.
Контрольное мероприятие по разделу (12 баллов)		Подготовка мультимедийной презентации и сообщения об источниках угроз информационной безопасности и способах совершения компьютерных преступлений • Информационная (содержательная) насыщенность продукта; • Авторская интерпретация содержания; • Уровень структуризации информации; • Адекватный выбор выразительных средств; • Выбор адекватного сервиса для представления презентации; • Корректность цитирования источников; • Реализация технологических возможностей сервиса • Размещение на серверах www.slideshare.net,www.slideboom.com; создание Google-презентаций; использование сервиса www.prezy.com и т.п.	Угрозы безопасности информации, их классификация Знает: основные виды компьютерных преступлений; последствия нарушения авторских прав на программное обеспечение и роль соответствующих правоохранительных организаций; Умеет: приводить примеры реализации угроз информационной безопасности; Владеет: навыками определения причин, видов и каналов утечки конфиденциальной информации методами анализа эффективности использования аппаратных и программных средств защиты информации и беспечения безопасности ее использования, в том числе в процессе сетевой коммуникации

Текущий контроль по разделу «Защита информации в информационно-образовательной среде»			
1	Аудиторная работа (18 баллов)	Выполнение лабораторно-практических работ «Особенности защиты информации в локальных и глобальных компьютерных сетях». *Выполнение лабораторной работы – 4 балла * 2 работы=8 баллов.* Отчёт о выполнении лабораторной работы. *Критерии:* *отчёт содержит полную информацию по изучаемым вопросам;* *студент чётко и ясно объясняет методы защиты;* *студент демонстрирует знания программных средств защиты информации при работе в компьютерных сетях;* *студент демонстрирует навыки организации защиты при работе в компьютерных сетях.* *Каждый критерий – 0,25 балла*	**Тема 3.** Современные методы защиты информации. Политика безопасности и механизмы разграничения прав доступа к массивам информации в информационно-образовательной среде. Парольные методы защиты информации. Программные средства для хранения паролей. Основные методы и средства защиты информационных систем. Классификация способов и средств комплексной защиты информации. Защита Интернет-подключений, функции и назначение межсетевых экранов (брандмауэров). **Знает**: основные виды угроз информационной безопасности; алгоритмы и методы, программные средства и устройства обеспечения безопасности информации в профессиональной сетевой среде; **Умеет:** осуществлять выбор необходимых для защиты информации аппаратных и программных средств, средств сетевой коммуникации на основе стандартов и норм, принятых в профессиональной среде и с учетом требований информационной безопасности; защищать информацию с использованием паролей, противостоять методам социальной инженерии; применять методы защиты данных в процессе решения практических задач получения, хранения, обработки и передачи информации; **Владеет:** навыками применения методов защиты данных в процессе решения практических задач получения, хранения, обработки и передачи информации. навыками применения методов и средств организационно-правовой защиты информации; навыками применения методов и средств инженерно-технической защиты;
		Выполнение лабораторно-практических работ «Компьютерные вирусы», «Антивирусные средства защиты». *Критерии: выполнение лабораторной работы – 2 балла * 2 работы =4 балла* Отчёт о выполнении лабораторной работы. *Критерии:* *отчёт содержит полные ответы на контрольные вопросы;* *студент чётко и ясно объясняет алгоритм действий пользователя при заражении компьютера вирусами;* *студент демонстрирует знания способов профилактики заражения компьютера вирусами, многообразия антивирусных средств, их возможностей и особенностей приобретения, установки и использования;*	**Тема 4.** Понятие и классификация «компьютерных вирусов». Защита от «компьютерных вирусов». Классификация «компьютерных вирусов». Общая организация защиты от «компьютерных вирусов». Защита от деструктивных действий и размножения вирусов с использованием средств аппаратного и программного контроля. Антивирусное программное обеспечение. **Знает:** понятие и виды компьютерных вирусов, их разрушительные действия; методы защиты от компьютерных вирусов; **Умеет:** прогнозировать действие вирусов и атак, направленных на вызов отказа в обслуживании; объяснить угрозы безопасности из-за компьютерных вирусов и атак, направленных на инициирование отказов в обслуживании; **Владеет:** навыками работы с антивирусным программным обеспечением.

