Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Шебзухова Татьяна Александровна
Должность: Директор Пятигорского института (филиал) Северо-Кавказского федерального университета
Дата подписания: 06.10.2023 14:55:47
Уникальный программный ключ:
d74ce93cd40e39275c3ba2f58486412a1de8ef96

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

Методические указания

по выполнению практических работ
по дисциплине «Информационная безопасность в сфере экономической безопасности»
для студентов специальности:
38.05.01 Экономическая безопасность
Специализация:
«Финансово-экономическое обеспечение федеральных государственных органов, обеспечивающих безопасность Российской федерации»

Пятигорск
2021

Содержание

Введение

Программа дисциплины «Информационная безопасность в сфере экономической безопасности» предназначена для студентов специальности 38.05.01 «Экономическая безопасность».

Цель изучения дисциплины «Информационная безопасность», изучение комплекса проблем информационной безопасности предпринимательских структур различных типов и направлений деятельности, построения, функционирования и совершенствования правовых, организационных, технических и технологических процессов, обеспечивающих информационную безопасность и формирующих структуру системы защиты ценной и конфиденциальной информации в сферах охраны интеллектуальной собственности предпринимателей и сохранности, их информационных ресурсов.

Поэтому основными задачами изучения дисциплины являются:

- формирование знаний о концепциях защиты информации и системах безопасности персональных компьютеров и компьютерных сетей;
-изучить теорию и практику новейших достижений и перспектив в развития в области создания систем безопасности локальных вычислительных сетей и сети Internet;
- формирование знаний о криптографических методах зашиты информации; основах криптографии; основных методах и приемах защиты от несанкционированного доступа; о компьютерных вирусах и антивирусных программах; организационно-правовом обеспечение ИБ;
- развитие способности работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации;
- овладение способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности;
- формирование навыков выбора инструментальных средств для обработки финансовой, бухгалтерской и иной экономической информации и умения обосновывать свой выбор.

ОПИСАНИЕ ПРАКТИЧКСКИХ РАБОТ

Практическое занятие №1,2

Тема: Основные понятия теории информационной безопасности

Цель работы: изучить основные понятия теории информационной безопасности

Знания: содержание базовых определений и понятий, проблемы информационной безопасности;

Умения: ориентироваться в области информационной безопасности, пользоваться специальной литературой в изучаемой предметной области;.

Актуальность темы: Появление персональных ЭВМ, локальных и глобальных сетей, спутниковых каналов связи, эффективной технической разведки и конфиденциальной информации существенно обострило проблему защиты информации. Проблема надежного обеспечения сохранности информации является одной из важнейших проблем современности.

Теоретическая часть: При рассмотрении вопросов информационной безопасности в настоящее время можно выделить два подхода: Неформальный, или описательный. При этом комплекс вопросов построения защищённых систем делится на основные направления, соответствующие угрозам, разрабатывается комплекс мер и механизмов защиты по каждому направлению. Формальный. Основан на понятии политики безопасности и определении способов гарантирования выполнения её положений. Как естественнонаучная дисциплина теория информационной безопасности развивается в направлении формализации и математизации основных положений, выработки комплексных подходов к решению задач защиты информации. Теория информационной безопасности постоянно развивается т.к. в связи с развитием технологий обработки и передачи информации постоянно возникают новые задачи по обеспечению информационной безопасности.

Теория информационной безопасности наука сравнительно молодая. Свое развитие она получила в связи с бурным развитием информационных технологий, радиоэлектроники и связи и необходимостью сохранения информационных ресурсов. Как и любая другая наука, информационная безопасность имеет свой понятийный аппарат, который способен наиболее точно охарактеризовать все аспекты защиты информации. Многие понятия по своему содержанию соответствуют зарубежным аналогам. В то же время некоторые термины не являются устоявшимися и не всегда точно и полно характеризуют какой-либо процесс, свойство или предмет. Предметной областью информационной безопасности являются: · информация и ее свойства; · угрозы безопасности информации и ее собственникам; · политика безопасности и модели безопасности; · способы, методы и средства защиты информации; · классификация систем защиты; · требования к защищенности информационных систем; · методология оценки защищенности информационных систем и проектирования защиты. · конкретные системы защиты информации, применяемые в различных органах управления, учреждениях и на пред- приятиях различных форм собственности.

Основные термины и определения правовых понятий в изучаемой области установлены в Федеральном законе «Об информации, информационных технологиях и о защите информации». В нем сформулировано понятие информации и информационных технологий, определены субъекты информационных отношений и защиты.

Задание:

1. Проанализируйте историю становления теории информационной безопасности
2. Охарактеризуйте средства реализации комплексной защиты информации.

Контрольные вопросы:

1. Предметная область теории информационной безопасности.
2. Систематизация понятий в области защиты информации.
3. Основные термины и определения правовых понятий в области информационных отношений и защиты информации.
4. Понятия предметной области «Защита информации».
5. Основные принципы построения систем защиты.
6. Концепция комплексной защиты информации.
7. Задачи защиты информации.

Список литературы, рекомендуемый к использованию по данной теме:

1.Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — Саратов : Вузовское образование, 2019. — 214 c. — ISBN 978-5-4487-0585-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86938.html

2. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 c. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/87995.html

4. Информационная безопасность : лабораторный практикум / составители Т. Н. Катанова, Л. С. Галкина, Р. А. Жданов. — Пермь : Пермский государственный гуманитарно-педагогический университет, 2018. — 86 c. — ISBN 978-5-85219-007-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86357.html.

