Министерство науки и высшего образования РФ
ФГБОУ ВО «Ульяновский государственный университет»
Факультет математики, информационных и авиационных технологий

Иванцов А.М.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО ДИСЦИПЛИНЕ «ГУМАНИТАРНЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Для студентов специалитета по специальности 10.05.01
очной формы обучения

Ульяновск, 2020

Методические указания для самостоятельной работы студентов по дисциплине «Гуманитарные аспекты информационной безопасности» / составитель: А.М. Иванцов. - Ульяновск: УлГУ, 2020. Настоящие методические указания предназначены для студентов специалитета по специальности 10.05.01 очной формы обучения. В работе приведены литература по дисциплине, основные темы курса и вопросы в рамках каждой темы, рекомендации по изучению теоретического материала, контрольные вопросы для самоконтроля и тесты для самостоятельной работы. Студентам очной формы обучения они будут полезны при подготовке к зачёту по данной дисциплине.

Рекомендованы к введению в образовательный процесс Ученым советом факультета математики, информационных и авиационных технологий УлГУ (протокол № 6/20 от 22.09.2020 г.).

Содержание

1. ЛИТЕРАТУРА ДЛЯ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

1. Малюк А.А., Защита информации в информационном обществе [Электронный ресурс]: Учебное пособие для вузов. / А.А. Малюк - М.: Горячая линия - Телеком, 2015. - 230 с. - ISBN 978-5-9912-0481-1 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991204811.html.

2. Малюк А.А., Теория защиты информации [Электронный ресурс] / Малюк А.А. - М.: Горячая линия - Телеком, 2012. - 184 с. - ISBN 978-5-9912-0246-6 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991202466.html.

3. ГОСТ-Эксперт - единая база ГОСТов Российской Федерации для образования и промышленности:

3.1 ГОСТ Р ИСО 9000-2001. Системы менеджмента качества. Основные положения и словарь;

3.2 ГОСТ Р ИСО/МЭК 27001—2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». М.: Стандартинформ, 2008.

3.3 ГОСТ Р ИСО/МЭК 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности». - М.: Стандартинформ, 2009.

3.4 ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента.

3.5. ГОСТ Р 53647.1-2009 «Менеджмент непрерывности бизнеса. Часть 1. Практическое руководство». М.: Стандартинформ, 2011.

3.6 ГОСТ Р 53647.2-2009 «Менеджмент непрерывности бизнеса. Часть 2. Требования». М.: Стандартинформ, 2011.

3.7 ГОСТ Р 53647.3-2010 «Менеджмент непрерывности бизнеса. Часть 3. Руководство по внедрению». М.: Стандартинформ, 2011.

4. Дронов В.Ю., Международные и отечественные стандарты по информационной безопасности [Электронный ресурс]: Дронов В.Ю. - Новосибирск: Изд-во НГТУ, 2016. - 34 с. - ISBN 978-5-7782-3112-2 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785778231122.html.

5. Некоммерческая интернет-версия СПС "КонсультантПлюс":

5.1 Доктрина информационной безопасности Российской Федерации (Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации")
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_208191/

5.2 Стратегия национальной безопасности Российской Федерации (Указ Президента Российской Федерации от 31 декабря 2015 года N 683 "О Стратегии национальной безопасности Российской Федерации")
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_191669/

6. Разработка типовых документов в области информационной безопасности: методические указания [Электронный ресурс]: электронный учебный курс / Иванцов Андрей Михайлович; УлГУ. - Ульяновск : УлГУ, 2016. - 1 электрон. опт. диск (CD-ROM). **URL:** http://edu.ulsu.ru/cources/750/interface/.

7. Домарев В.В. Безопасность информационных технологий. Системный подход: К.: ООО «ТИД «ДС», 2004. – 992 с.

8. Информационная безопасность: герменевтический подход: монография / Л.В. Астахова. – М.: РАН, 2010. – 185 с.

9. Колин К.К. Неоглобализм и культура: новые угрозы для национальной безопасности. //Знание. Понимание. Умение: Научн. журнал Московского гуманитарного университета. – 2005. – № 2. С. 104-111;

10. Колин К.К. Неоглобализм и культура: новые угрозы для национальной безопасности. //Знание. Понимание. Умение: Научн. журнал Московского гуманитарного университета. – 2005. № 3. – С. 80-87.

11. Малюк А.А., Полянская О.Ю., Алексеева Ю.И. Этика в сфере информационных технологий. М.: Горячая линия - Телеком, 2016. – 352 с.

12. Информационная безопасность компьютерных систем и сетей: учебное пособие / В.Ф. Шаньгин. – М.: ИД «ФОРУМ»; ИНФРА-М, 2014. – 416 с. ил.

13. А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. Основы управления информационной безопасностью. Учебное пособие для вузов. – 2-е изд., испр. М.: Горячая линия – Телеком, 2014. – 244 с.: ил.

14. Основы информационной безопасности: курс лекций: учебное пособие / издание третье / Галатенко В. А. Под редакцией академика РАН В.Б. Бетелина - М.: ИНТУИТ.РУ «Интернет-университет Информационных Технологий, 2006. -208 с.

15. Управление инцидентами информационной безопасности и непрерывностью бизнеса. Учебное пособие для вузов. - 2-е изд., испр. - М.: Горячая линия-Телеком, 2014. - 170 с.: ил. - Серия «Вопросы управления информационной безопасностью. Выпуск 3».