		студент демонстрирует навыки работы с антивирусной программой. • *Каждый критерий – 0,5 балла*	•
		Выполнение лабораторно-практических работ «Принципы криптографической защиты информации». *Критерии: выполнение лабораторной работы – 2 балла * 3 работы =6 баллв* Отчёт о выполнении лабораторных работ в MS Excel. *Критерии:* *отчёт содержит полные ответы на контрольные вопросы;* *студент чётко и ясно объясняет изучаемый алгоритм (метод) шифрования;* *студент демонстрирует примеры выполненных практических заданий в MS Excel.* • *Каждый критерий оценивается в 1 балл*	**Тема 5.** Криптографические методы информационной безопасности. Средства криптографической защиты информации (СКЗИ). Криптографические преобразования. Шифрование и дешифрование информации. Использование криптографических средств для решения задач идентификации и аутентификации. **Знает:** основные виды угроз информационной безопасности; алгоритмы и методы, программные средства и устройства обеспечения безопасности информации в профессиональной сетевой среде; возможности и ограничения широко распространенных криптографических методов; понятия криптография, криптоанализ, криптостойкость; понятия шифрование и цифровая подпись, требования к алгоритму шифрования. **Умеет:** объяснить принципы симметричного и асимметричного шифрования; особенности криптографических стандартов. **Владеет:** основами технологии криптографической защиты информации.
2	Самостоятельная работа (обязательные формы) (20 баллов)	Самостоятельное обучение в Интернет-университете http://www.intuit.ru/studies/courses/680/536/info Курс «Основы информационной безопасности при работе на компьютере» Курс обучает правильному обеспечению безопасности персональных данных. В курсе рассмотрены общие понятия в области защиты персональных данных, а также методы их защиты от злоумышленников. *Сертификат – 5 баллов.*	**Тема 3.** Современные методы защиты информации. Политика безопасности и механизмы разграничения прав доступа к массивам информации в информационно-образовательной среде Примеры реализации угроз информационной безопасности. Причины, виды и каналы утечки конфиденциальной информации. Методы и средства несанкционированного доступа к компьютерным ресурсам и программным средствам. Аппаратные и программные средства защиты информации. Компьютерные вирусы. Действия вирусов. Разновидности вирусов. Профилактика и лечение. Антивирусные программы и их виды. Использование файерволов. Противодействие методам социальной инженерии. Безопасность банковских карт. Безопасность работы в интернете. **Знает:** основные виды угроз информационной безопасности; алгоритмы и методы, программные средства и устройства обеспечения безопасности информации в профессиональной сетевой среде; правовые нормы организации информационного пространства на основе сетевых технологий; основные обязанности по обеспечению и защите авторского права в процессе информационного обмена в профессиональной деятельности; **Умеет:**

			осуществлять выбор необходимых для защиты информации аппаратных и программных средств, средств сетевой коммуникации на основе стандартов и норм, принятых в профессиональной среде и с учетом требований информационной безопасности использовать методы и программно-аппаратные средства защиты информации в процессе профессиональной деятельности; **Владеет:** основными технологиями обеспечения защиты информации как на локальном компьютере, так и в процессе сетевого взаимодействия.
		Составление ментальной карты (кластера, фишбоун и др.) по теме «Понятие и классификация компьютерных вирусов. Защита от компьютерных вирусов». Оценка достижений – максимум **3 балла** 1. Работа как результат изученного в аудитории материала – **1 балл** 2. Использован материал, не рассмотренный на практических занятиях на уроке. – **2 балла** 3. Работа с элементами новизны и оригинальности – **3 балла**	**Тема 4.** Понятие и классификация «компьютерных вирусов». Защита от «компьютерных вирусов». Классификация «компьютерных вирусов». Способы заражения компьютерными вирусами. Методы защиты от компьютерных вирусов. **Знает:** классификацию компьютерных вирусов по различным признакам; методы защиты от компьютерных вирусов; **Умеет:** компьютерных вирусов и атак, направленных на инициирование отказов в обслуживании.
