ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ В.Ф. УТКИНА»

Факультет вычислительной техники

Кафедра «Информационная безопасность»

# ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

по дисциплине

**ФТД.О.02 «Управление информационной безопасностью»**

Специальность: 10.05.01 Компьютерная безопасность

Специализация: № 5 Разработка систем защиты информации компьютерных систем объектов информатизации" (по отрасли или в сфере профессиональной деятельности)

Квалификация выпускника: - специалист по защите информации

Форма обучения - очная

Срок обучения — 5,5 лет

Рязань 2021 г.

# 1 ОБЩИЕ ПОЛОЖЕНИЯ

Оценочные материалы – это совокупность учебно-методических материалов (практических заданий, описаний форм и процедур проверки), предназначенных для оценки качества освоения обучающимися данной дисциплины как части основной образовательной программы (ОПОП).

Цель – оценить соответствие знаний, умений и уровня приобретенных компетенций обучающихся целям и требованиям ОПОП в ходе проведения промежуточной аттестации.

Основная задача – обеспечить оценку уровня сформированности общекультурных и профессиональных компетенций и индикаторов их достижения, приобретаемых обучающимся в соответствии с требованиями ОПОП.

Контроль знаний обучающихся проводится в форме текущего контроля и промежуточной аттестации.

Текущий контроль успеваемости и промежуточная аттестация проводятся с целью определения степени усвоения учебного материала, своевременного выявления и устранения недостатков в подготовке обучающихся, организации работы обучающихся в ходе учебных занятий и оказания им индивидуальной помощи.

К контролю текущей успеваемости относятся проверка знаний, умений и навыков обучающихся на практических занятиях по результатам выполнения и защиты обучающимися индивидуальных заданий, по результатам выполнения контрольных работ и тестов, по результатам проверки качества конспектов лекций и иных материалов.

В качестве оценочных средств на протяжении семестра используется устные и письменные ответы студентов на индивидуальные вопросы, письменное тестирование по теоретическим разделам курса. Дополнительным средством оценки знаний и умений студентов является отчет о выполнении практических заданий их защита.

По итогам курса обучающиеся сдают зачет. Форма проведения зачета – устный ответ с письменным подкреплением по утвержденным билетам, сформулированным с учетом содержания дисциплины. В билет для зачета включается два теоретических вопроса и задача. В процессе подготовки к устному ответу студент должен составить в письменном виде план ответа.

## 2 ПАСПОРТ ОЦЕНОЧНЫХ МАТЕРИАЛОВ ПО ДИСЦИПЛИНЕ

| № п/п | Контролируемые разделы (темы) дисциплины (результаты по разделам) | Код контролируемой компетенции (или её части) | Наименование оценочного мероприятия |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| 1 | Тема 1. Введение в дисциплину. Базовая терминология | ОПК-5(ОПК-5.5) | Зачет |
| 2 | Тема 2. Стандартизация систем и процессов управления информационной безопасностью | ОПК-5(ОПК-5.5) | Зачет |
| 3 | Тема 3. Политика информационной безопасности | ОПК-5(ОПК-5.5) | Зачет |
| 4 | Тема 4. Управление и система управления информационной безопасностью | ОПК-5(ОПК-5.5) | Зачет |
| 5 | Тема 5. Оценка и управление рисками информационной безопасности | ОПК-5(ОПК-5.5) | Зачет |
| 6 | Тема 6. Управление инцидентами информационной безопасности и обеспечение непрерывности бизнеса | ОПК-5(ОПК-5.5) | Зачет |
| 7 | Тема 7. Процессы проверки системы управления информационной безопасностью | ОПК-5(ОПК-5.5) | Зачет |

## 2 ПЕРЕЧЕНЬ КОМПЕТЕНЦИЙ С УКАЗАНИЕМ ЭТАПОВ ИХ ФОРМИРОВАНИЯ

При освоении дисциплины формируются следующие компетенции: ОПК-5 (ОПК-5.5).

Указанные компетенции формируются в соответствии со следующими этапами:

– формирование и развитие теоретических знаний, предусмотренных указанными компетенциями (лекционные занятия, самостоятельная работа студентов);

– приобретение и развитие практических умений предусмотренных компетенциями (практические занятия, самостоятельная работа студентов);

– закрепление теоретических знаний, умений и практических навыков, предусмотренных компетенциями, в ходе решения конкретных задач на занятиях, выполнения индивидуальных заданий на практических занятиях и их защиты, а так же в процессе сдачи зачета и экзамена.

## 3 ПОКАЗАТЕЛИ И КРИТЕРИИ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ (РЕЗУЛЬТАТОВ) НА РАЗЛИЧНЫХ ЭТАПАХ ИХ ФОРМИРОВАНИЯ, ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

Сформированность каждой компетенции (или ее части) в рамках освоения данной дисциплины оценивается по трехуровневой шкале:

1) пороговый уровень является обязательным для всех обучающихся по завершении освоения дисциплины;

2) продвинутый уровень характеризуется превышением минимальных характеристик сформированности компетенций по завершении освоения дисциплины;

3) эталонный уровень характеризуется максимально возможной выраженностью компетенций и является важным качественным ориентиром для самосовершенствования.

Принимается во внимание наличие и степень сформированности у обучающихся знаний, умений и обладание навыками, которые должны были формироваться в процессе изучения дисциплины.

**Уровень освоения компетенций, формируемых дисциплиной:**
**Описание критериев и шкалы оценивания тестирования:**

| Шкала оценивания | Критерий |
|---|---|
| 3 балла (эталонный уровень) | уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 85 до 100% |
| 2 балла (продвинутый уровень) | уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 70 до 84% |
| 1 балл (пороговый уровень) | уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 50 до 69% |
| 0 баллов | уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 0 до 49% |

**Описание критериев и шкалы оценивания теоретического вопроса:**

| Шкала оценивания | Критерий |
|---|---|
| 3 балла (эталонный уровень) | выставляется студенту, который дал полный ответ на вопрос, показал глубокие систематизированные знания, смог привести примеры, ответил на дополнительные вопросы преподавателя |
| 2 балла (продвинутый уровень) | выставляется студенту, который дал полный ответ на вопрос, но на некоторые дополнительные вопросы преподавателя ответил только с помощью наводящих вопросов |
| 1 балл (пороговый уровень) | выставляется студенту, который дал неполный ответ на вопрос в билете и смог ответить на дополнительные вопросы только с помощью преподавателя |
| 0 баллов | выставляется студенту, который не смог ответить на вопрос |

**На промежуточную аттестацию (зачет, экзамен) выносится тест и два теоретических вопроса.** Максимально обучающийся может набрать 6 баллов. Итоговый суммарный балл студента, полученный при прохождении промежуточной аттестации, переводится в традиционную форму по системе «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно».

**Оценка «отлично»** выставляется студенту, который набрал в сумме 6 баллов (выполнил все задания на эталонном уровне). Обязательным условием является выполнение всех предусмотренных в течение семестра лабораторных работ.

**Оценка «хорошо»** выставляется студенту, который набрал в сумме от 4 до 5 баллов при условии выполнения всех заданий на уровне не ниже продвинутого. Обязательным условием является выполнение всех предусмотренных в течение семестра лабораторных работ.

**Оценка «удовлетворительно»** выставляется студенту, который набрал в сумме 3 балла. Обязательным условием является выполнение всех предусмотренных в течение семестра лабораторных работ.

**Оценка «неудовлетворительно»** выставляется студенту, который набрал в сумме менее 3 баллов или не выполнил всех предусмотренных в течение семестра лабораторных работ.

# 4 ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ

## 4.1. Промежуточная аттестация в форме зачета

| Код компетенции | Результаты освоения ОПОП<br>Содержание компетенций |
|---|---|
| ОПК-5<br>(ОПК-5.5) | Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации<br>ОПК-5.5 Контролирует работы по выполнению режима защиты информации, в том числе ограниченного доступа |

### Типовые тестовые вопросы:

**Вопрос 1**

Комплексность решения задач информационной безопасности предполагает:

**Ответ:**

**(1) (+)** исключение "узких мест" в системе защиты информации

**(2) (+)** анализ всех возможных сценариев нарушения безопасности и способов защиты

**(3)** обеспечение круглосуточной ежедневной работы службы информационной безопасности

---

**Вопрос 2**

Как в соответствии со стандартом ISO 15408-1999 «Общие критерии оценки безопасности информационных технологий» называются требования, предъявляемые к технологии и процессу разработки и эксплуатации компонентов системы информационной безопасности?