16. Аверченков В.И., Аудит информационной безопасности: учеб. пособие для вузов / В.И. Аверченков - М.: ФЛИНТА, 2016. - 269 с. - ISBN 978-5-9765-1256-6 - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL: http://www.studentlibrary.ru/book/ISBN9785976512566.html (дата обращения: 09.06.2020). - Режим доступа: по подписке.

17. Милославская Н.Г., Проверка и оценка деятельности по управлению информационной безопасностью: Учебное пособие для вузов / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - Вып. 5. - М.: Горячая линия - Телеком, 2013. - 166 с. (Серия "Вопросы управления информационной безопасностью".) - ISBN 978-5-9912-0275-6 - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL: http://www.studentlibrary.ru/book/ISBN9785991202756.html (дата обращения: 09.06.2020). - Режим доступа: по подписке.

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ

2.1. РАЗДЕЛ 1. ГУМАНИТАРНАЯ СУЩНОСТЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТЕМА 1. ВВЕДЕНИЕ В ДИСЦИПЛИНУ «ГУМАНИТАРНЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Основные вопросы:

1. Предмет и задачи курса «Гуманитарные аспекты информационной безопасности»
2. Гуманитарная сущность безопасности
3. Гуманитарная сущность информации
4. Гуманитарная сущность информационной безопасности

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 6-14.

Вопрос 2 изложен в лекции и в монографии [8].

Для самостоятельного изучения вопроса 2 следует обратиться к монографии [8].

Вопрос 3 изложен в лекции и в [5.1, 5.2].

Для самостоятельного изучения вопроса 3 следует обратиться к монографии [8].

Контрольные вопросы по теме 1:

1. Дать характеристику направлений области информационной безопасности (Доктрина информационной безопасности Российской Федерации)
2. Раскрыть составляющие национальных интересов Российской Федерации в информационной сфере
3. Пояснить сущность понятий «безопасности» и «информации»
4. Что такое «Информационная безопасность» (Доктрина информационной безопасности Российской Федерации)
5. Раскрыть понятие «гуманитарная сущность информации».
6. Пояснить технократический и гуманитарный подходы к информации
7. Что понимается под «Гуманитарной сущностью информационной безопасности»

Тесты для самостоятельной работы:

1. Что в основном понимается под термином "гуманитарный" в дисциплине Гуманитарные аспекты информационной безопасности?

а) Гуманитарные науки

б) Гуманитарные знания

в) Сфокусированность на человеке, его правах, свободах, чувствах и др.

2. Какое направление в области информационной безопасности рассматривается в дисциплине «Гуманитарные аспекты информационной безопасности»?

а) Защита информации и защита от информации

б) Защита информации и обеспечение информационной безопасности

в) Защита информации и противодействие иностранным техническим разведкам

г) Защита информации и юридические аспекты защиты от информации

3. Указать наиболее правильное толкование термина "Безопасность"

а) Положение, при котором кому-либо или чему-либо не угрожает опасность

б) Наличие физической защиты для кого-либо или чего-либо

в) Состояние абсолютного покоя и умиротворения

4. В каком документе даётся определение понятия "Информационная безопасность"?

а) Закон РФ "О безопасности"

б) Доктрина информационной безопасности Российской Федерации

в) Стратегия национальной безопасности Российской Федерации

5. Какой из подходов к информации (технократический или гуманитарный) должен преобладать в области информационной безопасности?

а) Технократический

б) Гуманитарный

в) И Технократический и Гуманитарный

2.2. РАЗДЕЛ 1. ГУМАНИТАРНАЯ СУЩНОСТЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТЕМА 2. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ГУМАНИТАРНАЯ ПРОБЛЕМА

Основные вопросы:

1. Системный кризис цивилизации и его гуманитарные причины
2. Моральное зло в современном мире и проблема нравственного выбора
3. Обеспечение национальной и международной безопасности - приоритетные проблемы развития цивилизации в XXI веке
4. Нравственные приоритеты молодого поколения и будущее России
5. Преемственность поколений в области науки, образования и высоких технологий как проблема интеллектуальной безопасности России
6. Нравственная ориентация молодого поколения и национальная безопасность

Рекомендации по изучению темы:

Вопрос 1 изложен в лекции и в [9] на с. 104-108.

Для самостоятельного изучения вопроса 1 следует обратиться к учебному пособию [2] на с. 11-15.

Вопрос 2 изложен в лекции и в [9] на с. 108-109.

Вопрос 3 изложен в лекции и в [9] на с. 109-111.

Вопрос 4 изложен в лекции и в [10] на с. 80-85.

Вопрос 5 изложен в лекции и в [10] на с. 85-86.

Вопрос 6 изложен в лекции и в [10] на с. 86-87.

Для самостоятельного изучения вопроса 6 следует обратиться к [5.1-5.2].

Контрольные вопросы по теме 2:

1. Пояснить сущность гуманитарных аспектов информационной безопасности.
2. В чём заключается системный кризис цивилизации?
3. Что такое «Моральное зло в современном мире и проблема нравственного выбора».
4. Проблемы обеспечения национальной и коллективной международной безопасности.
5. Нравственные приоритеты молодого поколения.
6. Проблема интеллектуальной безопасности России.
7. Нравственная ориентация молодого поколения и национальная безопасность.