		Создание коллективного Google-документа о состоянии нормативно-правовой базы в сфере электронной цифровой подписи, цифровых сертификатов, лицензирования деятельности удостоверяющих центров. Оценка достижений – максимум **2 балла.** *Критерии (каждый критерий – 1 балл):* *тема раскрыта полностью;* *студент владеет материалом и демонстрирует знания при ответе на вопросы.*	**Тема 5.** Криптографические методы информационной безопасности. Электронная подпись. Электронный сертификат. Удостоверяющий центр. Открытый и закрытый ключи. Лицензирование. **Знает:** понятия электронной подписи, электронного сертификата, удостоверяющего центра; **Умеет:** объяснить особенности сертификации средств электронной подписи. **Владеет:** методами анализа эффективности использования аппаратных и программных средств защиты информации и беспечения безопасности ее использования, в том числе в процессе сетевой коммуникации навыками применения методов и средств организационно-правовой защиты информации в информационно-образовательной среде (персональной, коллективной, образовательного учреждения);
		Создание Google-сайта (10 баллов) 1. Контент (содержание) – 5 баллов Ясно ли предназначение сайта? Присутствует ли информация на всех страницах (во всех разделах) сайта? Ориентирован ли сайт на целевую аудиторию?	**Тема 3.** Современные методы защиты информации. Политика безопасности и механизмы разграничения прав доступа к массивам информации в информационно-образовательной среде. Защита информации при работе в компьютерных сетях. Парольная защита информации. Разграничение доступа. **Знает:** основные виды угроз информационной безопасности;

		Соответствует ли содержание сайта (текстовое, графическое) его тематике? Есть ли грамматические или синтаксические ошибки? **2.** Эргономичность использования – 2 балла Организовано ли содержание логически? Насколько проста и понятна навигация? Расположена ли навигация в одном и том же месте на всех страницах? Позволяет ли навигация вернуться на предыдущие подуровни? **3.** Внешний вид (дизайн) – 3 балла Выдержаны ли цвета, шрифты, графика в едином стиле? Сбалансированы ли цвета дизайна страниц? Сбалансирован ли макет страницы (наличие сетки)? Не перегружена ли страница информацией (особенно касается главных станиц)? Качественна ли графика и сочетается ли она с остальными составляющими страницы? Не мешает ли графика пользователю воспринимать информацию	алгоритмы и методы, программные средства и устройства обеспечения безопасности информации в профессиональной сетевой среде; способы защиты информации при работе в компьютерных сетях; методы и устройства обеспечения безопасности информации в профессиональной сетевой среде; **Умеет:** структурировать информацию по изучаемой теме; открывать для доступа (защищать) размещаемую в сети информацию.
3	Самостоятельная работа (на выбор студента) (14 баллов)	Подготовка мультимедийной презентации о классификации и схемах функционирования компьютерных вирусов или антивирусных программных средствах. *Оценивание – 5 баллов.* *Критерии:* 1. Полнота раскрытия темы - 1 б. 2. Актуальность материалов, отражающих современный уровень состояния вопроса - 1 б. 3. Оригинальность изложения идеи, наличие интересных фактов - 1 б. 4. Дизайн оформления визуального ряда (презентации и т.д.) - 0,5 б. 5. Логичность, последовательность изложения, отсутствие информации, не относящейся к теме - 1 б. 6. Отсутствие синтаксических, стилистических и орфографических ошибок - 0,5 б.	**Тема 4.** Понятие и классификация «компьютерных вирусов». Защита от «компьютерных вирусов». Классификация «компьютерных вирусов». Способы заражения компьютерными вирусами. Методы защиты от компьютерных вирусов. **Знает:** классификацию компьютерных вирусов по различным признакам; методы защиты от компьютерных вирусов; **Умеет:** основные виды угроз информационной безопасности; алгоритмы и методы, программные средства и устройства обеспечения безопасности информации в профессиональной сетевой среде; применять на практике методы защиты от компьютерных вирусов.