**Ответ:**

**(1)** функциональные

**(2)** технические

**(3) (+)** требования доверия

**(4)** требования надежности

---

**Вопрос 3**

На формирование политики безопасности предприятия непосредственно влияют такие факторы как:

**Ответ:**

**(1) (+)** требования законодательства

**(2)** информационная политика предприятий-конкурентов

**(3) (+)** использование в работе предприятия сведений составляющих государственную или банковскую тайну

---

**Вопрос 4**

Информирование персонала предприятия об основных целях в сфере информационной безопасности осуществляется с помощью:

**Ответ:**

**(1)** аудита безопасности

**(2) (+)** политики безопасности
**(3)** положения о департаменте информационной безопасности

---

**Вопрос 5**
Целями верхнего уровня политики безопасности предприятия являются:
**Ответ:**

**(1) (+)** демонстрация руководством предприятия своего отношения к вопросам защиты информации
**(2)** определение структуры департамента информационной безопасности
**(3) (+)** информирование персонала об основных приоритетах в сфере защиты информации
**(4)** формирование требований к поставщикам средств защиты информации

---

**Вопрос 6**
Долгосрочное развитие политики информационной безопасности предприятия предполагает:
**Ответ:**

**(1)** статичность
**(2)** пропорциональность
**(3) (+)** цикличность

---

**Вопрос 7**
Политика информационной безопасности, относящаяся к определенной технологии или бизнес-процессу, должна содержать:
**Ответ:**

**(1) (+)** описание области применения политики
**(2) (+)** конкретные правила обращения с информацией и средствами ее обработки
**(3) (+)** распределение ролей и функций, закрепленных за различными сотрудниками

---

**Вопрос 8**
Меры физической защиты объектов в том числе включают в себя:
**Ответ:**

**(1) (+)** укрепление помещений и бронирование дверей
**(2)** установку средств биометрической идентификации посетителей
**(3) (+)** расположение защищаемых помещений на максимальном удалении от зон затопления
**(4)** ведение журнала посетителей

---

**Вопрос 9**
Биометрические средства идентификации основаны на распознавании:
**Ответ:**

**(1)** персональных кодов доступа
**(2)** персональных идентификационных карт и жетонов
**(3) (+)** индивидуальных физических особенностей

---

**Вопрос 10**
Политика опубликования материалов в открытых источниках нацелена на:
**Ответ:**

**(1) (+)** предотвращение утечек конфиденциальной информации
**(2)** недопущение нарушений авторских прав на объекты интеллектуальной собственности
**(3)** повышение уровня доступности информации

---

**Вопрос 11**
Организационная структура службы информационной безопасности определяется:
**Ответ:**

**(1)** требованиями законодательства
**(2)** требованиями государственных и международных стандартов
**(3) (+)** потребностями в защите информационных ресурсах и возможностями в соответствии с оценками руководителей предприятия

---

**Вопрос 12**
К задачам обучения и информационной работы с персоналом предприятия относится:
**Ответ:**

**(1)** недопущение утечек информации с использованием уязвимостей в сетях и ПО
**(2) (+)** ознакомление с требованиями законодательства и локальных регламентов
**(3) (+)** противодействие методам "социальной инженерии"

---

**Вопрос 13**
Приемы социотехники (используемой в социальной инженерии) основаны на:
**Ответ:**

**(1) (+)** особенностях человеческой психологии
**(2)** недостатках организационных структур
**(3)** недостатках программных и аппаратных средств защиты информации

---

**Вопрос 14**
Нарушения информационной безопасности с использованием социотехники предполагают:
**Ответ:**

**(1)** социологическое обследование персонала предприятия
**(2)** использование недостатков в организационной структуре предприятия
**(3) (+)** обман сотрудников предприятия

---

**Вопрос 15**
Регламент реагирования на инциденты должен предусматривать:
**Ответ:**

**(1)** регламент круглосуточного дежурства технического персонала
**(2) (+)** распределение функций персонала в процессе реагирования на инциденты
**(3) (+)** соглашение с поставщиками ИТ-платформ о срочной поставке компонент, вышедших из строя в результате инцидентов

---

**Вопрос 16**
К косвенным признакам, по которым могут быть выявлены нарушения информационной безопасности, относятся:
**Ответ:**

**(1)** опубликование конфиденциальной информации в открытых источниках
**(2) (+)** использование баз данных и учетных записей в нехарактерное время
**(3) (+)** резкое повышение нагрузки на информационные системы предприятия
**(4)** несанкционированный выход в Интернет сотрудников предприятия
**(5)** несанкционированный запуск посторонних программ сотрудниками предприятия

---

**Вопрос 17**
Высокий уровень полномочий необходим для локализации длящихся нарушений в связи с тем что:
**Ответ:**

**(1)** Локализация нарушений требует дорогостоящих услуг сторонних аналитиков
**(2) (+)** для локализации нарушений может потребоваться временное оперативное отключение важных информационных систем предприятия
**(3)** для локализации нарушений может потребоваться проинформировать о нарушениях большое число пользователей информационных систем

---

**Вопрос 18**
Аудит информационной безопасности - это:
**Ответ:**

**(1) (+)** экспертное обследование различных аспектов защищенности информационных ресурсов
**(2)** проверка правильности оформления и учета расходов на средства защиты информации
**(3) (+)** проверка уровня защищенности информационных ресурсов

---

**Вопрос 19**
Аудит информационной безопасности представляет собой:
**Ответ:**

**(1)** проверку выполнения требований законодательства по защите сведений, составляющих коммерческую тайну
**(2) (+)** оценку мер по защите информационных ресурсов
**(3)** проверку выполнения требований государственных стандартов в сфере информационной безопасности

---

**Вопрос 20**
К целям аудита информационной безопасности относятся:
**Ответ:**

**(1) (+)** проверка достижения поставленных целей в сфере информационной безопасности
**(2)** выявление фактов нарушения информационной безопасности
**(3)** привлечение к ответственности лиц, виновных в краже и утрате конфиденциальных данных

---

**Вопрос 21**
Проведение комплексного внешнего аудита предприятия с последующей сертификацией демонстрирует его контрагентам:
**Ответ:**

**(1) (+)** способность предприятия выступать в качестве надежного партнера, которому можно доверить конфиденциальные сведения
**(2)** полное отсутствие уязвимостей в сетях, серверах и базах данных
**(3)** достаточную страховую защиту от информационных рисков

---

**Вопрос 22**

Сертификация системы безопасности на соответствие требованиям стандарта ISO 17799 может быть осуществлена по результатам:

**Ответ:**

**(1) (+)** внешнего аудита
**(2)** внутреннего аудита
**(3)** инструментальной проверки защищенности

---

**Вопрос 23**

Аудит информационной безопасности подразделяется на:

**Ответ:**

**(1)** текущий и итоговый
**(2) (+)** внешний и внутренний
**(3)** объективный и субъективный

---

**Вопрос 24**

Услуги внешних аудиторов используются для:

**Ответ:**

**(1)** снижения затрат на аудит
**(2) (+)** повышения объективности аудита
**(3) (+)** получения сертификатов на соответствие определенным стандартам

---

**Вопрос 25**

Что в сфере информационной безопасности принято считать риском?

**Ответ:**

**(1) (+)** потенциальную возможность понести убытки из-за нарушения безопасности информационной системы
**(2)** потенциально возможное происшествие неважно, преднамеренное или нет, которое может оказать нежелательное воздействие на компьютерную систему, а также информацию, хранящуюся и обрабатывающуюся в ней
**(3)** характеристику, которая делает возможным возникновение угрозы

---

**Вопрос 26**

Что отличает риск от угрозы?

**Ответ:**

**(1)** объем вероятных потерь
**(2) (+)** наличие количественной оценки возможных потерь и (возможно) оценки вероятности реализации угрозы
**(3)** угроза и риск - понятия идентичные

---

**Вопрос 27**

Риски в сфере информационной безопасности разделяются на:

**Ответ:**

**(1)** внешние и внутренние
**(2)** объективные и субъективные
**(3) (+)** системные и операционные

---

**Вопрос 28**

Угроза безопасности информации представляет собой совокупность:

**Ответ:**

**(1)** Канала утечки информации и нарушителя
**(2)** Условий возникновения угрозы источника угрозы
**(3)** Факторов внешней среды и источника информации
**(4) (+)** Факторов, воздействующие на информацию и условий возникновения угрозы

---

**Вопрос 29**

Выделите внешние по отношению к объекту уязвимости дестабилизирующие факторы и угрозы безопасности:

**Ответ:**

**(1) (+)** ошибки персонала при эксплуатации
**(2)** ошибки программирования
**(3) (+)** сбой и отказы аппаратуры ЭВМ
**(4)** ошибки алгоритмизации задач

---

**Вопрос 30**

Выделите внутренние по отношению к объекту уязвимости дестабилизирующие факторы и угрозы безопасности:

**Ответ:**

**(1)** ошибки персонала при эксплуатации
**(2) (+)** ошибки программирования
**(3)** сбой и отказы аппаратуры ЭВМ
**(4) (+)** ошибки алгоритмизации задач

---

**Вопрос 31**

Как называется модель, описывающая вероятный облик злоумышленника, т. е. его квалификацию, имеющиеся средства для реализации тех или иных атак, обычное время действия и т. п?

**Ответ:**

**(1)** модель угрозы
**(2)** модель уязвимости
**(3) (+)** модель нарушителя
**(4)** модель безопасности

---

**Вопрос 32**

Какой термин определяет фактические расходы, понесенные субъектом в результате нарушения его прав, утраты или повреждения имущества, а также расходы, которые он должен будет произвести для восстановления нарушенного права и стоимости поврежденного или утраченного имущества?

**Ответ:**

**(1)** угроза
**(2)** риск
**(3) (+)** ущерб

**(4)** утрата

---

**Вопрос 33**

Для чего предназначена матрица взаимосвязи источников угроз и уязвимостей?

**Ответ:**

**(1)** определения квалификации злоумышленника
**(2)** категорирования рисков
**(3) (+)** вычисления коэффициента значимости угрозы
**(4)** выбора контрмер

---

**Вопрос 34**

Какая формула применяется для оценки риска?