Тесты для самостоятельной работы:

1. Какие проблемы, из названных, находятся в зоне гуманитарной сферы?

а) Бедность населения

б) Состояние экономического развития страны

в) Геополитика

2. Кризис цивилизации в подавляющем большинстве случаев является результатом:

а) Развития технологий

б) Деятельности людей

в) Природных катаклизмов

3. Чем в основном должны определяться нравственные приоритеты молодого поколения? Выбрать 3 ответа.

а) Знание истории страны

б) Вера в будущее

в) Наличие нравственных ориентиров

г) Профессионализм в своей сфере деятельности

4. Какие основные причины, из перечисленных, не приводят к потере преемственности поколений в области высоких технологий?

а) Старение научных и педагогических кадров

б) Разрушение целостной системы воспитательной работы с молодёжью
в) Система наставничества на предприятиях

2.3. РАЗДЕЛ 1. ГУМАНИТАРНАЯ СУЩНОСТЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТЕМА 3. ПРОБЛЕМЫ РЕАЛИЗАЦИИ ГУМАНИТАРНОЙ СУЩНОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основные вопросы:

1. Стадии формирования информационной безопасности (ИБ)
2. Система ИБ
3. Профессиональное сообщество ИБ
4. Технологии и методы деятельности ИБ
5. Становление и признание значимости отрасли ИБ

Рекомендации по изучению темы:

Вопрос 1 изложен в лекции и в учебном пособии [1] на с. 13-19.

Для самостоятельного изучения вопроса 1 следует обратиться к монографии [8].

Вопрос 2 изложен в учебном пособии [1] на с. 21-23.

Для самостоятельного изучения вопроса 1 следует обратиться к [5.1]

Вопрос 3 изложен в лекции и в монографии [8].

Вопрос 4 изложен в учебном пособии [1] на с. 112-120.

Для самостоятельного изучения вопроса 4 следует обратиться к монографии [8].

Вопрос 5 изложен в учебном пособии [1] на с. 124-129.

Для самостоятельного изучения вопроса 5 следует обратиться к [5.1].

Контрольные вопросы по теме 3

1. Основные стадии формирования информационной безопасности
2. Что понимается под институционализацией ИБ
3. Раскрыть основу нормативно-правового компонента институализации
4. Пояснить сущность самоорганизационного компонента институализации
5. Система подготовки специалистов по защите информации
6. Основные технологии и методы деятельности ИБ
7. Что такое социализация ИБ?

Тесты для самостоятельной работы:

1. Какие угрозы информационной безопасности России относятся к наиболее опасным? Выбрать 4 ответа.

а) Оказание информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в стране

б) Наращивание возможностей информационно-технического воздействия на информационную структуру в военных целях
в) Расширение экономических санкций
г) Дискриминация российских средств массовой информации за рубежом
д) Возрастание масштабов компьютерной преступности

2. Какие компоненты не относятся к стадии институализации системы информационной безопасности?
а) Нормативно-правовой
б) Организационный
в) Социально-культурный
г) Когнитивный
д) Технический

2.4. РАЗДЕЛ 1. ГУМАНИТАРНАЯ СУЩНОСТЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТЕМА 4. КУЛЬТУРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основные вопросы:

1. Формирование информационной культуры общества. Этика в сфере информационных технологий
2. Основные элементы глобальная культуры кибербезопасности
3. Всеобуч в области культуры информационной безопасности

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [11] на с. 26-30.
Вопрос 2 изложен в учебном пособии [1] на с. 12-15.
Вопрос 3 изложен в учебном пособии [1] на с. 114-127.

Контрольные вопросы по теме 4:

1. Этика в сфере информационных технологий
2. Информационная культура личности
3. Основные факторы, влияющим на уровень информационной культуры современного общества
4. Основные элементы глобальной культуры кибербезопасности
5. Всеобуч в области культуры информационной безопасности
6. В чем отличие профессионального и массового обучения?
7. Существует ли, на ваш взгляд, проблема цифрового неравенства в России по образовательным, территориальным, экономическим, национальным и гендерным признакам? Есть ли отличие этих проблем в России от аналогичных проблем в других странах?

Тесты для самостоятельной работы:

1. В каких документах отражены концептуальные вопросы обеспечения

информационной безопасности? Выбрать 2 ответа.
а) Доктрина информационной безопасности РФ
б) Стратегия развития информационного общества в РФ
в) Закон РФ «О государственной тайне»
г) Федеральный закон РФ "О персональных данных"

2. Какие структуры относятся к общественным объединениям в сфере информационной безопасности? Выбрать 3 ответа.
а) Некоммерческое партнерство «Инфофорум»
б) Ассоциация защиты информации
в) Межрегиональная общественная организация «Ассоциация защиты информации»
г) Межведомственная комиссия Совета безопасности РФ по информационной безопасности
д) Комитет по безопасности государственной думы РФ

3. Какие признаки указывают на достаточно широкое признание социального статуса информационной безопасности? Выбрать 3 ответа.
а) Информированность общества о существовании ИБ и профильных специалистов в организациях, учреждениях и предприятиях различных форм собственности
б) Признание феномена ИБ как важнейшего инструмента управления организацией, достижения ею конкурентных преимуществ
в) Формирование представления о ИБ как необходимом компоненте культуры управления
г) Использование иностранных ПЭВМ и программного обеспечения
д) Наличие большого количества нормативно-правовых актов в области ИБ

