Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Северо-Западный институт управления – филиал РАНХиГС

Кафедра бизнес-информатики

УТВЕРЖДЕНО

Директор СЗИУ РАНХиГС
А.Д. Хлутков

ПРОГРАММА МАГИСТРАТУРЫ
Аналитическое обеспечение информационной безопасности

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ФТД.01 Средства защиты информации
(индекс, наименование дисциплины, в соответствии с учебным планом)

38.04.05 Бизнес-информатика
(код, наименование направления подготовки (специальности)

Очная
(форма обучения)

Год набора – 2024

Санкт-Петербург, 2024 г.

Автор–составитель:
Кандидат технических наук, доцент, доцент кафедры бизнес-информатики Зеленина Лариса Ивановна.

Заведующий кафедрой бизнес-информатики
Доктор военных наук, профессор Наумов Владимир Николаевич

В новой редакции РПД ФТД.01 «Средства информационной безопасности» одобрена протоколом № 10 заседания кафедры бизнес-информатики от 26.06.2024 г

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы

Дисциплина ФТД.01 «Средства информационной безопасности» обеспечивает овладение следующими компетенциями:

Таблица 1

Код компетенции	Наименование компетенции	Код компонента компетенции	Наименование компонента компетенции
ПКс-2	Способен обосновывать подходы и требования к системе обеспечения информационной безопасности, оценивать уровни безопасности компьютерных систем и сетей	ПКс-2.3	Способен оценивать уровни безопасности компьютерных систем и сетей
ПКс-4	Способен управлять информационными сервисами, ресурсами ИТ и ИТ-инновациями. Управлять ИАС в защищенном исполнении, обслуживать системы защиты	ПКс-4.2	Способен управлять ИАС в защищенном исполнении

В результате освоения дисциплины у магистрантов должны быть сформированы компетенции:

Таблица 2

ОТФ/ТФ (при наличии профстандарта)/ профессиональные действия	Код компонента компетенции	Результаты обучения
Формирование требований к защите информации в автоматизированных системах	ПКс-2.3 • свободно оперировать терминами в сфере информационной безопасности.	на уровне знаний: Знать: – основные понятия и задачи информационной безопасности; – основные средства обеспечения информационной безопасности
		на уровне умения: Уметь: - анализировать проблемы информационной безопасности организаций; - анализировать требования руководящих документов по обеспечению информационной безопасности

		на уровне навыков: Владеть: - навыками соотношения правовых норм в сфере информационной безопасности с условиями ее обеспечения; -навыками выбора организационных мер и технических методов обеспечения информационной безопасности согласно обстоятельствам
Применение ИАС в защищенном исполнении в процессах АИАД	ПКс-4.2	на уровне знаний: Знать: - основы информационной безопасности; - систему организационных мер обеспечения информационной безопасности; - принципы и методы организации службы информационной безопасности; - средства технического обеспечения информационной безопасности
		на уровне умения: Уметь: - аргументировать мнение и решения в технических, организационных и правовых терминах обеспечения информационной безопасности в процессах АИД
		на уровне навыков: Владеть: - навыками использования аппаратных средств и программных методов защиты структурных компонентов ИТ-систем

2.Объем и место дисциплины в структуре ОП ВО

Объем дисциплины

Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 акад. часа/54 астрон. часа.

Таблица 3

Очная форма

Вид работы	Трудоемкость (акад/астр.часы)
Общая трудоемкость	72/54
Контактная работа с преподавателем	36/27
Лекции	16/12
Практические занятия	20/15
Лабораторные занятия	-
Самостоятельная работа	36/27
Контроль	-
Формы текущего контроля	Устный опрос, задание, тестирование
Форма промежуточной аттестации	Зачет

Место дисциплины в структуре образовательной программы

Дисциплина ФТД.01 «Средства информационной безопасности» относится к части ФТД. Факультативные дисциплины. Преподавание дисциплины опирается на дисциплины «Моделирование бизнес-процессов и формирование требований к информационным системам в защищенном исполнении», «Организационное и правовое обеспечение информационной безопасности», «Моделирование информационной безопасности. Управление рисками», «Управление информационной безопасностью». Дисциплина изучается во втором семестре второго года обучения.

В свою очередь она создаёт необходимые предпосылки для освоения программ таких дисциплин, как «Криптографические методы защиты информации», «Управление информационной инфраструктурой предприятий», «Информационная инфраструктура предприятия».

Знания, умения и навыки, полученные при изучении дисциплины, используются студентами при выполнении выпускных квалификационных работ.