**Ответ:**

**(1)** сложение вероятности осуществления угрозы и величины предполагаемого ущерба
**(2)** вычитание вероятности осуществления угрозы (в процентах) из величины предполагаемого ущерба
**(3)** деление вероятности осуществления угрозы (в процентах) на величину предполагаемого ущерба
**(4) (+)** умножение вероятности осуществления угрозы на величину предполагаемого ущерба

---

**Вопрос 35**

Как называется устранение источника риска или направление его действия на некритичные объекты?

**Ответ:**

**(1)** принятие
**(2)** смягчение
**(3)** передача
**(4) (+)** уклонение

---

**Вопрос 36**

Если риск приемлемый, на что будет направлена политика информационной безопасности?

**Ответ:**

**(1) (+)** принятие
**(2)** смягчение
**(3)** передача
**(4)** уклонение

---

**Вопрос 37**

Если риск оправданный, на что будет направлена политика информационной безопасности?

**Ответ:**

**(1)** принятие
**(2) (+)** смягчение
**(3) (+)** передача
**(4)** уклонение

---

**Вопрос 38**

Если риск недопустимый, на что будет направлена политика информационной безопасности?

**Ответ:**

**(1)** принятие
**(2)** смягчение
**(3)** передача
**(4) (+)** уклонение

---

**Вопрос 39**

Как называется подтверждение возможности негативной ситуации и сознательное решение принять последствия?

**Ответ:**

**(1) (+)** принятие
**(2)** смягчение
**(3)** передача
**(4)** уклонение

---

**Вопрос 40**

Как называется минимизация влияния негативной ситуации при невозможности устранения источника риска?

**Ответ:**

**(1)** принятие
**(2) (+)** смягчение
**(3)** передача
**(4)** уклонение

---

**Вопрос 41**

Как называется перенесение ответственности за принятие и управление риском на других участников совместной деятельности без его устранения?

**Ответ:**

**(1)** принятие
**(2)** смягчение
**(3) (+)** передача
**(4)** уклонение

---

**Вопрос 42**

Идентифицируется ли риск уязвимостью, через которую может быть реализована некая угроза в отношении определенного ресурса?

**Ответ:**

**(1) (+)** да
**(2)** нет
**(3)** да, но только в случае отсутствия угрозы

---

**Вопрос 43**

Какие из перечисленных вариантов решений в отношении рисков являются неуместными:

**Ответ:**

**(1)** принят, устранен
**(2)** принят, дезавуирован
**(3) (+)** дезавуирован, отклонен

---

**Вопрос 44**
На основании каких из перечисленных документов разрабатываются задания по безопасности?
**Ответ:**

**(1)** каталог сертифицированных профилей защиты и продуктов
**(2)** технический регламент
**(3) (+)** профиль защиты

---

**Вопрос 45**
Что представляет собой событие - триггер?
**Ответ:**

**(1) (+)** событие, повлекшее реализацию или дальнейшее развитие рисков и являющееся идентификатором риска
**(2)** событие, увеличивающее время отклика web - сервера
**(3)** это одна из разновидностей атак на сервер

---

**Вопрос 46**
Что достигается посредством оценки рисков организации?
**Ответ:**

**(1) (+)** анализируется вероятность возникновения угроз, а также оценка возможных последствий
**(2) (+)** происходит выявление угроз активам организации
**(3) (+)** осуществляется изучение уязвимости соответствующих активов

---

**Вопрос 47**
В каких целях осуществляется анализ рисков?
**Ответ:**

**(1)** в целях соблюдения требований об обязательной отчетности учреждения, его проведение формально необходимо
**(2) (+)** в целях установления и поддержания эффективного управления системой защиты
**(3)** в целях укрепления имиджевой политики учреждения

---

**Вопрос 48**
В каких целях разрабатываются методы реагирования в случае инцидентов?
**Ответ:**

**(1) (+)** в целях обеспечения эффективных мер защиты
**(2)** в целях обеспечения расширения функционала сотрудников учреждения
**(3) (+)** в целях обеспечения скорейшего восстановления работоспособности системы в случае инцидентов

---

**Вопрос 49**
Какова связь анализа рисков с другими компонентами модели информационной безопасности?
**Ответ:**

**(1) (+)** на базе полученных результатов по оценке рисков осуществляется анализ состояния системы и разрабатывается план построения системы защиты сети
**(2)** анализ рисков увязан с процедурами анализа рисков
**(3)** анализ не увязывается с другими компонентами системы

---

**Вопрос 50**
Являются ли термины управление рисками и оценка рисков взаимозаменяемыми?
**Ответ:**

**(1) (+)** нет
**(2)** да
**(3)** лишь частично

---

**Вопрос 51**
К какому состоянию зрелости управления рисками безопасности согласно методики фирмы Microsoft относится уровень, когда процесс управления рисками глубоко изучен сотрудниками и в значительной степени автоматизирован?
**Ответ:**

**(1)** управляемый
**(2) (+)** оптимизированный

---

**Вопрос 52**
К какому состоянию зрелости управления рисками безопасности, согласно методики фирмы Microsoft, относится уровень, когда процесс документирован не полностью, но управление рисками является всеобъемлющим и руководство вовлечено в управление рисками?
**Ответ:**

**(1)** оптимизированный
**(2) (+)** повторяемый
**(3)** узкоспециализированный

---

**Вопрос 53**
К какому состоянию зрелости управления рисками безопасности согласно методики фирмы Microsoft относится уровень, когда политики и процессы в организации не документированы, процессы не являются полностью повторяемыми?
**Ответ:**

**(1)** оптимизированный
**(2)** повторяемый
**(3) (+)** узкоспециализированный

---

**Вопрос 54**
К какому состоянию зрелости управления рисками безопасности согласно методики фирмы Microsoft относится уровень, когда принято формальное решение об интенсивном внедрении управления рисками, разработан базовый процесс и внедряется управление рисками?
**Ответ:**

**(1)** **(+)** наличие определенного процесса
**(2)** повторяемый
**(3)** оптимизированный

---

**Вопрос 55**
Является ли возможным в процессе идентификации рисков определить цели потенциального нарушителя и уровни защиты, на которых можно ему противостоять?
**Ответ:**

**(1)** нет
**(2)** **(+)** да
**(3)** нет, но такая попытка может дать некий эффект

---

**Вопрос 56**
Способствует ли организация защиты от угрозы на нескольких уровнях снижению уровня риска?
**Ответ:**

**(1)** **(+)** да
**(2)** нет
**(3)** спорно

---

**Вопрос 57**
Какая из перечисленных распространенных методик анализа рисков использует метод оценки риска на качественном уровне (например, по шкале "высокий", "средний", "низкий")?
**Ответ:**

**(1)** FRAP
**(2)** RiskWatch
**(3)** **(+)** CRAMM

---

**Вопрос 58**
Какая из перечисленных распространенных методик анализа рисков использует количественные методики оценки рисков?
**Ответ:**

**(1)** FRAP
**(2)** **(+)** RiskWatch
**(3)** CRAMM
**(4)** Microsoft

---

**Вопрос 59**
Какие из перечисленных распространенных методик анализа рисков используют смешанный метод оценки риска?
**Ответ:**

**(1)** **(+)** CRAMM
**(2)** **(+)** Microsoft
**(3)** RiskWatch
**(4)** FRAP

---

**Вопрос 60**

Чем определяется ценность физических ресурсов в методике CRAMM?

**Ответ:**

**(1)** временем, необходимым на восстановление в случае разрушения

**(2)** объемом финансовых активов организации

**(3) (+)** стоимостью их восстановления в случае разрушения

---

**Вопрос 61**

Какому значению по шкале оценки уязвимости CRAMM соответствует инцидент, происходящий в среднем один раз в четыре месяца?

**Ответ:**

**(1)** очень низкий

**(2)** очень высокий

**(3) (+)** высокий

---

**Вопрос 62**

Какому из перечисленных значений по шкале оценки уязвимости CRAMM соответствует инцидент, если вероятность развития событий по наихудшему сценарию составляет от 0, 33 до 0,66?

**Ответ:**

**(1)** высокий

**(2)** низкий

**(3) (+)** средний

---

**Вопрос 63**

Как в методике FRAP осуществляется определение защищаемых активов?

**Ответ:**

**(1)** по результатам заполнения опросных листов и автоматизированного анализа (сканирования) сетей

**(2)** по результатам изучения документации на систему

**(3) (+)** по результатам заполнения опросных листов, изучения документации на систему, использования инструментов автоматизированного анализа (сканирования) сетей

---

**Вопрос 64**

Что из перечисленного характерно для методики OCTAVE?

**Ответ:**

**(1)** весь процесс анализа автоматизирован, производится на основании параметрических функций

**(2) (+)** весь процесс анализа производится силами сотрудников организации, без привлечения внешних консультантов

**(3)** весь процесс анализа производится силами внешних консультантов, без привлечения сотрудников организации

---

**Вопрос 65**

Какие из перечисленных критериев оценки и управления рисками используются в методике RiskWatch?