		Эссе рефлексивного характера по одной из проблем курса: «Как я лично понимаю термин *информационная безопасность*?», «Защита информации: основные подходы», «Использование методов социальной инженерии для получения доступа к информации», «Особенности парольной защиты информации» **(2 балла).** Отражена глубина изучения проблемы, проведен ее многофакторный анализ; Работа отражает личное видение автора проблемы и пути ее решения; Соответствие стилю эссе; Содержание эссе размещено в Google-группе *Каждый критерий оценивается в 0,5 балла*	**Тема 3.** Современные методы защиты информации. Политика безопасности и механизмы разграничения прав доступа к массивам информации в информационно-образовательной среде. Парольные методы защиты информации. Программные средства для хранения паролей. Основные методы и средства защиты информационных систем. Классификация способов и средств комплексной защиты информации. Защита Интернет-подключений, функции и назначение межсетевых экранов (брандмауэров). **Знает**: терминологический аппарат науки; **Умеет:**

			применять методы защиты данных в процессе решения практических задач получения, хранения, обработки и передачи информации; формулировать критерии и проводить рациональный поиск информации в соответствии с поставленными целями; критически оценивать информацию с точки зрения ее качества, достоверности и релевантности; **Владеет:** навыками применения методов защиты данных в процессе решения практических задач получения, хранения, обработки и передачи информации.
		Создание индивидуального *блога* с обзором правовых и технологических аспектов электронной цифровой подписи и электронных сертификатов.– *5 баллов* *Критерии* оценки блога *Технологичность (наличие навигационных элементов (облако тегов, аннотация содержания и пр., целесообразность используемых дополнений, расширений, гаджетов и т.п.) – 3 балла* *Социальность (блог ориентирован на профессиональную сферу) – 2 балла*	**Тема 5.** Криптографические методы информационной безопасности. Электронная подпись. Электронный сертификат. Удостоверяющий центр. Открытый и закрытый ключи. Лицензирование. **Знает:** понятия электронной подписи, электронного сертификата, удостоверяющего центра; **Умеет:** объяснить особенности сертификации средств электронной подписи. **Владеет:** навыками самостоятельного поиска и структурирования информации.
		Составление аннотированного каталога Интернет-ресурсов по теме (по выбору студента) (2 балла -10-15 ресурсов) Репрезентативность ресурсов, Соответствие выбранной тематике, Научная новизна, доступность изложения, Качество оформления каталога, выбор средств для его тиражирования. *Каждый критерий оценивается в 0,5 балла*	**Тема 3.** Современные методы защиты информации. Политика безопасности и механизмы разграничения прав доступа к массивам информации в информационно-образовательной среде Основные методы и средства защиты информационных систем. Понятие политики безопасности информационных систем. Парольные схемы аутентификации. Защита Интернет-подключений, функции и назначение межсетевых экранов. Знает: основные понятия информационной безопасности; нормативно-правовую и законодательную базу по обеспечению информационной безопасности; Умеет: разъяснить понятие информационной безопасности; основные составляющие информационной безопасности; указать сильные и слабые стороны различных подходов к обеспечению безопасности; описывать правовые основы обеспечения конфиденциальности; Владеет: терминологическим аппаратом.
Контрольное мероприятие по разделу (8 баллов)		Создание индивидуального *блога* с обзором правовых и технологических аспектов электронной цифровой подписи и электронных сертификатов. *баллов*	Криптографические методы информационной безопасности. Электронная подпись. Электронный сертификат. Удостоверяющий центр. Открытый и закрытый ключи. Лицензирование. Знает: понятия электронной подписи, электронного сертификата, удостоверяющего центра; Умеет

		объяснить особенности сертификации средств электронной подписи. Владеет: методами анализа эффективности использования аппаратных и программных средств защиты информации и беспечения безопасности ее использования, в том числе в процессе сетевой коммуникации навыками применения методов и средств организационно-правовой защиты информации в информационно-образовательной среде (персональной, коллективной, образовательного учреждения);.
Промежуточная аттестация	Представлены в фонде оценочных средств для промежуточной аттестации по дисциплине	