3.Содержание и структура дисциплины

3.1. Структура дисциплины

№ п/п	Наименование тем	Объем дисциплины, час.					Форма текущего контроля успеваемости**, промежуточной аттестации***
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий		СР		
			Л/ДОТ	ПЗ/ДОТ	КСР	СРО	СП	
Тема 1	Доступ к данным. Идентификация и аутентификация субъектов доступа.	22	4	6/3		12		УО/Зад/Т
Тема 2	Аппаратные системы разграничения доступа.	24	6	6/3		12		УО/Т
Тема 3	Защита программ от несанкционированного копирования и изучения. Деструктивные программные воздействия.	26	6	8/4		12		УО/Т
Промежуточная аттестация		-						Зачет
Всего (акад./астр. часы):		72/54	16/12	20/15		36/27		

Примечание:

Используемые сокращения:

Л – занятия лекционного типа (лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях, обучающимся);

ПЗ – практические занятия (виды занятия семинарского типа за исключением лабораторных работ);

КСР – индивидуальная работа обучающихся с педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях (в том числе индивидуальные консультации);
СР – самостоятельная работа, осуществляемая без участия педагогических работников организации и (или) лиц, привлекаемых организацией к реализации образовательных программ на иных условиях;
СП – самопроверка;
СРО – самостоятельная работа обучающегося
Опрос (О), тестирование (Т), задание (Зад)

3.2. Содержание дисциплины

Тема 1. Доступ к данным. Идентификация и аутентификация субъектов доступа.

Необходимость использования дополнительных программных и аппаратных СЗИ. Процедура доступа к данным в современных компьютерных системах. Выбор объекта для доступа. Форма хранения прав доступа субъектов к объектам. Средства осуществления доступа к объектам со стороны пользователей

Аппаратная идентификация пользователей. Технологии аутентификации. Причины использования аппаратной идентификации пользователей в компьютерных системах. Виды аппаратных идентификаторов, присутствующих на рынке, их характеристики и области применения. Технологии биометрической идентификации пользователей. Области использования различных систем биометрической идентификации

Виды аутентификации. Методы аутентификации. Реализация методов аутентификации. Схема интеграции методов аутентификации в существующую информационную систему

Тема 2. Аппаратные системы разграничения доступа.

Варианты реализации средств аппаратной поддержки механизмов обеспечения ИБ. Рынок решений, использующих механизмы аппаратной поддержки механизмов разграничения доступа. Примеры аппаратных систем разграничения доступа. Недостатки аппаратных СЗИ. Трудности интеграции аппаратных СЗИ в существующие информационные системы

Тема 3. Защита программ от несанкционированного копирования и изучения. Деструктивные программные воздействия

Классификация методов защиты программного обеспечения от копирования Оптимальные варианты реализации схемы защиты от копирования для прикладной программы, программы математического моделирования, операционной системы, программного СЗИ. Трудности использования средств защиты от копирования. Критерии выбора средств защиты ПО от несанкционированного копирования

Защита программ от изучения. Модель нарушителя целостности и конфиденциальности программного кода. Средства изучения программного кода. Последствия взлома программного обеспечения. Методы противодействия изучению и отладке программного обеспечения

Деструктивные программные воздействия. Классификация деструктивных программные воздействия по методам реализации угроз безопасности. Опасность самореплицирующихся программ. Классификация разработчиков деструктивного программного обеспечения. Классификация компьютерных вирусов. Классификация программ-шпионов. Организационные меры противодействия деструктивным программным воздействиям. Технические средства противодействия деструктивным программным воздействиям различных типов. Классификация разработчиков деструктивного программного обеспечения

4.Материалы текущего контроля успеваемости обучающихся

4.1. В ходе реализации дисциплины используются следующие методы текущего контроля успеваемости обучающихся:

Таблица 4.1

Тема (раздел)	Формы текущего контроля успеваемости
Тема 1. Доступ к данным. Идентификация и аутентификация субъектов доступа.	УО/Зад/Т
Тема 2. Аппаратные системы разграничения доступа.	УО/Т
Тема 3. Защита программ от несанкционированного копирования и изучения. Деструктивные программные воздействия.	УО/Т

4.2. Типовые материалы текущего контроля успеваемости обучающихся.

Типовые оценочные материалы по теме 1

Задания по теме 1

Задание 1.