**Ответ:**

**(1) (+)** годовые потери (Annual Loss Expectancy, ALE) и оценка возврата инвестиций (Return on Investment, ROI)
**(2)** угрозы, исходящие от человека-нарушителя, действующего через сеть передачи данных
**(3)** влияние потерь на HR - аспект деятельности организации

---

**Вопрос 66**
Какую величину, согласно методике Microsoft, определяют произведением стоимости актива на фактор подверженности воздействию?
**Ответ:**

**(1)** качественную оценку влияния
**(2)** Фактор подверженности воздействию
**(3) (+)** количественную оценку влияния

---

**Вопрос 67**
При вычислении вероятности влияния результирующий уровень вероятности определяется на основании двух значений. Первое значение определяет вероятность существования уязвимости в текущей среде. Что определяет второе значение?
**Ответ:**

**(1)** изменения останова сервера по причине физического износа оборудования
**(2) (+)** вероятность существования уязвимости исходя из эффективности текущих элементов контроля
**(3)** вероятность существования уязвимости при гипотетических параметрах систе

---

**Вопрос 68**
Позволяет проведение анализа рисков в сфере информационной безопасности определять уязвимость отдельных компонентов и недостатки политики системы?
**Ответ:**

**(1) (+)** да, гарантированно позволяет
**(2)** несмотря на то, что в целом проблема определения уязвимости системы решается, определение уязвимости компонентов достичь нельзя
**(3)** нет, не позволяет

---

**Вопрос 69**
Какие из перечисленных распространенных методик анализа рисков не используют количественные методики оценки рисков?
**Ответ:**

**(1) (+)** FRAP
**(2)** RiskWatch
**(3) (+)** CRAMM

---

**Вопрос 70**
Что обеспечивает ранжирование рисков по приоритетам?
**Ответ:**

**(1)** возможность системного анализа рисков
**(2) (+)** возможность выделить наиболее приоритетные направления для внедрения новых СЗИ, мер и процедур обеспечения ИБ
**(3)** возможность оценить выгоды от внедрения средств и механизмов защиты и принять участие в процессе определения требуемого уровня защищенности КС

---

**Вопрос 71**

Позволяет проведение анализа рисков в сфере информационной безопасности выделить наиболее приоритетные направления для внедрения новых средств защиты информации?

**Ответ:**

**(1)** да, но с ограничениями
**(2)** нет, не позволяет
**(3) (+)** да, гарантированно позволяет

---

**Вопрос 72**

Какие из перечисленных классов активов входят в систему оценки и управления рисками безопасности, предлагаемый корпорацией Майкрософт?

**Ответ:**

**(1) (+)** активы, имеющие среднее влияние на бизнес (СВБ)
**(2) (+)** активы, имеющие низкое влияние на бизнес (НВБ)
**(3) (+)** активы, имеющие высокое влияние на бизнес(ВВБ)
**(4)** активы, имеющие приоритеное влияние на бизнес(ПВБ)

---

**Вопрос 73**

Какому значению по шкале оценки уязвимости CRAMM соответствует инцидент, происходящий в среднем один раз в три года?

**Ответ:**

**(1)** высокий
**(2) (+)** низкий
**(3)** средний

---

**Вопрос 74**

По каким из перечисленных критериев осуществляется определение защищаемых активов в методике FRAP?

**Ответ:**

**(1) (+)** по результатам изучения документации на систему
**(2) (+)** по результатам автоматизированного анализа (сканирования) сетей
**(3) (+)** по результатам заполнения опросных листов

---

**Вопрос 75**

Основой для автоматизированного анализа рисков является:

**Ответ:**

**(1)** список персонала предприятия и оценка уровня его подготовки
**(2) (+)** перечень информационных активов и соответствующие этим активам угрозы
**(3)** перечень политик безопасности

---

**Вопрос 76**

Оценка рисков по методологии CRAMM является:

**Ответ:**

**(1)** основным результатом аудита информационной безопасности
**(2) (+)** основой для выработки системы контрмер
**(3)** показателем эффективности вложений в средства информационной безопасности

---

**Вопрос 77**
К негативным факторам, ограничивающим передачу на аутсорсинг функций по обеспечению информационной безопасности, относятся:
**Ответ:**

**(1)** высокий уровень затрат на услуги, предоставляемыми сторонними организациями-поставщиками услуг
**(2) (+)** доступ предприятия-поставщика услуг к конфиденциальной информации
**(3) (+)** потенциальная возможность перехвата и утечки информации в процессе оказания услуг сторонней организацией

---

**Вопрос 78**
При проведении тестового преодоления защиты внешними аудиторами договор с заказчиком таких услуг должен предусматривать:
**Ответ:**

**(1)** конкретный детализированный план тестового проникновения
**(2)** порядок уведомления всех заинтересованных сотрудников предприятия-заказчика о предстоящем тестовом проникновении
**(3) (+)** снятие ответственности с аудитора за возможный ущерб, который может быть нанесен в процессе такого проникновения

---

**Вопрос 79**
Сложность экономического анализа вложений в информационную безопасность определяется:
**Ответ:**

**(1) (+)** большим числом возможных сценариев нападения на информационные ресурсы
**(2) (+)** постоянным динамичным развитием как средств защиты, так и средств нападения
**(3)** частым изменением правовых норм и требований в сфере информационной безопасности

---

**Вопрос 80**
Как называется показатель, количественно выражающийся суммой ежегодных прямых и косвенных затрат на функционирование корпоративной системы защиты информации?
**Ответ:**

**(1)** экономическая эффективность бизнеса
**(2)** общая величина затрат на внедрение системы ИБ
**(3) (+)** совокупная стоимость владения системой ИБ
**(4)** коэффициент возврата инвестиций

---

**Вопрос 81**
К каким затратам относятся потери в результате простоев, сбоев в работе и отказов корпоративной системы защиты информации?
**Ответ:**

**(1)** прямые
**(2) (+)** косвенные

**Вопрос 82**

К каким затратам относятся затраты на покупку аппаратного и программного обеспечения для корпоративной системы защиты информации?

**Ответ:**

**(1) (+)** прямые
**(2)** косвенные

---

**Вопрос 83**

В каком случае возникает угроза «разорения» от защиты?

**Ответ:**

**(1)** когда мера общей эффективности защиты близка к 100%
**(2) (+)** когда рентабельность защиты имеет отрицательное значение
**(3)** когда рентабельность защиты имеет положительное значение
**(4)** когда вероятность реализации какой-то угрозы более 60%

---

**Вопрос 84**

Как вычисляется рентабельность защиты?

**Ответ:**

**(1)** сумма защищенности и относительных затрат на ресурсы
**(2)** произведение защищенности и относительных затрат на ресурсы
**(3)** отношение защищенности и относительных затрат на ресурсы
**(4) (+)** разность защищенности и относительных затрат на ресурсы

---

**Вопрос 85**

Какие из перечисленных мер рекомендуется выполнять для обеспечения непрерывности бизнес-процессов?

**Ответ:**

**(1) (+)** требуется идентифицировать события, которые могут быть причиной прерывания бизнес-процессов
**(2) (+)** требуется провести оценку последствий, после чего разработать планы восстановления
**(3)** требуется согласовать порядок компенсации потенциального ущерба

---

**Вопрос 86**

Для чего  необходимо проводить мониторинг системы безопасности?

**Ответ:**

**(1)** в целях формирования требований политики контроля доступа
**(2)** в целях обеспечения релевантности действий сотрудников учреждения
**(3) (+)** в целях обеспечения доказательства на случай выявления инцидентов нарушения информационной безопасности

---

**Вопрос 87**

Как называется семейство «добровольных стандартов» Великобритании, помогающих организациям на практике сформировать программы безопасности?

**Ответ:**

**(1)** NIST 7799
**(2)** IEEE 7799
**(3)** **(+)** BS 7799
**(4)** PS 7799

---

**Вопрос 88**
Чему посвящен британский стандарт BS 7799?
**Ответ:**

**(1)** построению корпоративной системы информационной безопасности
**(2)** **(+)** управлению информационной безопасностью
**(3)** оценке рисков
**(4)** выбору критерии оценки механизмов безопасности

---

**Вопрос 89**
Какой из стандартов ISO отражает британский стандарт BS 7799?
**Ответ:**

**(1)** ISO 10181
**(2)** ISO 13335
**(3)** ISO 15408
**(4)** **(+)** ISO/IEC 17799

---

**Вопрос 90**
Какой подход предлагает ГОСТ Р ИСО/МЭК 17799 по работе с системами менеджмента информационной безопасности?
**Ответ:**

**(1)** **(+)** процессный подход
**(2)** клиринговый подход
**(3)** методика хеджирования рисков

---

**Вопрос 91**

На каком из этапов в ГОСТ Р ИСО/МЭК 17799 предполагается выполнение следующих пунктов системы менеджмента информационной безопасности:

- определить способ измерения результативности выбранных мер управления;
- реализовать программы по обучению и повышению квалификации сотрудников;

**Ответ:**

**(1)** **(+)** этап "внедрение и функционирование системы менеджмента информационной безопасности"
**(2)** этап "проведение мониторинга и анализа системы менеджмента информационной безопасности"
**(3)** этап разработки системы менеджмента информационной безопасности

---

**Вопрос 92**
Какие из перечисленных мер ГОСТ Р ИСО/МЭК 17799 предлагает выполнять на этапе "поддержка"?
**Ответ:**

**(1)** **(+)** выявлять возможности улучшения системы менеджмента информационной безопасности; предпринимать необходимые корректирующие и предупреждающие действия, использовать на практике опыт по обеспечению ин-

формационной безопасности, полученный как в собственной организации, так и в других организациях;