4. Какие процессы способствуют формированию информационной культуры? Выбрать 4 ответа.
а) Формирование адекватной и динамичной картины мира
б) Совершенствованием средств правового регулирования, сконцентрированных на позитивном праве
в) Эффективный информационный обмен
г) Информационная нравственность, регулирующая вопросы доступа к чужой информации, использования информации для корыстных целей или целей давления на личность, ограничения доступа других к полезной информации
д) Выработка и совершенствование способов сохранения и усвоения информации

5. Какие элементы не включены в глобальную культуру кибербезопасности, утверждённую Генеральной Ассамблеей ООН? Выбрать 2 ответа.
а) Осведомленность
б) Этика

в) Демократия
г) Управление обеспечением безопасности
д) Финансирование
е) Техническая оснащённость

6. Какие меры борьбы с негативным контентом, распространяемым в сети Интернет, не противоречащие принципам свободы слова, Вы считаете самыми действенными? Выбрать 3 ответа.
а) Использование действующего международного и российского законодательства
б) Блокирование негативного контента по решению суда
в) Создание действенных систем контроля трафика
г) Блокирование негативного контента по жалобам пользователей

2.5. РАЗДЕЛ 2. УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

ТЕМА 5. СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основные вопросы:

1. Роль стандартов информационной безопасности
2. Международные стандарты информационной безопасности
3. Отечественные стандарты безопасности информационных технологий

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [12] на с. 76-78.

Для самостоятельного изучения вопроса 1 следует обратиться к учебному пособию [4] на с. 3-5.

Вопрос 2 изложен в учебном пособии [12] на с. 78-88.

Для самостоятельного изучения вопроса 2 следует обратиться к учебному пособию [4] на с. 10-26.

Вопрос 3 изложен в учебном пособии [12] на с. 92-97.

Для самостоятельного изучения вопроса 3 следует обратиться к учебному пособию [4] на с. 27-29.

Контрольные вопросы по теме 5:

1. В чём заключается главная задача стандартов ИБ
2. Какие уровни безопасности были определены в оранжевой книге Министерства обороны США?
3. Какие задачи предполагает обеспечение ИБ в любой компании?
4. Какие основные стандарты рассматривают актуальные вопросы обеспечения ИБ организаций и предприятий?
5. Особенности Германского стандарта BSI
6. Международный стандарт ISO 15408 «Общие критерии безопасности информационных технологий»

7. Стандарты для беспроводных сетей
8. Стандарты информационной безопасности в сети Интернет
9. Отечественные стандарты безопасности информационных технологий

Тесты для самостоятельной работы:

1. Сколько уровней безопасности содержится в "Оранжевой книге"?
а) 4
б) 3
в) 8
г) 6
д) 9

2. Стандарт ISO 15408 рассматривает информационную безопасность как:
а) обеспечение конфиденциальности информации
б) совокупность конфиденциальности и целостности информации
в) совокупность конфиденциальности и доступности информации
г) совокупность доступности и целостности информации

3. Какой стандарт определяет протоколы, необходимые для организации беспроводных локальных сетей?
а) SSL
б) IEEE 802.11
в) SET
г) ISO 5408

4. Какой стандарт, из перечисленных, в настоящий момент отменён?
а) ГОСТ Р ИСО/МЭК 17799-06
б) ГОСТ Р ИСО/МЭК 27002-2012
в) ГОСТ Р 34.11-2012

2.6. РАЗДЕЛ 2. УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

ТЕМА 6. СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Основные вопросы:

1. Система управления ИБ организации
2. Область действия СУИБ
3. Документальное обеспечение СУИБ
4. Процессный подход
5. Основные этапы разработки СУИБ

Рекомендации по изучению темы:
Вопрос 1 изложен в учебном пособии [13] на с. 128-139.

Для самостоятельного изучения вопроса 1 следует обратиться к соответствующим стандартам [3].

Вопрос 2 изложен в учебном пособии [13] на с. 146-149.

Для самостоятельного изучения вопроса 2 следует обратиться к соответствующим стандартам [3].

Вопрос 3 изложен в учебном пособии [13] на с. 149-156.

Для самостоятельного изучения вопроса 3 следует обратиться к учебному пособию [6].

Вопрос 4 изложен в учебном пособии [13] на с. 160-172.

Для самостоятельного изучения вопроса 4 следует обратиться к соответствующим стандартам [3].

Вопрос 5 изложен в учебном пособии [13] на с. 190-195.

Для самостоятельного изучения вопроса 5 следует обратиться к соответствующим стандартам [3].

Контрольные вопросы по теме 6:

1. Основные функции системы управления информационной безопасностью (СУИБ) в организации
2. Важнейшие компоненты СУИБ
3. Основные выгоды от СУИБ
4. Область действия СУИБ
5. Примеры возможных целей управления ИБ, которые могут быть использованы в качестве входных данных для определения первоначальной области действия СУИБ
6. Документальное обеспечение СУИБ
7. Использование процессного подхода для разработки, внедрения, обеспечения функционирования, мониторинга, анализа, поддержки и улучшения СУИБ (СМИБ) организации
8. Сущность модели Шухарта-Деминга
9. Основные этапы разработки СУИБ
10. Инвентаризация активов компании
11. Категорирование активов компании
12. Оценка защищенности информационной системы компании
13. Оценка информационных рисков
14. Обработка информационных рисков
15. Политика управления информационной безопасностью и Политика информационной безопасности

Тесты для самостоятельной работы:

1. Какие компоненты, из перечисленных, должны быть обязательно включены в систему управления информационной безопасности (СУИБ)? Выбрать 4 варианта.