Установите взаимно однозначное соответствие

1	Идентификация	А	Может быть охарактеризован тем, какой пользователь обращается
2	Аутентификация	Б	Аутентификация Б Процесс распознавания элемента системы, обычно с помощью заранее определенного идентификатора или другой уникальной информации – за счѐт этого каждый субъект или объект системы должен быть однозначно идентифицируем.
3	Запрос на доступ к ресурсу	В	Проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется

			перед разрешением доступа к ресурсу)

Задание2.

Установите взаимно однозначное соответствие методы реализации систем одноразовых паролей

1	Метод "запрос-ответ"	А	В качестве исходной строки в нем используется не время, а количество успешных процедур аутентификации, проведенных до текущей
2	Метод "только ответ"	Б	В начале процедуры аутентификации пользователь отправляет на сервер свой логин. В ответ на это последний генерирует некую случайную строку и посылает ее обратно.
3	Метод "синхронизация по времени"	В	При этом в процессе создания строки используется значение предыдущего запроса
4	Метод "синхронизация по событию"	Г	При этом обычно используется не точное указание времени, а текущий интервал с установленными заранее границами (например, 30 секунд).

Тест по теме 1

1. Возможность за приемлемое время получить требуемую информационную услугу называется:

1. Конфиденциальность
2. Доступность
3. Целостность
4. Непрерывность

2. К аспектам информационной безопасности не относится:
1. Доступность
2. Целостность
3. Конфиденциальность
4. Защищенность

3. По каким критериям нельзя классифицировать угрозы:
1. по расположению источника угроз
2. по аспекту информационной безопасности, против которого угрозы направлены в первую очередь
3. по способу предотвращения
4. по компонентам информационных систем, на которые угрозы нацелены

4. Главное достоинство парольной аутентификации – …
1. простота
2. надежность
3. секретность
4. запоминаемость

5. К основным функциям подсистемы защиты операционной системы относятся:
1. идентификация, аутентификация, авторизация, управление политикой безопасности и разграничение доступа
2. криптографические функции
3. сетевые функции
4. все вышеперечисленные

6. Под системой защиты информации в компьютерных сетях понимается:
1. состояние всех компонент компьютерной системы, при котором обеспечивается защита информации от возможных угроз на требуемом уровне
2. одно из основных направлений обеспечения безопасности государства, отрасли, ведомства, государственной организации или частной фирмы
3. единый комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищенность информации в КС в соответствии с принятой политикой безопасности

7. Идентификация – это ...
1. пользователь подтверждает идентификацию, вводя в систему уникальную, не известную другим пользователям информацию о себе
2. информационных ресурсов, систем и технологий является субъект с полномочиями владения и пользования указанными объектами. Под пользователем информации будем понимать субъекта, обращающегося к информационной системе за получением необходимой ему информации и пользующегося ею
3. пользователь сообщает системе по ее запросу свое имя

Типовые вопросы для опроса по теме 1

1. В чем состоит необходимость использования дополнительных программных и аппаратных СЗИ.
2. Как осуществляется выбор объекта для доступа в современных компьютерных системах.
3. Какова форма хранения прав доступа субъектов к объектам.
4. Каковы средства осуществления доступа к объектам со стороны пользователей

9. Виды аппаратных идентификаторов, присутствующих на рынке, их характеристики и области применения.
10. Каковы технологии биометрической идентификации пользователей (перечислить). Области использования различных систем биометрической идентификации
11. Виды аутентификации.
12. Привести пример практической реализации одного из методов аутентификации.
13. Предложить схему интеграции одного из методов аутентификации в существующую информационную систему

Типовые оценочные материалы по теме 2

Тест по теме 2

1. Как называется совокупность условий и факторов, создающих потенциальную угрозу или реально существующую опасность нарушения безопасности информации?
1. атака
2. угроза
3. источник угрозы
4. цель злоумышленника

2. Как называется совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация?
1. несанкционированный канал утечки информации
2. технический канал утечки информации
3. параметрический канал утечки информации
4. физический канал утечки информации

3.Что является носителем информации в оптическом канале утечки информации?
1. акустическая волна
2. электрическое поле
3. электромагнитное поле
4. световая волна

4.В каком техническом канале утечки информации носителем является упругая акустическая волна?
1. оптический
2. акустический
3. материально-вещественный
4. радиоэлектронный

5.Как называется технический канал утечки информации, заключающийся в перехвате электромагнитных излучений на частотах работы передатчиков систем и средств связи?
1. электромагнитный
2. электрический
3. индукционный

6.Какие преимущества имеет квантовый компьютер в сравнении с классическим компьютером:
1. Может иметь память экспоненциально большого размера.
2. Любой алгоритм для квантового компьютера эффективнее алгоритма для классического компьютера.