4.Басыня, Е. А. Системное администрирование и информационная безопасность : учебное пособие / Е. А. Басыня. — Новосибирск : Новосибирский государственный технический университет, 2018. — 79 c. — ISBN 978-5-7782-3484-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/91423.html

Практическое занятие №3,4

Тема: Информация как объект защиты

Цель работы: изучить информацию как объект защиты

Знания: содержание базовых определений и понятий, проблемы информационной безопасности;

Умения: ориентироваться в области информационной безопасности, пользоваться специальной литературой в изучаемой предметной области;.

Актуальность темы: Степень ценности информации и необходимая надежность ее защиты находятся в прямой зависимости., как составной части системы государственного управления этой важной сферой.

Теоретическая часть: В общем случае информация — это знания в широком значении этого слова. Не только образовательные или научные знания, а сведения и данные, которые присутствуют в любом объекте и необходимы для функционирования любых информационных систем (живых существ или созданных человеком). Информация как объект познания имеет ряд особенностей: · нематериальна по своей природе, отображается в виде символов на носителях; · после записи на носитель информация приобретает определённые параметры и может быть измерена в объеме; · информация, записанная на материальный носитель, может храниться, обрабатываться, передаваться по различным каналам связи; · перемещаясь по линиям связи, информация создает физические поля, которые отражают ее содержание

Можно выделить несколько уровней представления информации: уровень носителей; уровень средств взаимодействия с носителем; логический уровень; синтаксический уровень; семантический уровень.

Информация как объект познания и объект защиты обладает множеством свойств. Перечислим важнейшие из них. Ценность. Как предмет собственности информация имеет определенную ценность. Именно потому, что информация имеет ценность, ее необходимо защищать. Секретность (конфиденциальность) информации — субъективно определяемая характеристика информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации. Эта характеристика обеспечивается способностью системы сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на доступ к ней. Объективные предпосылки подобного ограничения доступности информации для одних субъектов заключены в необходимости защиты законных интересов других субъектов информационных отношений.

Целостность информации — свойство информации существовать в неискаженном виде. Обычно интересует обеспечение более широкого свойства — достоверности информации, которое складывается из адекватности (полноты и точности) отображения состояния предметной области и непосредственно целостности информации, то есть ее неискаженности. Вопросы обеспечения адекватности отображения выходят за рамки проблемы обеспечения информационной безопасности.

Доступность информации — свойство системы, в которой циркулирует информация, обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и готовность к обслуживанию поступающих от субъектов запросов всегда, когда в обращении к ним возникает необходимость.

Концентрация. Суммарное количество информации может оказаться секретным, сводные данные обычно секретнее, чем одиночные.

Рассеяние. Ценная информация может быть разделена на части и перемешана с менее ценной с целью маскировки самого факта наличия информации. Примеры использования этого свойства — компьютерная стеганография.

Сжатие. Возможно сжатие без потери информации, например архивирование. Для уменьшения объема информации или увеличения пропускной способности канала передачи информации применяется сжатие с частичной потерей (например, сжатие в графических форматах типа jpg). Используется также необратимое сжатие (например, алгоритм электронно-цифровой подписи (ЭЦП), одностороннее ХЭШ-преобразование).

Прагматические свойства: важность; полнота (степень уменьшения априорной неопределенности); достоверность; своевременность; целесообразность; соотносимость с фактами, явлениями

Задание:

1. Изобразите схематично структуру и шкалу ценности информации.
2. Проанизируйте правовой режим информационных ресурсов.

Контрольные вопросы:

1. Понятие об информации как объекте защиты.
2. Уровни представления информации.
3. Основные свойства защищаемой информации.
4. Виды и формы представления информации.
5. Информационные ресурсы.
6. Классификация информационных ресурсов.

Список литературы, рекомендуемый к использованию по данной теме:

1.Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — Саратов : Вузовское образование, 2019. — 214 c. — ISBN 978-5-4487-0585-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86938.html

2. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 c. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/87995.html

3. Информационная безопасность : лабораторный практикум / составители Т. Н. Катанова, Л. С. Галкина, Р. А. Жданов. — Пермь : Пермский государственный гуманитарно-педагогический университет, 2018. — 86 c. — ISBN 978-5-85219-007-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86357.html.

4.Басыня, Е. А. Системное администрирование и информационная безопасность : учебное пособие / Е. А. Басыня. — Новосибирск : Новосибирский государственный технический университет, 2018. — 79 c. — ISBN 978-5-7782-3484-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/91423.html

Практическое занятие № 5,6

Тема: Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности

Цель работы: изучить государственную политику информационной безопасности. Концепцию комплексного обеспечения информационной безопасности

Знания: содержание базовых определений и понятий, проблемы информационной безопасности;

Умения: ориентироваться в области информационной безопасности, пользоваться специальной литературой в изучаемой предметной области;.

Актуальность темы: Основы защиты информации разрабатываются органами государственной власти исходя из условий обеспечения информационной безопасности в частности и национальной безопасности России в целом.