а) Соответствующая организационная структура
б) Соответствующие средства управления ИБ
в) Ответственность всех участвующих в процессе управления ИБ

г) Соответствующее документальное обеспечение функционирования СУИБ
д) Система обучения работе в СУИБ

2. Что, из перечисленного, не включается в область действия СУИБ организации?
а) Бизнес-процессы
б) Активы (кадры, финансовые средства, средства ВТ, телекоммуникационные средства и др.)
в) Технологии
г) Сведения об образовании сотрудников отдела информационной безопасности

3. Какие сведения, из перечисленных, должны в обязательном порядке быть включены в результирующий документ по определению области действия системы управления информационной безопасности (СУИБ)? Отметить 4 варианта.
а) Список бизнес-целей управления ИБ
б) Список критических бизнес-процессов, систем, информационных активов, организационных структур и географических районов, где будет применяться СУИБ
в) Описание того, как части области действия взаимодействуют с другими системами управления
г) Характеристики бизнеса самой организации, ее местонахождения, активов и используемых технологий
д) Описание технических характеристик информационных систем, обеспечивающих функционирование бизнес-процессов организации

4. Какие документы относятся к СУИБ 2 уровня? Выбрать 2 варианта.
а) Политика СУИБ
б) Политика обработки инцидентов ИБ
в) Описания (стандарты) технологий обеспечения ИБ
г) Планы работ по управлению ИБ

5. Какие документы, из перечисленных, обычно включаются в документацию СУИБ? Выбрать 4 варианта.
а) Рабочие инструкции
б) Спецификации
в) Перечень сведений, составляющих коммерческую тайну
г) Политика СУИБ
д) Внешние документы (международные стандарты, ГОСТ-ы и др.)

6. Выберите правильный порядок реализации этапов модели Шухарта-Деминга.

а) «Планирование, Действие, Осуществление, Проверка»
б) «Планирование, Проверка, Осуществление, Действие»
в) «Планирование, Осуществление, Проверка, Действие»
г) «Планирование, Проверка, Осуществление, Действие»

7. Инвентаризация какого актива компании наиболее трудоёмка?
а) Программное обеспечение
б) Материальные активы
в) Сотрудники компании
г) Нематериальные ресурсы
д) Сервисы
е) Информационные ресурсы

8. Какой из способов обработки рисков самый затратный для организации?
а) Принятие рисков
б) Передача рисков
в) Уклонение от рисков
г) Снижение рисков

2.7. РАЗДЕЛ 2. УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

ТЕМА 7. УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Основные вопросы:
1. Основные понятия управления рисками
2. Основные этапы управления рисками

Рекомендации по изучению темы:
Вопрос 1 изложен в учебном пособии [14] на с. 123-149.
Для самостоятельного изучения вопроса 1 следует обратиться к [7] На с. 672-690.
Вопрос 2 изложен в учебном пособии [7] на с. 675-680.

Контрольные вопросы по теме 7:
1. Основная терминология по управлению рисками
2. Основные этапы управления рисками
3. Выбор анализируемых объектов и уровня детализации их рассмотрения
4. Методология оценки рисков
5. Идентификация активов
6. Оценка рисков

7. Оценка стоимости мер защиты
8. Остаточные риски

Тесты для самостоятельной работы:

1. На каком уровне информационной безопасности рассматривается управление рисками?
а) На административном уровне
б) На процедурном уровне
в) На операционном уровне

2. Ликвидация риска – это?
а) Устранение причины риска
б) Заключение страхового соглашения
в) Использование дополнительных защитных средств
г) Выработка плана действия в соответствующих условиях

3. Принятие риска – это?
а) Устранение причины риска
б) Выработка плана действия в соответствующих условиях
в) Использование дополнительных защитных средств
г) Заключение страхового соглашения

4. Какие этапы управления рисками относятся к непосредственно к оценке рисков? Выбрать 6 ответов.
а) Выбор защитных мер
б Реализация и проверка выбранных мер
в) Оценка остаточного риска
г) Выбор анализируемых объектов и уровня детализации их рассмотрения
д) Идентификация активов
е) Выбор методологии оценки рисков
ж) Анализ угроз и их последствий, выявление уязвимых мест в защите
з) Оценка рисков

5. На каком этапе жизненного цикла выявленные риски следует учитывать при конфигурировании информационной системы?
а) На этапе инициации
б) На этапе установки
в) На этапе эксплуатации
г) На этапе закупки
д) На этапе утилизации

2.8. РАЗДЕЛ 2. УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

ТЕМА 8. СИСТЕМА УПРАВЛЕНИЯ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основные вопросы:

1. Нормативная база управления инцидентами ИБ
2. Понятие события и инцидента ИБ
3. Цели и задачи управления инцидентами
4. Система управления инцидентами ИБ
5. Этапы процесса управления инцидентами ИБ
6. Политика управления инцидентами ИБ
7. Обеспечение осведомленности и обучение в области инцидентов ИБ

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [15] на с. 9-19.