**(2) (+)** передавать подробную информацию о действиях по улучшению системы менеджмента информационной безопасности всем заинтересованным сторонам, при этом степень ее детализации должна соответствовать обстоятельствам и, при необходимости, согласовывать дальнейшие действия;
**(3) (+)** обеспечивать внедрение улучшений системы менеджмента информационной безопасности для достижения запланированных целей

---

**Вопрос 93**
Что из перечисленного входит в требования ГОСТ Р ИСО/МЭК 17799 к документации?
**Ответ:**

**(1) (+)** положения политики системы менеджмента информационной безопасности и описание области функционирования, описание методики и отчет об оценке рисков
**(2) (+)** план обработки рисков, документирование связанных процедур

**(3) (+)** положение, предписывающее определять процесс управления документами системы менеджмента информационной безопасности, включающий актуализацию, использование, хранение и уничтожение

---

**Вопрос 94**
Какие из перечисленных работ по улучшению системы менеджмента информационной безопасности входят в ГОСТ Р ИСО/МЭК 17799?
**Ответ:**

**(1) (+)** работы по улучшению системы менеджмента информационной безопасности
**(2) (+)** работы по обеспечению уровня соответствия текущего состояния системы, предъявляемым к ней требованиям
**(3)** работы по обеспечению надлежащей политики управления активами в организации
**(4)** работы по обеспечению экономической эффективности организации
**(5)** работы по обеспечению организацией требований экологии

---

**Вопрос 95**
К какому аспекту мероприятий по защите информации относится формирование политики информационной безопасности?
**Ответ:**

**(1)** законодательный
**(2) (+)** организационный
**(3)** программно-технический

---

**Вопрос 96**

На каком уровне политики информационной безопасности цели организации в области информационной безопасности формулируются в терминах целостности, доступности и конфиденциальности?
**Ответ:**

**(1) (+)** верхний
**(2)** средний
**(3)** нижний

**Вопрос 97**

К какому уровню политики информационной безопасности относятся вопросы доступа к тому или иному сервису?

**Ответ:**

**(1)** верхний
**(2)** средний
**(3) (+)** нижний

---

**Вопрос 98**

За что отвечает программа информационной безопасности нижнего уровня в организации?

**Ответ:**

**(1)** контроль за тем, чтобы действия организации не противоречили федеральным и региональным законам и нормативным актам
**(2)** выработка стратегии организации в области информационной безопасности
**(3) (+)** обеспечение надежной и экономичной защиты информационных подсистем, конкретных сервисов или групп однородных сервисов

---

**Вопрос 99**

За что отвечает программа информационной безопасности верхнего уровня в организации?

**Ответ:**

**(1) (+)** контроль за тем, чтобы действия организации не противоречили федеральным и региональным законам и нормативным актам
**(2) (+)** выработка стратегии организации в области информационной безопасности
**(3)** обеспечение надежной и экономичной защиты информационных подсистем, конкретных сервисов или групп однородных сервисов

---

**Вопрос 100**

Что такое метрика?

**Ответ:**

**(1)** адаптивное СЗИ
**(2)** количественный показатель
**(3) (+)** качественный показатель
**(4)** универсальный показатель

---

**Вопрос 101**

С какой целью при разработке и реализации политики безопасности используются метрики?

**Ответ:**

**(1)** для определения рамок, в которых осуществляются мероприятия по обеспечению безопасности информации, и задаются критерии оценки полученных результатов
**(2)** для замеров уровней безопасности
**(3) (+)** с целью определения параметров защищенности системы, что позволяет соотнести сделанные затраты и полученный эффект

---

**Вопрос 102**

Определите процедуру, которая должна быть проведена с целью оценки соответствия требованиям по безопасности информации принятых на объекте мер по защите информации:

**Ответ:**

**(1)** Сертификация
**(2) (+)** Аттестация
**(3)** Аккредитация
**(4)** Лицензирование

---

**Вопрос 103**

По результатам проведения комплекса организационно-технических мероприятий, в результате которых подтверждается, что объект информатизации соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации выдается:

**Ответ:**

**(1) (+)** Аттестат соответствия
**(2)** Аттестат аккредитации
**(3)** Сертификат соответствия
**(4)** Лицензия
**(5)** Заключение
**(6)** Предписание

---

**Вопрос 104**

Аттестация объекта информатизации проводится:

**Ответ:**

**(1) (+)** В реальных условиях эксплуатации
**(2)** В специальной лаборатории органа по аттестации
**(3)** В экранированной камере
**(4)** На территории заявителя, в помещении площадью не менее 20 кв.м.

---

**Вопрос 105**

Проверка объекта информатизации в целях выявления и изъятия возможно внедренных закладочных устройств- это:

**Ответ:**

**(1)** Специальные исследования
**(2)** Оценка защищенности
**(3) (+)** Специальная проверка
**(4)** Контроль эффективности

---

**Вопрос 106**

Выявление с использованием контрольно-измерительной аппаратуры возможных технических каналов утечки защищаемой информации от ОТСС и ВТСС:

**Ответ:**

**(1)** Специальная проверка
**(2)** Контроль защищенности
**(3) (+)** Специальные исследования
**(4)** Анализ уязвимости

---

**Вопрос 107**
Выделите утверждение, верное в отношении защиты сетей.
**Ответ:**

**(1)** уровень защищенности сети определяется уровнем защищенности ее самого «сильного» звена
**(2)** уровень защищенности сети определяется суммой уровней защищенности ее звеньев
**(3) (+)** уровень защищенности сети определяется уровнем защищенности ее самого «слабого» звена
**(4)** уровень защищенности сети не зависит напрямую от защищенности ее отдельных звеньев

---

**Вопрос 108**
Что означает система защиты с полным перекрытием?
**Ответ:**

**(1)** для половины (и более) уязвимостей есть устраняющие барьеры
**(2) (+)** для любой уязвимости есть устраняющий ее барьер
**(3)** у любой уязвимости есть риск ее реализации
**(4)** количество уязвимостей меньше, чем количество препятствующих им барьеров

---

**Вопрос 108**
Чем характеризуется степень сопротивляемости механизма защиты?
**Ответ:**

**(1) (+)** вероятностью его преодоления
**(2)** количеством угроз, которым этот механизм препятствует
**(3)** величиной потерь в случае успешного прохождения
**(4)** стоимостью механизма защиты

---

**Вопрос 109**
В чем заключается принцип минимизации привилегий?
**Ответ:**

**(1)** выделение полных прав доступа только администраторам системы
**(2) (+)** выделение только тех прав, которые необходимы для реализации своих должностных обязанностей
**(3)** выделение прав доступа в зависимости от величины возможного ущерба

---

**Вопрос 110**
С какой целью проводится контроль эффективности защиты информации?
**Ответ:**

**(1)** Проверки правильности установки средств защиты информации
**(2)** Проверки отсутствия возможно внедренных закладных устройств
**(3) (+)** Проверки достаточности принятых мер по защите информации
**(4) (+)** Проверки выполнения заданных требований по защите информации

---

**Вопрос 111**
Проведение контроля эффективности принятых мер по защите информации на объекте ин-

форматизации проводится в рамках:

**Ответ:**

**(1)** Экспертно-документальной оценки
**(2)** Оценка эффективности функционирования средств защиты от несанкционированного доступа
**(3) (+)** Инструментальных измерений и оценки защищенности

---

**Вопрос 112**

Какие мероприятия проводятся в рамках проверки подсистемы управления доступом:

**Ответ:**

**(1)** Проверка настроек осуществления записей событий в системный журнал
**(2) (+)** Оценка соответствия реализованных правил разграничения доступа заявленным требованиям
**(3) (+)** Проверка аутентификации субъектов доступа при входе в систему
**(4)** Проверка наличия средств восстановления СЗИ от несанкционированного доступа

---

**Вопрос 113**

В ходе контроля за обеспечением уровня защищенности информации, обрабатываемой объектом информатизации осуществляется:

**Ответ:**

**(1) (+)** Анализ и оценка функционирования системы защиты информации объекта информатизации
**(2) (+)** Периодический анализ изменения угроз безопасности информации
**(3)** Регистрация и анализ событий, связанных с защитой информации
**(4)** Информирование пользователей об угрозах безопасности информации

---

**Вопрос 114**

К объектам информатизации, подлежащим аттестации по требованиям безопасности информации относятся:

**Ответ:**

**(1)** Средства защиты информации
**(2) (+)** Защищаемые помещения
**(3)** Операционные системы и прикладные программы
**(4) (+)** Автоматизированные системы

---

**Вопрос 115**

При проведении ремонта технических средств объекта информатизации допускается ли их передача ремонтной организации?