Теоретическая часть: Информационная безопасность Российской Федерации (далее в данном разделе — информационная безопасность) — состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

Поскольку в условиях информатизации страны, развития информационных технологий информационные ресурсы формируются во всех сферах деятельности, и в первую очередь в политической, военной, экономической, научно-технической, информационную безопасность следует рассматривать как комплексный показатель национальной безопасности. Этим определяется ее важное место и одна из ведущих ролей в системе национальной безопасности страны в современных условиях.

Обеспечение информационной безопасности осуществляется в рамках обеспечения национальной безопасности. Национальная безопасность достигается проведением единой государственной политики в области обеспечения безопасности, системой мер экономического, политического и иного характера, адекватных угрозам жизненно важных интересов личности, общества и государства. Политика России в области национальной безопасности строится на основе «Стратегии национальной безопасности Российской Федерации», утвержденной Указом Президента Российской Федерации 31.12.2015 № 683.

На основе Стратегии разработана «Доктрина информационной безопасности Российской Федерации», введенная в действие Указом Президента РФ от 05.12.2016 N 646. Доктрина представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере. В Доктрине определены национальные интересы в информационной сфере, введены основные информационные угрозы и состояние информационной безопасности, сформулированы стратегические цели и основные направления обеспечения информационной безопасности, описаны организационные основы обеспечения информационной безопасности.

Законодательную основу обеспечения безопасности составляют:

· Конституция РФ;

· законы и другие нормативные акты РФ, регулирующие отношения в области безопасности; · конституции, законы, нормативные акты республик;

· нормативные акты органов власти и управления краев, областей, принятые в пределах их компетенции; · международные договоры и соглашения, заключенные или признанные РФ;

· основные законы в области защиты информации, прав субъектов, участвующих в информационных процессах и информатизации;

· федеральный закон «О безопасности» № 390-ФЗ от 28.12.2010;

· федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

· федеральный закон от 21.09.93 г. № 182 «О государственной тайне»;

· федеральный закон от 27.07.06 г. №152-ФЗ «О персональных данных»;

· федеральный закон от 27.12.91 г. «О средствах массовой информации»;

· федеральный закон от 6.04.11 г. № 63-ФЗ «Об электронной подписи»;

· Гражданский кодекс РФ (ч. 1, 2. 4);

· Уголовный кодекс РФ.

Помимо правовых документов, в Российской Федерации действуют нормативно-методические документы:

· методические документы государственных органов России: Доктрина информационной безопасности РФ, Руководящие документы ФСТЭК (Гостехкомиссии России), ведомственные приказы;

· стандарты информационной безопасности: международные стандарты, Государственные стандарты РФ, рекомендации по стандартизации, методические указания.

В целом развитие законодательной базы в области информационной безопасности идет по четырем основным направлениям:

· защита сведений, составляющих государственную тайну;

· защита конфиденциальной информации;

· защита авторского права в сфере информатизации;

· защита права на доступ к информации.

Задание:

1. Оцените место информационной безопасности в системе национальной безопасности Российской Федерации

2. Изобразите схематично структуру государственной системы защиты информации

Контрольные вопросы:

1. Информационная безопасность и ее место в системе национальной безопасности Российской Федерации.

2. Органы обеспечения информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность

Список литературы, рекомендуемый к использованию по данной теме:

1.Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — Саратов : Вузовское образование, 2019. — 214 c. — ISBN 978-5-4487-0585-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86938.html

2. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 c. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/87995.html

3. Информационная безопасность : лабораторный практикум / составители Т. Н. Катанова, Л. С. Галкина, Р. А. Жданов. — Пермь : Пермский государственный гуманитарно-педагогический университет, 2018. — 86 c. — ISBN 978-5-85219-007-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86357.html.

4.Басыня, Е. А. Системное администрирование и информационная безопасность : учебное пособие / Е. А. Басыня. — Новосибирск : Новосибирский государственный технический университет, 2018. — 79 c. — ISBN 978-5-7782-3484-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/91423.html

Практическое занятие № 7,8

Тема: Угрозы информационной безопасности

Цель работы: изучить угрозы информационной безопасности

Знания: содержание базовых определений и понятий, проблемы информационной безопасности;

Умения: ориентироваться в области информационной безопасности, пользоваться специальной литературой в изучаемой предметной области; обосновывать выбор средств для решения конкретных задач информационной безопасности; сводить постановки задач на содержательном уровне к формальным и относить их к соответствующим информационным

технологиям; ориентироваться в существующих технологиях информационной безопасности, их возможностях и перспективах развития.

Актуальность темы: При построении системы защиты информации обязательно нужно определить, что следует защищать и от кого (или чего) следует строить защиту

Теоретическая часть: Определение перечня угроз и построение модели нарушителя являются обязательным этапом проектирования системы защиты. Для каждой системы перечень наиболее вероятных угроз безопасности, а также характеристика наиболее вероятного нарушителя индивидуальны, поэтому перечень и модель должны носить неформальный характер.

Защищенность информации обеспечивается только при соответствии предполагаемых угроз и качеств нарушителя реальной обстановке. При наличии в системе уязвимости потенциальная угроза безопасности может реализоваться в виде атаки. Атаки принято классифицировать в зависимости от целей, мотивов, используемого механизма, места в архитектуре системы и местонахождения нарушителя.