Для самостоятельного изучения вопроса 1 следует обратиться к соответствующим стандартам [3].

Вопрос 2 изложен в учебном пособии [15] на с. 20-26.

Для самостоятельного изучения вопроса 2 следует обратиться к соответствующим стандартам [3].

Вопрос 3 изложен в учебном пособии [15] на с. 26-31.

Для самостоятельного изучения вопроса 3 следует обратиться к соответствующим стандартам [3].

Вопрос 4 изложен в учебном пособии [15] на с. 31-39.

Для самостоятельного изучения вопроса 4 следует обратиться к соответствующим стандартам [3].

Вопрос 5 изложен в учебном пособии [15] на с. 39-45.

Для самостоятельного изучения вопроса 5 следует обратиться к соответствующим стандартам [3].

Вопрос 6 изложен в учебном пособии [15] на с. 71-72.

Для самостоятельного изучения вопроса 6 следует обратиться к соответствующим стандартам [3].

Вопрос 7 изложен в учебном пособии [15] на с. 83-92.

Для самостоятельного изучения вопроса 7 следует обратиться к соответствующим стандартам [3].

Контрольные вопросы по теме 8:

1. Нормативная база управления инцидентами ИБ
2. Суть жизненного цикла СУИБ
3. Понятие события и инцидента ИБ
4. Цели и задачи управления инцидентами ИБ
5. Цели организации по эффективному управлению инцидентами ИБ.
6. Процесс «Управление инцидентами ИБ»

7. Система управления инцидентами ИБ
8. Ключевые вопросы при создании результативно функционирующей СУИИБ
9. Этапы процесса управления инцидентами ИБ
10. Политика управления инцидентами ИБ
11. Обеспечение осведомленности и обучение в области инцидентов ИБ

Тесты для самостоятельной работы:

1. На каком этапе управления рисками целесообразно создание карты информационной системы организации?

а) вопрос скорректировать
б) Выбор анализируемых объектов и уровня детализации их рассмотрения
в) Анализ угроз и их последствий, выявление уязвимых мест в защите
г) Идентификация активов
д) Оценка рисков

2. Какой пример, из перечисленных, может быть квалифицирован, как событие ИБ?

а) Отключение электропитания
б) Неверный ввод пароля 2 раз подряд
в) Отправка информации ограниченного доступа в сети Интернет без паролирования (шифрования)
г) Несанкционированное копирование информации ограниченного доступа на личный флэш-носитель

3. Какой пример, из перечисленных, может быть квалифицирован, как инцидент ИБ?

а) Отказ в обслуживании
б) Неудавшаяся попытка кражи носителя с информацией ограниченного доступа
в) Ввод неправильного пароля
г) Пароль, написанный на стикере, прикреплённый к монитору сотрудника

4. Какой вариант цели организации не способствует эффективному управлению инцидентами ИБ?

а) Сохранить и восстановить данные
б) Наказать нарушителей Политики ИБ организации
в) Гарантировать целостность критически важных систем
г) Предотвратить развитие атак и будущие инциденты ИБ
д) Избежать нежелательной огласки информации об инциденте ИБ

5. На каком этапе процесса управления инцидентами происходят реагирование на инцидент ИБ и определение необходимости проведения расследования инцидента ИБ?

а) На этапе планирования и подготовки

б) На этапе совершенствования
в) На этапе использования
г) На этапе анализа

6. Какие вопросы согласно требованиям стандартов отражаются в политике управления инцидентами ИБ? Указать 4 варианта.
а) Обязательства высшего руководства относительно поддержки управления инцидентами
б) Подробная программа обеспечения осведомлённости и обучения управлению инцидентами ИБ
в) Перечень ответственных лиц, необходимые для выполнения действия, уведомления об инцидентах ИБ
г) Извлечение уроков и улучшение процесса, следующего за инцидентами ИБ
д) Краткое изложение действий после подтверждения категории инцидента ИБ

1.9. РАЗДЕЛ 2. УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

ТЕМА 9. ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Основные вопросы:

1. Основные понятия политики информационной безопасности организации
2. Содержание Политики информационной безопасности организации
3. Стратегии действий на нарушения безопасности

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [13] на с. 84-101.

Для самостоятельного изучения вопроса 1 следует обратиться к соответствующим стандартам [3].

Вопрос 2 изложен в учебном пособии [13] на с. 102-110.

Для самостоятельного изучения вопроса 1 следует обратиться к соответствующим стандартам [3].

Вопрос 3 изложен в учебном пособии [2] на с. 111-121.

Контрольные вопросы по теме 9:

1. Основные понятия политики информационной безопасности организации
2. Содержание Политики информационной безопасности предприятия
3. В чём отличие частных политик от общей политики организации?
4. Назвать примеры частных политик организации
5. Основные стратегии действий на нарушения безопасности
6. Уровни политик безопасности
7. На каком уровне описываются механизмы защиты информации?
8. Основные разделы ПИБ организации

Тесты для самостоятельной работы:

1. Что не следует использовать при выборе пароля?

