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 «УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»

Для студентов специалитета по специальности 10.05.03
очной формы обучения

Ульяновск, 2019

Методические указания для самостоятельной работы студентов по дисциплине «Управление информационной безопасностью» / составитель: А.М. Иванцов. - Ульяновск: УлГУ, 2019. Настоящие методические указания предназначены для студентов специалитета по специальности 10.05.03 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 № 2/19 от 19.03.2019 г.).

Содержание

1. ЛИТЕРАТУРА ДЛЯ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

1. Курило А.П. Основы управления информационной безопасностью: учебное пособие для вузов / А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - Вып. 1. - Москва: Горячая линия - Телеком, 2013. - 244 с. (Серия "Вопросы управления информационной безопасностью".) - ISBN 978-5-9912-0271-8. - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL:

2. Щеглов, А. Ю. Защита информации: основы теории: учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва: Издательство Юрайт, 2018. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://www.biblio-online.ru/bcode/449285

3. Шилов, А. К. Управление информационной безопасностью: учебное пособие / Шилов А. К. - Ростов н/Д: Изд-во ЮФУ, 2018. - 120 с. - ISBN 978-5-9275-2742-7. - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL: https://www.studentlibrary.ru/book/ISBN9785927527427.html

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. 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/.

6. 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.

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

8. 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.

9. 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.

10. 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.

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

11.1 ГОСТ Р ИСО 9000-2001. Системы менеджмента качества. Основные

положения и словарь;

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

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

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

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

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

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

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ

2.1. РАЗДЕЛ 1. СТАНДАРТИЗАЦИЯ СИСТЕМ И ПРОЦЕССОВ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

ТЕМА 1. УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ. ОСНОВНЫЕ ПОНЯТИЯ

Основные вопросы:

Понятия: системы, системного подхода, процесса, процессного подхода, управления, информационной безопасности. Процессный подход к управлению организации. Управление информационной безопасностью.

Рекомендации по изучению темы:

Вопросы темы 1 изложены в учебном пособии [1] на с. 1-33, 160-174.

Для самостоятельного изучения темы следует обратиться к учебному пособию [3] на с. 9-18 и [2] на с. 9-12.

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. Процессный подход к управлению организации
6. Что такое «Управление информационной безопасностью»

Тесты для самостоятельной работы:

1. 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

2. 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. СТАНДАРТИЗАЦИЯ СИСТЕМ И ПРОЦЕССОВ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

ТЕМА 2. СЕРИЯ СТАНДАРТОВ ISO/IEC 27000

Основные вопросы:

Роль стандартов информационной безопасности для решения проблемы ИБ. Серия стандартов ISO/IEC 27000 «Информационные технологии. Методы обеспечения безопасности». Международные стандарты информационной безопасности. Управление информационной безопасностью. Общие критерии безопасности информационных технологий. Основные отечественные стандарты безопасности информационных технологий.

Рекомендации по изучению темы:

Вопросы темы 2 изложен в учебном пособии [1] на с. 34-65 и при изучении конкретных вопросов следует обратиться к соответствующим стандартам [11].

Для самостоятельного изучения темы следует обратиться к учебному пособию [4] на с. 5-26.

Контрольные вопросы по теме 2:

1. Роль стандартов информационной безопасности для решения проблемы ИБ
2. История развития серии стандартов ISO/IEC 27000
3. Основные отечественные стандарты безопасности информационных технологий
4. Что такое система управления информационной безопасностью (СУИБ)?
5. Какие стандарты посвящены СУИБ?
6. Основные требования к СУИБ

2.3. РАЗДЕЛ 1. СТАНДАРТИЗАЦИЯ СИСТЕМ И ПРОЦЕССОВ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

ТЕМА 3. СТАНДАРТЫ НА ОТДЕЛЬНЫЕ ПРОЦЕССЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Основные вопросы:

ISO/IEC 13335-Методы и средства обеспечения безопасности информационных технологий. ГОСТ Р ИСО/МЭК 13335-1-2006, ГОСТ Р ИСО/МЭК 13335-3-2007, ГОСТ Р ИСО/МЭК 13335-4-2007, ГОСТ Р ИСО/МЭК 13335-5-2006 «Информационная технология. Методы и средства обеспечения

безопасности». ISO/IEC 15408 – Общие критерии и методология оценки безопасности информационных технологий. ГОСТ Р ИСО/МЭК 15408-1, 2, 3-2008. Международные стандарты ISO серий 9000 (качество) и 14000 (экология). Международные и отечественные стандарты обеспечения непрерывности бизнеса.

Рекомендации по изучению темы:

Вопросы темы 3 изложены в учебном пособии [1] на с. 66-74.

Для самостоятельного изучения вопроса 1 следует обратиться к соответствующим стандартам [11].

Контрольные вопросы по теме 3

1. Дать характеристику стандарту ISO/IEC 13335
2. Что такое менеджмент безопасности
3. Назвать основные методы менеджмента безопасности
4. Особенности ГОСТ Р ИСО/МЭК 13335
5. Что такое менеджмент риска?
6. Общие критерии и методология оценки безопасности информационных технологий

2.4. РАЗДЕЛ 1. СТАНДАРТИЗАЦИЯ СИСТЕМ И ПРОЦЕССОВ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

ТЕМА 4. ОТРАСЛЕВЫЕ СТАНДАРТЫ В ОБЛАСТИ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Основные вопросы:

Стандарты, направленные на минимизацию рисков (ГОСТ Р 53647). Стандарты банковской системы Российской Федерации (СТО БР ИББС). Комплекс документов по обеспечению и поддержанию ИБ организаций банковской системы. Аудит ИБ.

Рекомендации по изучению темы:

Вопросы темы 4 изложены в учебном пособии [1] на с. 75-82.

Для самостоятельного изучения вопроса 1 следует обратиться к соответствующим стандартам [11].

Контрольные вопросы по теме 4:

1. Что такое минимизация рисков?
2. Дать характеристику стандарту ГОСТ Р 53647
3. Основные цели стандартизации обеспечения и управления ИБ в банковской системе (БС) РФ?

4. Комплекс документов по ОИБ в БС РФ
5. Основные цели аудита ИБ
6. Методика оценки соответствия ИБ требованиям
7. Основные показатели ИБ

2.5. РАЗДЕЛ 2. УПРАВЛЕНИЕ И СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

ТЕМА 5. АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(2/7)

Основные вопросы:

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

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [6] 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 5:

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

2.6. РАЗДЕЛ 2. УПРАВЛЕНИЕ И СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

ТЕМА 6. СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ (2/6)

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 [8] на с. 128-139.

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

Вопрос 2 изложен в учебном пособии [8] на с. 146-149.

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

Вопрос 3 изложен в учебном пособии [8] на с. 149-156.

Для самостоятельного изучения вопроса 3 следует обратиться к учебному пособию [5].

Вопрос 4 изложен в учебном пособии [8] на с. 160-172.

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

Вопрос 5 изложен в учебном пособии [8] 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 И СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

ТЕМА 7. ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ (2/9)

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 [8] на с. 84-101.

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

Вопрос 2 изложен в учебном пособии [8] на с. 102-110.

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

Вопрос 3 изложен в учебном пособии [9] на с. 111-121.

Контрольные вопросы по теме 7:

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

2.8. РАЗДЕЛ 2. УПРАВЛЕНИЕ И СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

ТЕМА 8. ПЛАН ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА (2/10)

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 [10] 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 8:

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

1.9. РАЗДЕЛ 2. УПРАВЛЕНИЕ И СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

ТЕМА 9. ПЛАН ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОЙ РАБОТЫ И ВОССТАНОВЛЕНИЯ РАБОТОСПОСОБНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ (2/11)

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 [5] на с. 21-28.

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

Контрольные вопросы по теме 9:

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