Для предупреждения успешных атак необходим поиск и анализ уязвимостей системы. Уязвимости различаются в зависимости от источника возникновения, степени риска, распространенности, места в жизненном цикле системы, соотношения с подсистемами защиты. Анализ уязвимостей — обязательная процедура при аттестации объекта информатизации. В связи с возможностью появления новых уязвимостей необходим их периодический анализ на уже аттестованном объекте.

Угроза — это фактор, стремящийся нарушить работу системы. В настоящее время рассматривается достаточно обширный перечень угроз информационной безопасности, насчитывающий сотни пунктов. Кроме выявления возможных угроз, должен быть проведен анализ этих угроз на основе их классификации по ряду признаков. Каждый из признаков классификации отражает одно из требований к системе защиты. При этом угрозы, соответствующие каждому признаку классификации, позволяют уточнить требования.

Соответственно для информационных систем было предложено рассматривать три основных вида угроз:

· Угроза нарушения конфиденциальности реализуется в том случае, если информация становится известной лицу, не располагающему полномочиями доступа к ней. Угроза нарушения конфиденциальности имеет место всякий раз, когда получен доступ к некоторой секретной информации, хранящейся в информационной системе или передаваемой от одной системы к другой. Иногда в связи с угрозой нарушения конфиденциальности используется термин «утечка».

· Угроза нарушения целостности реализуется при несанкционированном изменении информации, хранящейся в ин- формационной системе или передаваемой из одной системы в другую. Когда злоумышленники преднамеренно изменяют информацию, говорится, что целостность информации нарушена. Целостность также будет нарушена, если к несанкционированному изменению приводит случайная ошибка программного или аппаратного обеспечения. Санкционированными изменениями являются те, которые сделаны уполномоченными лицами с обоснованной целью (например, санкционированным изменением является периодическая запланированная коррекция некоторой базы данных).

· Угроза нарушения доступности (отказа служб) реализуется, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислитель- ной системы. Блокирование может быть постоянным — запрашиваемый ресурс никогда не будет получен, или может вызывать только задержку запрашиваемого ресурса.

Задание:

1. Определите перечень основных угроз для АС, состоящей из автономно работающего компьютера без выхода в сеть, расположенной в одной из лабораторий университета.
2. Постройте неформальную модель нарушителя для учебной компьютерной лаборатории.
3. Выведите формулу для расчета прочности трехуровневой защитной оболочки.

4. Охарактеризуйте защитные оболочки и перечень преград, применяемые в учебной компьютерной лаборатории.

Контрольные вопросы:

1. Анализ уязвимостей системы.
2. Классификация угроз информационной безопасности.
3. Основные направления и методы реализации угроз.
4. Неформальная модель нарушителя.
5. Оценка уязвимости системы.

Список литературы, рекомендуемый к использованию по данной теме:

1.Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — Саратов : Вузовское образование, 2019. — 214 c. — ISBN 978-5-4487-0585-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86938.html

2. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 c. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/87995.html

3. Информационная безопасность : лабораторный практикум / составители Т. Н. Катанова, Л. С. Галкина, Р. А. Жданов. — Пермь : Пермский государственный гуманитарно-педагогический университет, 2018. — 86 c. — ISBN 978-5-85219-007-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86357.html.

4.Басыня, Е. А. Системное администрирование и информационная безопасность : учебное пособие / Е. А. Басыня. — Новосибирск : Новосибирский государственный технический университет, 2018. — 79 c. — ISBN 978-5-7782-3484-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/91423.html

Практическое занятие №9,10.

Тема: Построение систем защиты от угрозы нарушения конфиденциальности

Цель работы: изучить принцип построения систем защиты от угрозы нарушения конфиденциальности

Знания: содержание структур, назначений, особенностей и краткой характеристики функциональных возможностей различных технологий информационной безопасности, организационно-технических, законодательных, программно-аппаратных, математических и т.п. средств их реализации; современное состояние и развитие методов и средств информационной безопасности, методику их применения для решения задач практических задач различного уровня.

Умения: ориентироваться в области информационной безопасности, пользоваться специальной литературой в изучаемой предметной области; обосновывать выбор средств для решения конкретных задач информационной безопасности; сводить постановки задач на содержательном уровне к формальным и относить их к соответствующим информационным технологиям; ориентироваться в существующих технологиях информационной безопасности, их возможностях и перспективах развития.

Актуальность темы: Целью определения угроз безопасности информации является установление того, существует ли возможность нарушения конфиденциальности, целостности или доступности информации, содержащейся в информационной системе, и приведет ли нарушение хотя бы одного из указанных свойств безопасности информации к наступлению неприемлемых негативных последствий (ущерба) для обладателя информации или оператора, а в случае обработки персональных данных и для субъектов персональных данных.

Теоретическая часть: В соответствии с определением несанкционированный доступ является одним из видов утечки информации. Как уже было сказано выше, несанкционированным доступом к информации (НСД), согласно руководящим документам Гостехкомиссии, является

доступ к информации, нарушающий установленные правила разграничения доступа. НСД может носить случайный или преднамеренный характер. В результате НСД чаще всего реализуется угроза конфиденциальности информации, однако целью злоумышленника может быть и реализация других видов угроз (целостности информации, раскрытия параметров системы).