**Ответ:**

**(1)** Да, в полном объеме
**(2) (+)** Да, за исключением носителей информации
**(3)** Да, в полном объеме, с разрешения органа по аттестации
**(4)** Не допускается проведение ремонта технических средств аттестованного объекта информатизации

---

**Вопрос 116**

При необходимости проведения ремонта технических средств, входящих в состав объекта информатизации:

**Ответ:**

**(1) (+)** Ремонт осуществляться только в присутствии должностного лица, ответственного за объект информатизации

**(2) (+)** Осуществляется резервное копирование информации с целью возможности ее восстановления в случае выхода из строя накопителей
**(3) (+)** Технические средства передаются в ремонтную организацию без накопителей информации
**(4)** Технические средства, подлежащие ремонту, самостоятельно заменяются заявителем на аналогичные

---

**Вопрос 117**

Укажите мероприятия, проводимые органом по аттестации в рамках предварительного ознакомления с аттестуемым объектом информатизации:
**Ответ:**

**(1)** Анализ результатов оценки эффективности средств защиты информации
**(2) (+)** Анализ размещения объекта информатизации относительно границ контролируемой зоны
**(3)** Анализ системы электроснабжения, заземления, инженерных коммуникаций
**(4) (+)** Выработка рекомендаций по подготовке объекта к аттестации
**(5)** Проверка правильности установки средств защиты информации

---

**Вопрос 118**
Какие действия включает в себя комплекс работ по аттестации объекта информатизации?
**Ответ:**

**(1) (+)** Определение угроз безопасности информации
**(2) (+)** Разработка и реализация разрешительной системы доступа
**(3) (+)** Настройка сертифицированных средств защиты информации
**(4)** Обучение сотрудников заявителя вопросам защиты информациис выдачей документа, подтверждающего прохождение обучения

---

**Вопрос 119**
Государственные информационные системы – это:
**Ответ:**

**(1)** Системы, создаваемые государством для собственных нужд
**(2) (+)** Системы, создаваемые с целью реализации полномочий государственных органов
**(3)** Системы, доступ к которым имеют только государственные органы
**(4) (+)** Системы, созданные для обеспечения обмена информацией между государственными органами

---

**Вопрос 120**
Определите мероприятия, которые необходимо осуществлять в ходе эксплуатации аттестованной ГИС:
**Ответ:**

**(1) (+)** Мониторинг за обеспечением уровня безопасности информации
**(2) (+)** Выявление инцидентов и реагирование на них
**(3) (+)** Администрирование системы защиты информации
**(4) (+)** Управление конфигурацией аттестованного объекта информатизации

---

**Вопрос 121**

В ходе управления системой защиты информации аттестованной ГИС осуществляется:

**Ответ:**

**(1) (+)** Регистрация и анализ событий, связанных с защитой информации

**(2) (+)** Управление средствами защиты информации объекта информатизации

**(3)** Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий

**(4)** Периодический анализ изменения угроз безопасности информации

---

**Вопрос 122**

В рамках управления конфигурацией аттестованной ГИС и ее системы защиты информации осуществляется:

**Ответ:**

**(1) (+)** Анализ потенциального воздействия планируемых изменений на обеспечение защиты информации

**(2)** Контроль за событиями безопасности и действиями пользователей при обработке информации

**(3)** Регистрация и анализ событий, связанных с защитой информации

**(4) (+)** Определение параметров настройки программного обеспечения

---

**Вопрос 123**

К защищаемым помещениям относятся:

**Ответ:**

**(1)** Помещения для ведения секретных переговоров

**(2) (+)** Помещения для проведения переговоров с обсуждением конфиденциальной информации

**(3)** Помещения для хранения документов, содержащих информацию ограниченного доступа

**(4) (+)** Помещения для проведения совещания с доведением информации, содержащей коммерческую тайну

---

**Вопрос 124**

Что такое защищаемое помещение?

**Ответ:**

**(1)** Помещение, в котором хранятся носители сведений, содержащие информацию ограниченного доступа

**(2)** Помещение, в котором планируется в ходе закрытых совещанийобсуждать информацию, содержащую сведения, составляющие государственную тайну

**(3)** Помещение, которое защищено с точки зрения вопросов защиты информации

**(4) (+)** Помещение, в котором планируется в ходе закрытых совещаний обсуждать информацию ограниченного доступа, не содержащую сведения, составляющие государственную тайну

---

**Вопрос 125**

Какие разделы включает в себя Технический паспорт на защищаемое помещение?

**Ответ:**

**(1) (+)** Перечень мебели и предметов интерьера

**(2)** Порядок проведения совещаний в защищаемом помещении

**(3) (+)** Схема сети электропитания и заземления

**(4) (+)** Сведения об аттестации объекта информатизации

---

**Вопрос 126**

Необходимо ли при проведении аттестации объекта информатизации – защищаемого поме-

щения разрабатывать модель нарушителя?

**Ответ:**

**(1)** Да
**(2) (+)** Нет

---

**Вопрос 127**

Контролируемая зона – это

**Ответ:**

**(1)** Пространство вокруг объекта информатизации, в котором запрещено обрабатывать информацию ограниченного доступа
**(2)** Пространство вокруг объекта информатизации, в котором исключена возможность несанкционированного доступа к информации
**(3) (+)** Пространство вокруг объекта информатизации, в котором исключено неконтролируемое пребывание посторонних лиц, а также движение транспортных средств

---

**Вопрос 128**

Что включает в себя организационно-распорядительная документация разрешительной системы доступа сотрудников к защищаемым ресурсам автоматизированной системы?

**Ответ:**

**(1) (+)** Перечень обрабатываемых в автоматизированной системе информационных ресурсов
**(2)** Перечень программного обеспечения, установленного на объекте информатизации
**(3)** Инструкции, определяющие порядок обработки информации в автоматизированной системе
**(4) (+)** Перечень должностных лиц, допущенных к работе в автоматизированной системе

---

**Вопрос 129**

Какие инструкции должны быть разработаны для объекта информатизации – автоматизированной системы?

**Ответ:**

**(1) (+)** Инструкция по организации антивирусной защиты
**(2) (+)** Инструкция по организации парольной защиты
**(3)** Инструкция по подготовке объекта информатизации к аттестации
**(4)** Инструкция по обновлению антивирусной системы
**(5) (+)** Инструкция пользователю автоматизированной системы
**(6)** Инструкция по настройке и внесению изменений в штатную работу средств защиты информации

---

**Вопрос 130**

Анализ действий нарушителя необходим для:

**Ответ:**

**(1)** проверки правильности настроек систем защиты информации
**(2) (+)** установления сведений, известных нарушителю до нападения
**(3) (+)** установления круга контактов, которые могли быть у нарушителя до нападения

---

**Вопрос 131**

Кто такой инсайдер?

**Ответ:**

**(1) (+)** сотрудник являющийся источником утечки информации
**(2)** любой источник утечки информации
**(3)** программа-вирус являющаяся источником утечки информации

---

**Вопрос 132**
Какие из ниже перечисленных видов нарушителей действуют с умыслом?
**Ответ:**

**(1)** халатные
**(2)** манипулируемые
**(3) (+)** саботажники
**(4) (+)** нелояльные
**(5) (+)** мотивируемые извне

---

**Вопрос 132**
Какие из ниже перечисленных видов нарушителей действуют исходя из корыстных интересов?
**Ответ:**

**(1)** халатные
**(2)** манипулируемые
**(3) (+)** саботажники
**(4)** нелояльные
**(5) (+)** мотивируемые извне

---

**Вопрос 134**
Какие из ниже перечисленных видов нарушителей относится к группе незлонамеренных нарушителей?
**Ответ:**

**(1) (+)** халатные
**(2) (+)** манипулируемые
**(3)** саботажники
**(4)** нелояльные
**(5)** мотивируемые извне

---

**Вопрос 135**
Какие из ниже перечисленных видов нарушителей относится к группе злонамеренных нарушителей?
**Ответ:**

**(1)** халатные
**(2)** манипулируемые
**(3) (+)** саботажники
**(4) (+)** нелояльные
**(5) (+)** мотивируемые извне

---

**Вопрос 136**
Какие нарушители правил хранения конфиденциальной информации относятся к типу "мо-

тивированные извне"?

**Ответ:**

**(1)** **(+)** сотрудники специально устроенные на работу для похищения информации
**(2)** **(+)** подкупленные или запуганные сотрудники
**(3)** сотрудники, стремящиеся нанести вред компании из-за личных мотивов

---

**Вопрос 137**

Против нарушителей правил хранения конфиденциальной информации какого типа действенными являются простые технические средства предотвращения каналов утечек - контентная фильтрация исходящего трафика в сочетании с менеджерами устройств ввода-вывода?

**Ответ:**

**(1)** **(+)** халатные
**(2)** мотивируемые извне
**(3)** саботажники
**(4)** нелояльные

---

**Вопрос 138**

Какой вид нарушителей правил хранения конфиденциальной информации совершают их, действуя из лучших побуждений?

**Ответ:**

**(1)** **(+)** халатные
**(2)** **(+)** манипулируемые
**(3)** саботажники
**(4)** нелояльные
**(5)** мотивируемые извне

---

**Вопрос 139**

Сотрудники, стремящиеся нанести вред компании из-за личных мотивов относятся к типу

**Ответ:**

**(1)** **(+)** саботажник
**(2)** внедренный
**(3)** нелояльный

---

**Вопрос 140**

Каков мотив нарушения правил хранения конфиденциальной информации у сотрудников относящихся к типу "саботажник"?

**Ответ:**

**(1)** личная нажива
**(2)** **(+)** месть
**(3)** шантаж
**(4)** "саботажники" нарушают правил хранения конфиденциальной информации не осознавая этого

---

**Вопрос 141**

Каков мотив нарушения правил хранения конфиденциальной информации у сотрудников относящихся к типу "нелояльный"?

**Ответ:**

**(1)** личная нажива
**(2)** месть
**(3) (+)** шантаж
**(4)** "нелояльные" сотрудники нарушают правил хранения конфиденциальной информации не осознавая этого

---

**Вопрос 142**

Каков мотив нарушения правил хранения конфиденциальной информации у сотрудников относящихся к типу "внедренный"?