а) Даты, фамилии, регистрационные номера автомобилей

б) Основные методики, прописанные в инструкциях организации

в) Методики выбора пароля, описанные в сети Интернет

1.10. РАЗДЕЛ 2. УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

ТЕМА 10. ПЛАН ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Основные вопросы:

1. Назначение и основные положения Плана защиты
2. Организация режима информационной безопасности
3. Требования безопасности, предъявляемые к пользователям ИС
4. Определение обязанностей руководителя и координаторов восстановительных работ
5. Разработка мероприятий, формальных процедур и других технологических процессов по обеспечению ИБ
6. Выявление попыток НСД
7. Реагирование на нарушения информационной безопасности
8. Ликвидация последствий НСД

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [7] на с. 744-750.

Для самостоятельного изучения вопроса 1 следует обратиться к соответствующим стандартам [3].

Вопрос 2 изложен в лекции.

Для самостоятельного изучения вопроса 2 следует обратиться к соответствующим стандартам [3].

Вопрос 3 изложен в учебном пособии [7] на с. 738-749.

Для самостоятельного изучения вопроса 4 следует обратиться к соответствующим стандартам [3].

Вопрос 4 изложен в учебном пособии [7] на с. 738-749.

Для самостоятельного изучения вопроса 4 следует обратиться к соответствующим стандартам [3].

Вопрос 5 изложен в учебном пособии [7] на с. 729-740.

Для самостоятельного изучения вопроса 5 следует обратиться к соответствующим стандартам [3].

Вопрос 6 изложен в учебном пособии [1] на с. 50-60.

Вопрос 7 изложен в учебном пособии [7] на с. 678-680.

Вопрос 8 изложен в учебном пособии [7] на с. 798-802.

Контрольные вопросы по теме 10:

1. Раскрыть отличия между Политикой безопасности, Планом защиты и Планом обеспечения непрерывной работы и восстановления функционирования ИС
2. Назначение и основные положения Плана защиты
3. Состав и последовательность административных мероприятий, проводимых с целью организации защиты от НСД к информации
4. Действия по реагированию на нарушения безопасности, предусматривающие применение мер процедурного и программно-технического уровня.
5. Организация режима информационной безопасности
6. Распределение обязанностей между администраторами ИС
7. Требования безопасности, предъявляемые к пользователям ИС
8. Основные правила выбора пароля пользователем
9. Обязанности руководителя восстановительных работ
10. Планирование обучения персонала ИС
11. Основные рекомендации по обеспечению ИБ
12. Предупреждение нарушений безопасности
13. Внешний и внутренний аудиты безопасности
14. Анализ инцидента администратором безопасности
15. Выявление подозрительных процессов
16. Реагирование на нарушения информационной безопасности
17. Ликвидация последствий НСД

Тесты для самостоятельной работы:

1. Какие из приведённых составляющие входят в план защиты? Отметить 4 пункта.

а) Состав мероприятий и порядок действий по предотвращению нарушений безопасности

б) Действия по реагированию на нарушения безопасности, предусматривающие применение мер процедурного и программно-технического уровня

в) Система мероприятий по ликвидации последствий нарушений безопасности

г) Пошаговые инструкции по анализу нарушений безопасности

д) Система обучения для предотвращения нарушений безопасности

2. Какой из названных администраторов отвечает за выполнение мероприятий по установке, настройке и поддержанию в работоспособном состоянии прикладного программного обеспечения, эксплуатируемого в организации?

а) Системный администратор

б) Сетевой администратор

в) Администратор приложений

г) Администратор безопасности

3. Какие рекомендации в явном виде не относятся к обеспечению информационной безопасности?

а) По использование лицензионного ПО

б) По выбору паролей и использованию другой аутентификационной информации

в) По пользованию сетевыми сервисами

г) По предотвращению и ликвидации последствий воздействия компьютерных вирусов

д) По выбору прикладного ПО

4. К какому уровню относится некритическое событие, которое должно быть задокументировано для обеспечения последующих ссылок на него?

а) Уровень 1

б) Уровень 2

в) Уровень 3

г) Уровень 4

д) Уровень 5

1.11. РАЗДЕЛ 2. УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

ТЕМА 11. ПЛАН ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОЙ РАБОТЫ И ВОССТАНОВЛЕНИЯ РАБОТОСПОСОБНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Основные вопросы:

1. Понятие управления непрерывности бизнеса
2. Система управления непрерывностью бизнеса
3. Внедрение управления непрерывностью бизнеса в культуру организации
4. Общая характеристика планов управления инцидентами, обеспечения непрерывности бизнеса и восстановления бизнеса
5. Примерное содержание плана обеспечения непрерывности бизнеса
6. План восстановления бизнеса

Рекомендации по изучению темы:

Вопрос 1 изложен в лекции.

Для самостоятельного изучения вопроса 1 следует обратиться к соответствующим стандартам [3].

Вопрос 2 изложен в лекции.

Для самостоятельного изучения вопроса 2 следует обратиться к соответствующим стандартам [3].

Вопрос 3 изложен в лекции.

Вопрос 4 изложен в лекции.

Для самостоятельного изучения вопроса 4 следует обратиться к соответствующим стандартам [3].

Вопрос 5 изложен в учебном пособии [6] на с. 21-28.

Для самостоятельного изучения вопроса 5 следует обратиться к соответствующим стандартам [3].