Для преднамеренного НСД используются как общедоступные, так и скрытые способы и средства. Такими способами являются:

· инициативное сотрудничество (предательство);

· склонение к сотрудничеству (подкуп, шантаж);

· подслушивание переговоров самыми различными путями;

· негласное ознакомление со сведениями, составляющими тайну;

· хищение, копирование, подделка, уничтожение;

· незаконное подключение к каналам и линиям связи и передачи данных;

· перехват (акустический или радиоперехват, в том числе и за счет побочных электромагнитных излучений и наводок);

· визуальное наблюдение, фотографирование;

· сбор и аналитическая обработка детальной информации или производственных отходов.

К основным способам НСД в информационных системах относятся:

· непосредственное обращение к объектам доступа;

· создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;

· модификация средств защиты, позволяющая осуществить НСД;

· внедрение в технические средства информационной системы программных или технических механизмов, нарушающих предполагаемую структуру и функции системы и позволяющих осуществить НСД.

Зная совокупность источников информации, возможные каналы утечки охраняемых сведений и многообразие способов несанкционированного доступа к источникам, можно приступать к выработке мероприятий по защите.

Задание:

1. Выявите основные направления и цели использования криптографических методов.
2. Охарактеризуйте основные способы несанкционированного доступа

Контрольные вопросы:

1. Определение и основные способы несанкционированного доступа.
2. Методы защиты от НСД.
3. Организационные методы защиты от НСД.
4. Инженерно-технические методы защиты от НСД.
5. Построение систем защиты от угрозы утечки по техническим каналам.
6. Идентификация и аутентификация.
7. Защита от угрозы нарушения конфиденциальности на уровне содержания информации.

Список литературы, рекомендуемый к использованию по данной теме:

1.Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — Саратов : Вузовское образование, 2019. — 214 c. — ISBN 978-5-4487-0585-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86938.html

2. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 c. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/87995.html

3. Информационная безопасность : лабораторный практикум / составители Т. Н. Катанова, Л. С. Галкина, Р. А. Жданов. — Пермь : Пермский государственный гуманитарно-педагогический университет, 2018. — 86 c. — ISBN 978-5-85219-007-9. — Текст :

электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86357.html.
4.Басыня, Е. А. Системное администрирование и информационная безопасность : учебное пособие / Е. А. Басыня. — Новосибирск : Новосибирский государственный технический университет, 2018. — 79 с. — ISBN 978-5-7782-3484-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/91423.html

Практическое занятие №11,12

Тема: Построение систем защиты от угрозы нарушения целостности информации и отказа доступа

Цель работы: изучить принцип построения систем защиты от угрозы нарушения целостности информации и отказа доступа

Знания: содержание структур, назначений, особенностей и краткой характеристики функциональных возможностей различных технологий информационной безопасности, организационно-технических, законодательных, программно-аппаратных, математических и т.п. средств их реализации; современное состояние и развитие методов и средств информационной безопасности, методику их применения для решения задач практических задач различного уровня.

Умения: ориентироваться в области информационной безопасности, пользоваться специальной литературой в изучаемой предметной области; обосновывать выбор средств для решения конкретных задач информационной безопасности; сводить постановки задач на содержательном уровне к формальным и относить их к соответствующим информационным технологиям; ориентироваться в существующих технологиях информационной безопасности, их возможностях и перспективах развития.

Актуальность темы: Страна происхождения товара является инструментом не только экономического, но и политического воздействия. В зависимости от страны происхождения товарам могут предоставляться тарифные преференции, то есть могут создаваться условия повышения или понижения конкурентоспособности импортного товара.

Теоретическая часть: В информационной системе основное место хранения информации — электронные носители, поэтому рассмотрим меры защиты применительно к этому классу носителей. Определяя порядок хранения информации на электронных носителях, следует иметь в виду, что от состояния носителей зависит качество программ и защищаемых данных. Электронные носители являются утройствами, подвергаюшимися интенсивному износу. Кроме того, в электронные носители могут быть внедрены закладки, поэтому используемые методы записи, хранения и считывания нельзя считать защищенными.

Организационно-технологические меры защиты целостности информации на электронных носителях можно разделить на две основные группы: · организационные меры по поддержке целостности информации; · технологические меры контроля целостности битовых последовательностей.

При рассмотрении вопроса целостности данных при обработке используется интегрированный подход, основанный на ряде работ Д. Кларка и Д. Вилсона, а также их последователей и оппонентов и включающий в себя девять теоретических принципов:

· корректность транзакций;
· аутентификация пользователей;
· минимизация привилегий;
· разграничение функциональных обязанностей;
· аудит произошедших событий;
· объективный контроль;
· управление передачей привилегий;
· обеспечение непрерывной работоспособности;
· простота использования защитных механизмов

Средства контроля целостности должны обеспечивать защиту от несанкционированного изменения информации нарушителем при ее передаче по каналам

связи. При транспортировке информации следует защищать как целостность, так и подлинность информации. Схема контроля целостности данных подразумевает выполнение двумя сторонами — источником и приемником — некоторых (возможно, разных) криптографических преобразований данных. Источник преобразует исходные данные и передает их приемнику вместе с некоторым приложением, обеспечивающим избыточность шифрограммы. Приемник обрабатывает полученное сообщение, отделяет приложение от основного текста и проверяет их взаимное соответствие, осуществляя таким образом контроль целостности. Контроль целостности может выполняться с восстановлением или без восстановления исходных данных.