3. Некоторые алгоритмы для квантового компьютера эффективнее соответствующих алгоритмов для классического компьютера.
4. Может параллельно выполнять массивные вычисления.

7. Какие недостатки имеет квантовый компьютер в сравнении с классическим компьютером:
1. Не может иметь память большого размера.
2. Чтение состояния кубита разрушает это состояние.
3. Корректный ответ можно получить лишь с некоторой вероятностью.
4. Не способен выполнять параллельные вычисления.

Типовые вопросы для опроса по теме 2:

1. Перечислить варианты реализации средств аппаратной поддержки механизмов обеспечения ИБ

2. Привести пример использования аппаратной идентифкации пользователя

3. Охарактеризовать существующие на рынке решения, использующие механизмы аппаратной поддержки механизмов разграничения доступа

4. Каковы принципы организации контроллера защиты информации.

5. каковы области применения контроллеров ЗИ 6. Назовите факторы, препятствующие использованию контроллеров ЗИ.

6.Привести примеры аппаратных систем разграничения доступа

7. Предложите вариант реализации исключительно аппаратной СЗИ для защиты определённого компонента компьютерной системы

8. Недостатки аппаратных СЗИ

9.Предложите модель злоумышленника и модель нарушителя, для нейтрализации которых требуются аппаратные СЗИ

Типовые оценочные материалы по теме 3
Тест по теме 3

1. Межсетевой экран (Брандмауэр, firewall) – это…
1. Комплекс аппаратных средств
2. Комплекс программных средств
3. Комплекс аппаратных или программных средств
4. Комплекс аппаратных и программных средств

2. Что из перечисленного не входит в состав программного комплекса антивирусной защиты:
1. Подсистема сканирования
2. Подсистема управления
3. Подсистема обнаружения вирусной активности
4. Подсистема устранения вирусной активности

3. На каком этапе заканчивается жизненный цикл автоматизированной системы?
1. Бета-тестирование системы
2. Внедрение финальной версии системы в эксплуатацию
3. Прекращение сопровождения и технической поддержки системы
4. Альфа-тестирование системы

4. К биометрической системе защиты относятся:
1. антивирусная защита
2. защита паролем

3. идентификация по отпечаткам пальцев
4. физическая защита данных

5. Под информационной системой понимают:
1. упорядоченную совокупность документов и массивов документов и информационных технологий, реализующих информационные процессы
2. процессы сбора, обработки, накопления, хранения, поиска и распространения информации
3. информация циркулирует в технических средствах обработки и хранения информации, а также в каналах связи при ее передаче

6. К основным функциям подсистемы защиты операционной системы относятся:
1. идентификация, аутентификация, авторизация, управление политикой безопасности и разграничение доступа
2. криптографические функции
3. сетевые функции
4. все вышеперечисленные

7. Что является копированием документов?
1. Контактное или бесконтактное подсоединение к различного рода линиям и проводам с целью несанкционированного доступа к информации, образующейся или передаваемой в них тем или иным путем;
2. Получение разведывательной информации за счет приема сигналов электромагнитной энергии пассивными средствами приема, расположенными, как правило, на достаточно безопасном расстоянии от источника конфиденциальной информации;
3. Получения информации, к которой субъект не допущен, но при определенных условиях он может получить возможность узнать ее.
4. Процесс изготовления копий с оригиналов;

Типовые вопросы для опроса по теме 3:

1. Предложите оптимальные варианты реализации схемы защиты от копирования для: прикладной программы, программы математического моделирования, операционной системы, программного СЗИ
2. Трудности использования средств защиты от копирования
3. Критерии выбора средств защиты ПО от несанкционированного копирования
4. Правовые основы защиты программного обеспечения от изучения
5. Модель нарушителя целостности и конфиденциальности программного кода 3. Средства изучения программного кода 4. Последствия взлома программного обеспечения
6. Методы противодействия изучению и отладке программного обеспечения
7. Устранение человеческого фактора при проектировании защищённого программного обеспечения
8. Классифицируйте деструктивные программные воздействия по методам реализации угроз безопасности
9. Классификация разработчиков деструктивного программного обеспечения
10. Классификация компьютерных вирусов
11. Классификация программ-шпионов
12. Организационные меры противодействия деструктивным программным воздействиям.
13. Технические средства противодействия деструктивным программным воздействиям различных типов.
14. Классифицируйте разработчиков деструктивного программного обеспечения

5.Оценочные материалы промежуточной аттестации по дисциплине

5.1. Зачет проводится с применением следующих методов (средств): устный опрос, тестирование.