Контрольные вопросы по теме 11:

1. Понятие управления непрерывности бизнеса
2. Обеспечение устойчивости бизнес-процессов к инцидентам
3. Восстановление бизнеса, включая бизнес-процессы, операции и ресурсы, организации после инцидентов
4. Система управления непрерывностью бизнеса
5. Типовые технические решения для обеспечения непрерывности бизнеса
6. Внедрение управления непрерывностью бизнеса в культуру организации
7. Общая характеристика планов управления инцидентами, обеспечения непрерывности бизнеса и восстановления бизнеса
8. Примерное содержание плана обеспечения непрерывности бизнеса
9. Основные требования к ресурсам
10. План восстановления бизнеса

Тесты для самостоятельной работы:

1. Какие условия требуют реализации стратегия немедленной защиты и восстановления? Отметить 4 условия.

а) Если ресурсы ИС недостаточно хорошо защищены от нарушителя

б) Если действия нарушителя могут привести к небольшому финансовому риску

в) Если преследование нарушителя невыгодно с финансовой точки зрения, либо отсутствует такая возможность или желание

г) Если возможно предъявление претензий со стороны клиентов Компании

д) Если существует значительный риск для пользователей ИС

2. Какие условия требуют реализации стратегия наблюдения за нарушителем и его преследования? Отметить 4 условия.

а) Ресурсы ИС адекватно защищены

б) Попытка НСД является продолжением предыдущих попыток, уже имевших место ранее

в) Доступ нарушителя к ресурсам ИС находится под контролем

г) Средства мониторинга не в состоянии осуществлять достаточно полное протоколирование действий нарушителя для того, чтобы собрать необходимые доказательства

д) Администраторы ИС достаточно хорошо подготовлены в плане знания ОС, системных утилит, СУБД и прикладных систем, чтобы осуществлять

отслеживание действий нарушителя

3. Какие технические решения могут входить в состав системы управления непрерывностью бизнеса? Отметить 3 позиции.
а) Системы охранно-пожарной сигнализации
б) Системы резервного копирования
в) Системы криптографического преобразования информации
г) Системы резервного электропитания

4. В каком из названных планов содержится набор документированных процедур и информации, которые разработаны, обобщены и актуализированы с целью их использования в случае возникновения инцидента?
а) План защиты
б) План обеспечения непрерывности бизнеса
в) План восстановления

2.12. РАЗДЕЛ 2. УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

ТЕМА 12. ЭКСПЛУАТАЦИЯ И НЕЗАВИСИМЫЙ АУДИТ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Основные вопросы:

1. Понятие аудита безопасности и цели его проведения
2. Основные принципы аудита информационной безопасности
3. Критерии аудита информационной безопасности
4. Этапы работ по проведению аудита безопасности информационных систем

Рекомендации по изучению темы:

Вопрос 1 изложен в лекции.

Для самостоятельного изучения вопроса 1 следует обратиться к учебному пособию [16] на с. 15-28.

Вопрос 2 изложен в лекции.

Для самостоятельного изучения вопроса 2 следует обратиться к учебному пособию [17] на с. 12-20.

Вопрос 3 изложен в лекции.

Для самостоятельного изучения вопроса 3 следует обратиться к учебному пособию [17] на с. 21-35.

Вопрос 4 изложен в лекции.

Для самостоятельного изучения вопроса 4 следует обратиться к соответствующим стандартам [3].

Контрольные вопросы по теме 12:

1. Понятие аудита безопасности и цели его проведения
2. Основные виды аудита ИБ
3. Дополнительные задачи, стоящие перед внутренним аудитором
4. Основные принципы аудита информационной безопасности
5. Критерии аудита информационной безопасности
6. Этапы работ по проведению аудита безопасности информационных систем

Тесты для самостоятельной работы:

1. В каком плане описывается, что должно испытываться при проверке реализуемости плана, кто должен проводить испытания, когда должны осуществляться испытания и каковы их результаты?

а) План защиты
б) План обеспечения непрерывности бизнеса
в) План восстановления бизнеса

2.13. РАЗДЕЛ 2. УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

ТЕМА 13. ФОРМИРОВАНИЯ ТРЕБОВАНИЙ К СИСТЕМАМ ЗАЩИТЫ ИНФОРМАЦИИ (СЗИ)

Основные вопросы:

1. Основные требования к системам защиты информации (СЗИ)
2. Процесс формирование требований к СЗИ
3. Основные группы требований к СЗИ

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [2] на с. 102-127.

Для самостоятельного изучения вопроса 1 следует обратиться к учебному пособию [7] на с. 692-695.

Вопрос 2 изложен в учебном пособии [7] на с. 696-700.

Вопрос 3 изложен в учебном пособии [7] на с. 700-706.

Контрольные вопросы по теме 13:

1. Что такое требование? Требования к защите информации, к СЗИ, к подсистеме ЗИ
3. Основные группы требований к СЗИ
4. Общие требования к СЗИ
5. Организационные требования к СЗИ
6. Требования к основным подсистемам СЗИ
7. Основные требования к техническому обеспечению СЗИ

Тесты для самостоятельной работы:

1. Что, из перечисленного, не относится к организационным требованиям к системе защиты информации?

а) осуществление контроля за изменениями в системе программного обеспечения

б) выполнение тестирования и верификации изменений в системе ПО и программах защиты

в) регистрация и сопровождение посетителей

г) применение способов, методов и средств достижения необходимых показателей защищенности

д) организация системы обучения и повышения квалификации обслуживающего персонала