**Ответ:**

**(1) (+)** личная нажива
**(2)** месть
**(3)** шантаж
**(4)** "внедренные" сотрудники нарушают правил хранения конфиденциальной информации не осознавая этого

---

**Вопрос 143**

Почему при использовании режима активной защиты для контролирования информационных потоков необходимо постоянное присутствие офицера информационной безопасности?

**Ответ:**

**(1) (+)** для разбора спорных случаев и ложных срабатываний
**(2)** для оперативной установки программного обеспечения
**(3)** для оперативного реагирования на возникающие нарушения
**(4)** при использовании режима активной защиты постоянное присутствие офицера информационной безопасности вовсе не обязательно

## Типовые теоретические вопросы:

1. Какой стандарт (серия стандартов) стал основоположником стандартизации систем управления ИБ?

Ответ:

Основоположником подобной стандартизации стала серия стандартов ISO 9000, предъявляющих требования к системам менеджмента качества, соблюдение которых позволяет контролировать качество выпускаемой продукции или предоставляемых услуг. При разработке стандартов на СУИБ многое было взять за основу именно из стандартов серии ISO 9000, например, основной подход - процессный подход и использование циклической модели PDCA для непрерывного совершенствования как самой системы, так и отдельных ее процессов. Помимо этого, отличительной особенностью стандартов ISO 9000, которая была перенята при стандартизации СУИБ, является то, что они устанавливают степень ответственности руководства компании за качество. Причем руководство предприятия

отвечает как за разработку политики в области качества, так и за внедрение и поддержание в рабочем состоянии системы менеджмента качества. Очень большое количество процессов управления из систем менеджмента качества с некоторыми изменениями присутствует и в СУИБ, например, внутренние аудиты ИБ, корректирующие и предупреждающие действия и г. д.

2. Для организации какой сферы применимы стандарты серии ISO/IEC 27000?

Ответ:

Стандарты серии 27000 включают в себя появление стандартов, более подробно раскрывающих требования к отдельным процессам управления ИБ. Базируясь на единой структуре и методологии, заложенной в ISO/IEC 27001:2005, они предоставляют руководства по управлению ИБ для различных сфер деятельности, включая финансовый и страховой сектор, здравоохранение, телекоммуникации и т. д.

3. Каковы отличительные черты серии стандартов ISO/IEC 27000?

Ответ:

Стандарты серии 27000 включают в себя появление стандартов, более подробно раскрывающих требования к отдельным процессам управления ИБ. Базируясь на единой структуре и методологии, заложенной в ISO/IEC 27001:2005, они предоставляют руководства по управлению ИБ для различных сфер деятельности, включая финансовый и страховой сектор, здравоохранение, телекоммуникации и т. д.

4. Какой из стандартов серии ISO/IEC 27000 содержит требования к созданию, внедрению, эксплуатации, мониторингу, анализу, сопровождению и совершенствованию СУИБ?

Ответ:

ISO/IEC 20733-1-2009 Безопасность сетей. Часть 1. Общие положения и концепции.

5. В чем состоят основные различия и сходства стандартов ISO/IEC 27001 и ITU-T X.1051?

Ответ:

ITU-T X.1051 основан на следующих документах:

ITU-T Recommendation X.800 (1991 г.) (Архитектура безопасности для взаимодействия открытых систем для CCITT- приложений),

ITU-T Recommendation X.805 (2003) (Архитектура безопасности для систем, обеспечивающих сквозные коммуникации),

ISO 9001:2000 (Системы менеджмента качества. Требования),

ISO 14001:1996 (Системы менеджмента окружающей среды. Спецификация с руководством по использованию),

ISO/IEC 27001,

ISO/IEC 27002,

ISO/IEC Guide 73:2002 (Управление рисками. Словарь. Руководство по использованию в стандартах).

Международный стандарт ISO/IEC 27001:2005 «Information technology. Security techniques. Information security management systems. Requirements» (Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента ИБ. Требования) содержит модель создания, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования СУИБ.

В России принят аналогичный ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмент информационной безопасности. Требования», идентичный 27001:2005. Основной объект рассмотрения стандарта в этом документе переведен как «система менеджмента ИБ» (СМИБ). Целью построения такой системы является выбор соответствующих мер управления ИБ, предназначенных для защиты информационных активов и гарантирующих доверие заинтересованных сторон.

6. Какой из стандартов серии ISO/IEC 27000 признан каталогом «лучших» практик по ИБ?

Ответ:

ISO/IEC 27002:2005 и ГОСТ Р ИСО/МЭК 17799-2005 - ПРАКТИЧЕСКИЕ ПРАВИЛА УПРАВЛЕНИЯ ИБ.

ГОСТ Р ИСО/МЭК 17799-2005 не является техническим стандартом и не зависит от конкретных средств защиты или технологий. Он описывает концептуальные основы управления ИБ и является признанным набором «лучших практик» по ОИБ.

7. В каком стандарте серии ISO/IEC 27000 содержится руководство по внедрению СУИБ?

Ответ:

Стандарт ISO/IEC 27003:2010 «Information Technology. Security Techniques. Information Security Management Systems Implementation Guidance» (Информационная технология. Методы и средства обеспечения безопасности. Руководство по внедрению систем менеджмента ИБ) является общим руководством по практическому применению стандартов серии 27000 и базируется на ISO/IEC 27000 и

27001, которые полезны для всех организаций, независимо от их размера, типа, сферы деятельности, сложности и имеющихся рисков ИБ. Основная цель стандарта - обеспечение руководства по проектированию такой СУИБ, на основе которой риски ИБ для информационных активов поддерживаются в пределах приемлемых границ, с учетом реализации требований, предъявляемых к СУИБ в ISO/IEC 27001.

8. Почему аспекты, связанные с управлением рисками ИБ, играют такое большое значение в рамках СУИБ?

Ответ:

Для того чтобы минимизировать вероятность реализации угрозы ИБ, необходимо применять защитные меры - организационные, технические и другие. Построение эффективной системы обеспечения ИБ (СОИБ) в условиях ограниченности всех видов ресурсов и времени, с учетом ценности активов и их уязвимостей и вероятных угроз ИБ для активов, а, значит, и выбор адекватных защитных мер, необходимых для достижения достаточного уровня ИБ, должны основываться на результатах анализа рисков ИБ. Эти результаты являются отправной точкой для установления и поддержки эффективного управления ИБ и обязательно используются при написании всех политик ИБ (ПолИБ) организации - корпоративной и частных - и выработки требований по ОИБ.

9. В каких основных международных и национальных стандартах рассматриваются вопросы, посвящённые рискам ИБ?

Ответ:

- Международный стандарт ISO/IEC 27005:2018 «Информационная технология. Методы и средства обеспечения безопасности. Управление рисками ИБ» и ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» содержат общее руководство по управлению рисками ИБ, которое может быть использовано в различных типах организаций и предназначено для «содействия адекватному ОИБ на основе риск-ориентированного подхода».

- Британский стандарт BS 7799-3:2006 «Системы менеджмента ИБ. Руководство по управлению рисками ИБ» содержит рекомендации по оценке рисков ИБ, их обработке, непрерывным действиям по управлению рисками ИБ и приложения с примерами активов, угроз ИБ, уязвимостей, методов оценки рисков ИБ.

10. Какой стандарт (серия стандартов) стал основоположником стандартизации систем управления ИБ?

Ответ:

Изначально это был стандарт ISO/IEC 17799:2005, который в связи с формирование группы стандартов 27000 был преобразован в стандарт ISO/IEC 27002:2005 (актуальная на сегодняшний день версия 27002:2013). «Information technology. Security techniques. Code of practice for information security management» (Информационная технология. Методы и средства обеспечения безопасности. Практические правила управления ИБ).

11. Какие определения ПолИБ даются в различных международных стандартах?

Ответ:

Согласно самому первому определению, приведенному в стандарте «Оранжевая книга» (Trusted Compute System Evaluation Criteria), ПолИБ – набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации

Гостехкомиссия России определила такую ПолИБ как правила разграничения доступа, представляющие собой совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа

В ГОСТ Р ИСО/МЭК 13335–1–2006 отдельно выделена ПолИБ ИТТ (англ. ITT security policy) – правила, директивы, сложившаяся практика, которые определяют, как в пределах организации и ее ИТТ управлять, защищать и распределять активы, в том числе критичную информацию

ПолИБ сети (англ. network security policy) в различных англоязычных стандартах определяется как документ, в рамках единой информационной инфраструктуры и СОИБ организации формально устанавливающий правила доступа к ее компьютерной сети, на основе которых пользователи этой сети (сотрудники и бизнес-партнеры организации) накапливают, применяют и распоряжаются ее активами.

12. В чем различие политик, стандартов, правил и процедур ОИБ?