5.2. Оценочные материалы промежуточной аттестации

Показатели и критерии оценивания компетенций на различных этапах их формирования

Компонент компетенции	Промежуточный/ключевой индикатор	Критерий оценивания
ПКс-2.3	Использует возможности средств информационной безопасности в объеме, необходимом для решения задач бизнес-аналитики	Применяет средства защиты информации. Демонстрирует использование программно-аппаратных средств защиты информации.
ПКс-4.2	Управляет ИАС в защищенном исполнении, обслуживает системы защиты	Демонстрирует способность управления ИАС в защищенном исполнении и обслуживания систем защиты

Типовые вопросы, выносимые на зачет

1. Необходимость использования дополнительных программных и аппаратных СЗИ.
2. Процедура доступа к данным в современных компьютерных системах.
3. Выбор объекта для доступа. Форма хранения прав доступа субъектов к объектам
4. Средства осуществления доступа к объектам со стороны пользователей
5. Технологии аутентификации.
6. Виды аппаратных идентификаторов, присутствующих на рынке, их характеристики и области применения.
7. Технологии биометрической идентификации пользователей. Области использования различных систем биометрической идентификации
8. Виды аутентификации.
9. Методы аутентификации. Реализация методов аутентификации.
10. Варианты реализации средств аппаратной поддержки механизмов обеспечения ИБ.
11. Рынок решений, использующих механизмы аппаратной поддержки механизмов разграничения доступа.
12. Примеры аппаратных систем разграничения доступа.
13. Недостатки аппаратных СЗИ.
14. Трудности интеграции аппаратных СЗИ в существующие информационные системы
15. Классификация методов защиты программного обеспечения от копирования.
16. Трудности использования средств защиты от копирования.
17. Критерии выбора средств защиты ПО от несанкционированного копирования
18. Защита программ от изучения.
19. Последствия взлома программного обеспечения.
20. Методы противодействия изучению и отладке программного обеспечения
21. Классификация деструктивных программные воздействия по методам реализации угроз безопасности.

22. Классификация разработчиков деструктивного программного обеспечения.
23. Классификация компьютерных вирусов.
24. Классификация программ-шпионов.
25. Классификация разработчиков деструктивного программного обеспечения

Шкала оценивания

Оценка результатов производится на основе Положения о текущем контроле успеваемости обучающихся и промежуточной аттестации обегающихся по образовательным программам среднего профессионального и высшего образования в федеральном государственном бюджетном образовательном учреждении высшего образования «Российская академии народною хозяйства и государственной службы при Президенте Российской Федерации», утвержденного Приказом Ректора РАНХиГС при Президенте РФ от 30.01.2018 г. № 02-66 (п.10 раздела 3 (первый абзац) и п.11), а также Решения Ученого совета Северо-западного института управления РАНХиГС при Президенте РФ от 19.06.2018, протокол № 11.

Зачет

На «зачтено» оцениваются ответ, в котором системно, логично и последовательно изложен материал на все поставленные вопросы. Кроме того, студент должен показать способность делать самостоятельные выводы, комментировать излагаемый материал. При этом допускаются некоторые затруднения с ответами, например, затруднения с примерами из практики, затруднения с ответами на дополнительные вопросы.

«Не зачтено» ставится в случае, когда студент не знает значительной части учебного материала, допускает существенные ошибки; знания носят бессистемный характер; на большинство дополнительных вопросов даны ошибочные ответы; ответ дается не по вопросу.

6. Методические материалы для обучающихся по освоению дисциплины

Рабочей программой дисциплины предусмотрены следующие виды аудиторных занятий: лекции, практические занятия. На лекциях рассматриваются наиболее сложный материал дисциплины. На лекциях рассматривается наиболее сложный материал дисциплины. Лекция сопровождается презентациями, компьютерными текстами лекции, что позволяет магистранту самостоятельно работать над повторением и закреплением лекционного материала. Для этого магистранту должно быть предоставлено право самостоятельно работать в компьютерных классах в сети Интернет. Кроме того, часть теоретического материала предоставляется на самостоятельное изучение по рекомендованным источникам для формирования навыка самообучения.