Задание:

1. Проведите сравнительный анализ обычной и цифровой подписей
2. Составьте схему контроля целостности данных при транспортировке

Контрольные вопросы:

1. Защита целостности информации при хранении.
2. Защита целостности информации при обработке.
3. Защита целостности информации при транспортировке.
4. Защита от угрозы нарушения целостности информации на уровне содержания.
5. Построение систем защиты от угрозы отказа доступа к информации.
6. Защита семантического анализа и актуальности информации.

Список литературы, рекомендуемый к использованию по данной теме:

1.Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — Саратов : Вузовское образование, 2019. — 214 c. — ISBN 978-5-4487-0585-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86938.html

2. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 c. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/87995.html

3. Информационная безопасность : лабораторный практикум / составители Т. Н. Катанова, Л. С. Галкина, Р. А. Жданов. — Пермь : Пермский государственный гуманитарно-педагогический университет, 2018. — 86 c. — ISBN 978-5-85219-007-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86357.html.

4.Басыня, Е. А. Системное администрирование и информационная безопасность : учебное пособие / Е. А. Басыня. — Новосибирск : Новосибирский государственный технический университет, 2018. — 79 c. — ISBN 978-5-7782-3484-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/91423.html

Практическое занятие №13,14

Тема: Политика и модели безопасности

Цель работы: изучить политику и модели безопасности

Знания: содержание структур, назначений, особенностей и краткой характеристики функциональных возможностей различных технологий информационной безопасности, организационно-технических, законодательных, программно-аппаратных, математических и т.п. средств их реализации; современное состояние и развитие методов и средств информационной безопасности, методику их применения для решения задач практических задач различного уровня. Состав и функциональные возможности инструментальных средств и информационных технологий обработки информации для решения профессиональных задач экономической безопасности

Умения: ориентироваться в области информационной безопасности, пользоваться специальной литературой в изучаемой предметной области; обосновывать выбор средств для решения конкретных задач информационной безопасности; сводить постановки задач на

содержательном уровне к формальным и относить их к соответствующим информационным технологиям; ориентироваться в существующих технологиях информационной безопасности, их возможностях и перспективах развития. Выявлять угрозы информационной безопасности на основе инструментальной обработки финансовой, бухгалтерской и иной экономической информации;

Актуальность темы: Технология защиты информационных систем начала развиваться относительно недавно, но уже сегодня существует значительное число теоретических моделей, позволяющих описывать различные аспекты безопасности и обеспечивать средства защиты с формальной стороны

Теоретическая часть: Под политикой безопасности понимается совокупность норм и правил, регламентирующих процесс обработки информации, выполнение которых обеспечивает защиту от определенного множества угроз и составляет необходимое условие безопасности системы. Формальное выражение политики безопасности называют моделью безопасности. Основная цель создания политики безопасности — это определение условий, которым должно подчиняться поведение системы, выработка критерия безопасности и проведение формального доказательства соответствия системы этому критерию при соблюдении установленных правил и ограничений. Кроме того, модели безопасности позволяют решить еще целый ряд задач, возникающих в ходе проектирования, разработки и сертификации защищенных систем, поэтому их используют не только теоретики информационной безопасности, но и другие категории специалистов, участвующих в процессе создания и эксплуатации защищенных информационных систем.

Модели безопасности обеспечивают системотехнический подход, включающий решение следующих задач:

· выбор и обоснование базовых принципов архитектуры защищенных систем, определяющих механизмы реализации средств и методов защиты информации;

· подтверждение свойства защищенности разрабатываемых систем путем формального доказательства соблюдения политики безопасности;

· составление формальной спецификации политики безопасности как важнейшей составной части организационного и документационного обеспечения разрабатываемых защищенных систем.

Производители защищенных информационных систем используют модели безопасности в следующих случаях:

· при составлении формальной спецификации политики безопасности разрабатываемой системы;

· при выборе и обосновании базовых принципов архитектуры защищенной системы, определяющих механизмы реализации средств защиты; · в процессе анализа безопасности системы, при этом модель используется в качестве эталонной модели;

· при подтверждении свойств разрабатываемой системы путем формального доказательства соблюдения политики безопасности.

Потребители путем составления формальных моделей без- опасности получают возможность довести до сведения производителей свои требования, а также оценить соответствие защищенных систем своим потребностям. Эксперты в ходе анализа адекватности реализации политики безопасности в защищенных системах используют модели безопасности в качестве эталонов. По сути, модели безопасности являются связующим элементом между производителями, потребителями и экспертами

Задание:

1. Составьте матрицу доступа и граф доступа для организации документооборота факультета (объекты доступа: экзаменационные ведомости, персональные данные студентов, рабочие программы дисциплин; субъекты доступа: студенты, преподаватели, декан).
2. Оцените роль моделей разграничения доступа в теории информационной безопасности
3. Выявите основные достоинства и недостатки дискреционных моделей
4. Приведите примеры использования дискреционных моделей разграничения доступа.