Практические занятия предназначены для самостоятельной работы магистрантов по решению конкретных задач. Каждое практическое занятие сопровождается заданиями, выдаваемыми магистрантам для решения во внеаудиторное время. Для оказания помощи в решении задач имеются тексты практических заданий с условиями задач и вариантами их решения.

Для работы с печатными и электронными ресурсами СЗИУ имеется возможность доступа к электронным ресурсам. Организация работы магистрантов с электронной библиотекой указана на сайте института (странице сайта – «Научная библиотека»).

7. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

7.1. Основная литература

1. Баранова Е. К. Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с. - (Высшее образование) ISBN 978-5-369-01450-9 - Режим доступа http://znanium.com/bookread2.php?book=495249
2. М. А. Борисов, И. В. Заводцев, И. В. Чижов. Основы программно-аппаратной защиты информации. Издание четвертое, переработанное и дополненное. Учебное пособие. – М.: URSS, 2015 г. -412 с.
3. Жук А. П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.: http://znanium.com/bookread.php?book=474838 Электронный ресурс
4. Казарин О.В., Забабурин А.С. Программно-аппаратные средства защиты информации. Защита программного обеспечения. Учебник и практикум для вузов (серия специалист), 312 с. 2017 г.
5. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с. ISBN 978-5-8199-0331-5 - Режим доступа: http://znanium.com/catalog/product/423927

7.2. Дополнительная литература

1. Безопасность и управление доступом в информационных системах: Учебное пособие / А.В. Васильков, И.А. Васильков. - М.: Форум: НИЦ ИНФРА-М, 2013. - 368 с. - Режим доступа: http://znanium.com/bookread2.php?book=405313
2. Девянин П.Н., Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс] : Учебное пособие для вузов / Девянин П.Н. - 2-е изд., испр. и доп. - М. : Горячая линия - Телеком, 2013. - 338 с. - ISBN 978-5-9912-0328-9 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991203289.html
3. Информационная безопасность конструкций ЭВМ и систем: учебное пособие / Е.В. Глинская, Н.В. Чичварин. - М.: НИЦ ИНФРА-М, 2016. - 118 с. - Режим доступа: http://znanium.com/bookread2.php?book=507334
4. Котухов М. М. Комплексное обеспечение информационной безопасности автоматизированных систем. Курс лекций. Электронное издание.-М.: РАНХ и ГС при Президенте РФ, 2015 г.
5. Партыка Т. Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с. http://znanium.com/bookrea,d.php?book=420047 Электронный ресурс
6. Нестеров С. А. Информационная безопасность. Учебник и практикум. – М.: Юрайт. 2017 г. 322 с.

7.3. Нормативные правовые документы и иная правовая информация

Не используются.

7.4. Интернет-ресурсы

1. Электронно-образовательные ресурсы на сайте научной библиотеки СЗИУ РАНХиГС (http://nwipa.ru)

2. Электронные учебники электронно-библиотечной системы (ЭБС) «Айбукс» http://www.nwapa.spb.ru/index.php?page_id=76
3. Электронные учебники электронно-библиотечной системы (ЭБС) «Лань» http://www.nwapa.spb.ru/index.php?page_id=76
4. Электронные учебники электронно-библиотечной системы (ЭБС) «IPRbooks» http://www.nwapa.spb.ru/index.php?page_id=76
5. Электронные учебники электронно-библиотечной системы (ЭБС) «Юрайт»
6. Сайт лаборатории радиосистем (кафедра радиофизики) - http://radiosys.ksu.ru
7. Электронные книги по криптографии - http://www.knigka.info/kriptograf/

7.5. Иные источники.

Не используются.

8. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

Учебная дисциплина включает использование программного обеспечения Microsoft Office для подготовки текстового и табличного материала, выполнения заданий.

Интернет-сервисы и электронные ресурсы (поисковые системы, электронная почта, профессиональные тематические чаты и форумы, системы аудио и видео конференций, онлайн энциклопедии, справочники, библиотеки, электронные учебные и учебно-методические материалы).

Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

№ п/п	Наименование
	Компьютерные классы с персональными ЭВМ, объединенными в локальные сети с выходом в Интернет
	Мультимедийные средства в каждом компьютерном классе и в лекционной аудитории
	Браузер, сетевые коммуникационные средства для выхода в Интернет

Компьютерные классы из расчета ПК для одного обучающегося. Каждому обучающемуся должна быть предоставлена возможность доступа к сетям типа Интернет в течение не менее 20% времени, отведенного на самостоятельную подготовку.