Контрольные вопросы:

1. Политика безопасности.
2. Субъектно-объектные модели разграничения доступа.
3. Аксиомы политики безопасности.
4. Политика и модели дискреционного доступа.
5. Парольные системы разграничения доступа.
6. Политика и модели мандатного доступа.
7. Теоретико-информационные модели.
8. Политика и модели тематического разграничения доступа.
9. Ролевая модель безопасности.

Список литературы, рекомендуемый к использованию по данной теме:

1.Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — Саратов : Вузовское образование, 2019. — 214 c. — ISBN 978-5-4487-0585-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86938.html

2. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 c. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/87995.html

3. Информационная безопасность : лабораторный практикум / составители Т. Н. Катанова, Л. С. Галкина, Р. А. Жданов. — Пермь : Пермский государственный гуманитарно-педагогический университет, 2018. — 86 c. — ISBN 978-5-85219-007-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86357.html.

4.Басыня, Е. А. Системное администрирование и информационная безопасность : учебное пособие / Е. А. Басыня. — Новосибирск : Новосибирский государственный технический университет, 2018. — 79 c. — ISBN 978-5-7782-3484-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/91423.html

Практическое занятие №15,16

Тема: Обзор международных стандартов информационной безопасности

Цель работы: изучить международные стандарты информационной безопасности

Знания: современное состояние и развитие методов и средств информационной безопасности, методику их применения для решения задач практических задач различного уровня. Состав и функциональные возможности инструментальных средств и информационных технологий обработки информации для решения профессиональных задач экономической безопасности

Умения: ориентироваться в области информационной безопасности, пользоваться специальной литературой в изучаемой предметной области; обосновывать выбор средств для решения конкретных задач информационной безопасности; сводить постановки задач на содержательном уровне к формальным и относить их к соответствующим информационным технологиям; ориентироваться в существующих технологиях информационной безопасности, их возможностях и перспективах развития. Выявлять угрозы информационной безопасности на основе инструментальной обработки финансовой, бухгалтерской и иной экономической информации;

Актуальность темы: С развитием информационных технологий появилась необходимость стандартизации требований в области защиты информации.

Теоретическая часть: Главная задача стандартов ин- формационной безопасности — создать основу для взаимодействия между производителями, потребителями и специалистам по сертификации. Каждая из этих групп имеет свои интересы и свои взгляды на проблему информационной безопасности. Производители нуждаются в стандартах как средстве сравнения возможностей своих продуктов, и в применении процедуры сертификации как механизме оценки их свойств, а также в стандартизации определенного набора требований безопасности, который мог бы ограничить фантазию заказчика конкретного продукта и заставить его выбирать требования из этого набора. Потребители заинтересованы в методике,

позволяющей обоснованно выбрать продукт, отвечающий их нуждам и решающий их проблемы, для чего им необходима шкала оценки без- опасности и инструмент, с помощью которого они могли бы формулировать свои требования производителям.

Специалисты по сертификации рассматривают стандарты как инструмент, позволяющий им оценить уровень безопасности, обеспечиваемый системой, и предоставить потребителям возможность сделать обоснованный выбор. Специалисты по сертификации заинтересованы в четких и простых критериях, так как они должны дать обоснованный ответ пользователям — удовлетворяет продукт их нужды, или нет. В конечном счете именно они принимают на себя ответственность за безопасность продукта, получившего квалификацию уровня безопасности и прошедшего сертификацию. Таким образом, перед стандартами информационной безопасности стоит непростая задача создать эффективный механизм взаимодействия всех сторон.

«Критерии безопасности компьютерных систем» (Trusted Computer System Evaluation Criteria), получившие неформальное название Оранжевая книга, были разработаны Министерством обороны США в 1983 году с целью определения требований безопасности, предъявляемых к аппаратному, программному и специальному обеспечению компьютерных систем, и выработки соответствующей методологии и технологии анализа степени поддержки политики безопасности в компьютерных системах военного назначения. В данном документе были впервые нормативно определены такие понятия, как «политика безопасности», «ядро безопасности» (TCB) и т.д.. Предложенные в этом документе концепции защиты и на- бор функциональных требований послужили основой для формирования всех появившихся впоследствии стандартов безопасности.

Задание:

1. Опишите структуру Общих критериев безопасности информационных технологий.
2. Опишите технологию применения Общих критериев безопасности информационных технологий.

Контрольные вопросы:

1. Роль стандартов информационной безопасности.
2. Критерии безопасности компьютерных систем министерства обороны США (Оранжевая книга), TCSEC.
3. Европейские критерии безопасности информационных технологий (ITSEC).
4. Федеральные критерии безопасности информационных технологий США.
5. Единые критерии безопасности информационных технологий.
6. Группа международных стандартов 270000.

Список литературы, рекомендуемый к использованию по данной теме:

1.Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — Саратов : Вузовское образование, 2019. — 214 c. — ISBN 978-5-4487-0585-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86938.html

2. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 c. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/87995.html

3. Информационная безопасность : лабораторный практикум / составители Т. Н. Катанова, Л. С. Галкина, Р. А. Жданов. — Пермь : Пермский государственный гуманитарно-педагогический университет, 2018. — 86 c. — ISBN 978-5-85219-007-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86357.html.

4.Басыня, Е. А. Системное администрирование и информационная безопасность : учебное пособие / Е. А. Басыня. — Новосибирск : Новосибирский государственный технический университет, 2018. — 79 c. — ISBN 978-5-7782-3484-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/91423.html

Практическое занятие №17,18

Тема: Информационные войны и информационное противоборство

Цель работы: изучить новых формы борьбы, получивших название «информационная война», «информационное противоборство», «информационное воздействие»

Знания: современное состояние и развитие методов и средств информационной безопасности, методику их применения для решения задач практических задач различного уровня. Состав и функциональные возможности инструментальных средств и информационных технологий обработки информации для решения профессиональных задач экономической безопасности

Умения: ориентироваться в области информационной безопасности, пользоваться специальной литературой в изучаемой предметной области; обосновывать выбор средств для решения конкретных задач информационной безопасности; сводить постановки задач на содержательном уровне к формальным и относить их к соответствующим информационным технологиям; ориентироваться в существующих технологиях информационной безопасности, их возможностях и перспективах развития. Выявлять угрозы информационной безопасности на основе инструментальной обработки финансовой, бухгалтерской и иной экономической информации;

Актуальность темы: развитие информационных технологий ведет к появлению качественно новых форм борьбы, получивших название «информационная война», «информационное противоборство», «информационное воздействие»

Теоретическая часть: Информационная война — открытые или скрытые целенаправленные информационные воздействия систем друг на друга с целью получения определенного выигрыша в материальной, военной, политической или идеологической сферах

В зависимости от масштабов информационные войны делятся:

· на персональные,

· корпоративные,

· глобальные.

Персональные информационные войны чаще всего связаны с нарушением личной информационной неприкосновенности. Корпоративные информационные войны возникают вследствие соперничества между корпорациями и нацелены на получение информации о деятельности конкурента или его ликвидацию. Во время глобальной информационной войны наносится ущерб информационным ресурсам противника при одновременной защите своих на уровне государства.

При глобальной информационной войне можно выделить три основных направления ведения войны:

· воздействие на индивидуальное, групповое и массовое сознание с использованием СМИ;

· воздействие на системы принятия решений в политической, экономической, военной, научно-технической, социальной сферах;

· воздействие на информационные системы с целью управления, блокирования, съема обрабатываемой информации.

В информационно-технической борьбе главными объектами нападения и защиты являются системы управления и связи, телекоммуникационные системы, различные радиоэлектронные средства. Понятие «информационное оружие», получившее широкое распространение после завершения военной операции против Ирака в 1991 г., сформировалось как раз в результате появления средств ведения информационно-технической борьбы. Решающий вклад в поражение Ирака внесло комплексное применение средств разведки, управления, связи, навигации и радиоэлектронной борьбы, совокупность которых и была определена как информационное оружие театра военных действий. Опыт локальных войн конца XX в. свидетельствует о том, что обязательным атрибутом победы в современном бою является завоевание превосходства в информационной сфере. В военное время ведение информационной войны предполагается на стратегическом, оперативном и тактическом уровнях. Но ин- формационное оружие необходимо задействовать еще до начала боевых действий, а в полной мере применять уже в ходе сражений. Еще в мирное время объектами и

целями этой борьбы являются информационные ресурсы государства, в которые включается прежде всего информация, существующая на материальных носителях или в любой другой форме. Особое значение информационных ресурсов обусловлено тем ключевым положением, которое они в силу особой роли информации как системообразующего фактора занимают по отношению к любым другим ресурсам государства — экономическим, научно- техническим и собственно военным.

Задание:

1. Проведите сравнительный анализ «информационной войны» и «информационного противоборства»
2. Составьте схему ведения информационной войны
3. Приведите пример межкорпоративной информационной войны.
5. Выявите особенности информационно-психологической войны

Контрольные вопросы:

1. Определение и основные виды информационных войн.
2. Информационно-техническая война.
3. Информационно-психологическая война.

Список литературы, рекомендуемый к использованию по данной теме:

1.Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — Саратов : Вузовское образование, 2019. — 214 c. — ISBN 978-5-4487-0585-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86938.html

2. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 c. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/87995.html

3. Информационная безопасность : лабораторный практикум / составители Т. Н. Катанова, Л. С. Галкина, Р. А. Жданов. — Пермь : Пермский государственный гуманитарно-педагогический университет, 2018. — 86 c. — ISBN 978-5-85219-007-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86357.html.

4.Басыня, Е. А. Системное администрирование и информационная безопасность : учебное пособие / Е. А. Басыня. — Новосибирск : Новосибирский государственный технический университет, 2018. — 79 c. — ISBN 978-5-7782-3484-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/91423.html

Рекомендуемая литература

Основная литература:

1.Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — Саратов : Вузовское образование, 2019. — 214 c. — ISBN 978-5-4487-0585-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86938.html

2. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 c. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/87995.html

Дополнительная литература:

1. Информационная безопасность : лабораторный практикум / составители Т. Н. Катанова, Л. С. Галкина, Р. А. Жданов. — Пермь : Пермский государственный гуманитарно-педагогический университет, 2018. — 86 c. — ISBN 978-5-85219-007-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86357.html.

2.Басыня, Е. А. Системное администрирование и информационная безопасность : учебное пособие / Е. А. Басыня. — Новосибирск : Новосибирский государственный технический университет, 2018. — 79 с. — ISBN 978-5-7782-3484-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/91423.html