Ответ:

Политика ОИБ – набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации

Стандарт (англ. standard) представляет собой правило, указывающее конкретное направление действий или ответную реакцию на данную ситуацию. Стандарты являются директивными указаниями (директивами), которые должны выполняться в соответствии с политиками и которые используются для определения соответствия этим политикам. Стандарты служат спецификациями для осуществления политик. Стандарты разработаны в целях содействия осуществлению

высокоуровневой политики организации. При разработке стандартов используются лучшие практики, накопленные в данной области. Тоже самое относится и к процедурам

Процедуры (англ. procedures) определяют конкретно, как политики, стандарты будут реализованы в данной ситуации. Процедуры – это технологии или процессы, зависимые от и имеющие отношение к конкретным платформам, приложениям или процессам. Они используются для выработки шагов, которые должны быть предприняты на организационном уровне для ОИБ отдельных систем и процессов. Процедуры, как правило, разработаны, реализованы и обеспечены организацией, владеющей процессом или системой. С целью обеспечения конкретных технических или процедурных требований внутри организации, где они применяются, процедуры как должны можно точнее поддерживать организационные политики, стандарты руководства. Примеры процедур: сертификация и аккредитация, оценка рисков ИБ, обнаружение вторжений, тесты на проникновение, реагирование на чрезвычайные ситуации, восстановление после аварий, резервирование, реагирование на инциденты ИБ.

Руководства (руководящие принципы, директивы) содержат рекомендации по тому, как должны выполняться другие требования. Они уточняют, что должно быть сделано и как с целью достижения целей, установленных в ПолИБ. Руководство является общим заявлением, используемым в качестве рекомендации или предлагающим подход к осуществлению политики и стандартов, например, при ОИБ.

13. Что такое трастовые модели?

Ответ:

В основе любой политики лежат модели доверия, или трастовые модели (англ. trusted models).

Для ИС наиболее точно смысл понятие «доверие» передает следующая формулировка: можно сказать, что один субъект «доверяет» другому, когда предполагает, что второй субъект будет вести себя точно так, как ожидает от него первый на основе их взаимодействия.

14. С каких точек зрения и как можно описать виды ПолИБ?

Ответ:

ПолИБ в широком смысле определяется как система документированных управленческих решений по ОИБ организации.

ПолИБ в узком смысле – отдельный нормативный документ, определяющий требования безопасности, систему мер и/или порядок действий, а также ответ-

ственность сотрудников организации и средства управления для определенной области ОИБ.

1)корпоративную ПолИБ – ПолИБ организации в целом; такие политики называют также ПолИБ верхнего, или программного, уровня;

2)частные ПолИБ или ПолИБ по конкретным вопросам или ПолИБ по конкретным системам, ориентированная на отдельную область ОИБ или технологию, используемую в организации/ее подразделении.

3) ПолИБ подразделений организации; могут даже создаваться ПолИБ для отдельных пользователей (роли/должности) или для группы пользователей внутри организации или за ее пределами (для партнеров, клиентов, аудиторов и т.п.).

15. Что понимают под ПолИБ в широком и узком смыслах?

Ответ:

ПолИБ в широком смысле определяется как система документированных управленческих решений по ОИБ организации.

ПолИБ в узком смысле – отдельный нормативный документ, определяющий требования безопасности, систему мер и/или порядок действий, а также ответственность сотрудников организации и средства управления для определенной области ОИБ.

16. Для чего разрабатываются организационные (административные) и технические ПолИБ?

Ответ:

Административная или организационная ПолИБ (англ. Organisational security policy) и есть ПолИБ в выше определенном понимании. Она обычно излагается в документах трех уровней. Документы верхнего уровня носят общий характер и определяют ПолИБ для организации в целом. Второй уровень выделяют в случае структурной сложности организации или при необходимости обозначить специфичные области деятельности, подразделения, технологии, подсистемы и т.п. Третий уровень относится к конкретным службам или подразделениям организации и детализирует верхние уровни ПолИБ. На данном уровне определяются конкретные цели, частные критерии и показатели ИБ, задаются права групп пользователей, формулируются условия доступа к информации, выводятся правила ОИБ и т.п.

Техническая ПолИБ (англ. Technical security policy) – совокупность законов, правил и практических методов, регулирующих обработку чувствительной информации и использование ресурсов ПО и АО ИС.

Техническая ПолИБ базируется на правилах двух видов:

а) первая группа связана с заданием правил разграничения доступа ко всем информационным ресурсам организации;

б) вторая – основана на правилах анализа сетевого трафика как внутри интранета, так и при его выходе или входе из интранета.

17. Перечислите основные требования, предъявляемые в различных источниках к ПолИБ?

Ответ:

ПолИБ должна быть:

·обязательно согласована с общепризнанными основами теории ИБ, со всеми существующими нормативными и правовыми документами, соблюдение которых требуется от организации в стране ее функционирования, а также директивами, законами, приказами и общими задачами самой организации;

·интегрирована в общую политику организации и согласована с другими политиками (например, политикой приема/найма на работу);

·краткой (лучшие практики указывают на объем не более 10 страниц), простой для понимания и не допускать двойного толкования ее положений;

·наглядной. Это способствует ее эффективной реализации, помогая гарантировать ее знание и понимание всеми сотрудниками организации. Видеофильмы, семинары, статьи во внутренних изданиях организации или на ее внутреннем вебузле увеличивают такую наглядность;

·надлежащим образом доведена в доступной и понятной форме до сведения всех сотрудников организации, с которой они должны ознакомиться чаще всего под расписку. Программа обучения в области ИБ и контрольные проверки действий в тех или иных ситуациях могут достаточно эффективно демонстрировать всем пользователям действенность соблюдения ПолИБ;

·реализуема (т.е. содержать только те положения, которые могут быть реализованы на практике), а ее реализация контролируема;

·утверждена высшим руководством организации и издана.

Также ПолИБ должна:

·обеспечивать разумный баланс между защитой и при этом не влиять на эффективность работы сотрудников организации, т.е. не снижать результативность их работы;

·устанавливать ответственность руководства и излагать подход организации к управлению ИБ;

·регулярно (через запланированные промежутки времени, по графику) анализироваться. Анализ должен включать в себя оценивание возможностей для

улучшения ПолИБ и подходов к управлению ИБ в ответ на изменения в окружении организации, бизнес-обстоятельствах, юридических условиях или в технической среде. Анализ ПолИБ должен учитывать результаты ее анализа со стороны руководства;

· регулярно пересматриваться и модифицироваться (особенно в случае возникновения значительных изменений в текущем развитии организации) согласно разработанной заранее процедуре. Периодические пересмотры должны включать проверку соответствия ПолИБ актуальной законодательной базе, оценку ее эффективности, исходя из характера, числа и последствий зарегистрированных инцидентов ИБ, определение стоимости мероприятий по управлению ИБ и их влияние на бизнес, анализ влияния изменений в технологиях на деятельность организации. Такая процедура должна обеспечивать осуществление пересмотра ПолИБ в соответствии с изменениями, затрагивающими первоначальную оценку рисков ИБ, например, путем выявления существенных инцидентов ИБ, появление новых уязвимостей или изменения организационной или технологической инфраструктуры организации. Пересмотр и модификация ПолИБ обеспечивает ей адекватность и результативность. Пересмотренная ПолИБ должна быть утверждена руководством.

Должно быть назначено ответственное за ПолИБ должностное лицо, которое отвечает за ее реализацию и пересмотр в соответствии с установленной процедурой.

18. Каковы основные принципы, позволяющие разработать эффективную ПолИБ?

Ответ:

Законность, Определенность целей, сформулированных в ПолИБ, Системность

Комплексный (мультидисциплинарный) подход к разработке ПолИБ, Научная обоснованность и техническая реализуемость защитных мер,

Эшелонированность (многоуровневость) обороны защитных средств.

Способность к интеграции и согласованность (скоординированное функционирование) применения различных защитных мер.

Эффективность и непрерывность защиты, Разумная достаточность,

Своевременность, адекватность и пропорциональность защитных мер, определенных в ПолИБ, реальным угрозам и рискам ИБ

Рискориентированный подход при разработке ПолИБ, Гибкость управления и применения защитных мер, Невозможность миновать защитные средства, Усиление самого слабого звена, Простота и управляемость защитных средств

Невозможность перехода защитных средств в небезопасное состояние Наблюдаемость и контролируемость защитных мер,

Обязательность контроля (мониторинга и аудита) защитных мер и соблюдения ПолИБ

Совершенствование ОИБ за счет периодической переоценки защитных мер и потребности в них

Разделение полномочий (обязанностей), распределение ролей и ответственности

Минимизация полномочий и привилегий

Обеспечение всеобщей поддержки защитных мер, предусматривающей комплекс мер, направленный на обеспечение лояльности персонала и его постоянное теоретическое и практическое обучение

Информированность

Соблюдение этики и учет различных прав и законных интересов сотрудников организации, включая право на частную жизнь.

19. Каково содержание документа, описывающего корпоративную ПолИБ? Что излагается в каждом из разделов этой политики?

Ответ:

·Цель (назначение) ПолИБ.

Цель (назначение). Корпоративная ПолИБ обычно содержит утверждение, поясняющее, зачем она была разработана. Всегда полезно явно указать цель или причины ее написания.

·Область действия ПолИБ.

Область действия. Перед изложением самой ПолИБ определяется область ее действия с помощью ограничений и условий в понятных всем терминах, которые часть вводятся в явном виде.

·Основные положения ПолИБ.

Основные положения ПолИБ. В явной форме описывается позиция организации (то есть решение ее руководства) по данному вопросу. Позиция может быть сформулирована как в наиболее общем виде, как набор целей, которые преследует организация в данном аспекте, так и конкретизирована.

·Организационные меры.

Организационные меры. С целью формализации процесса управления ИБ в соответствии с ПолИБ требуется создание организационной структуры, которую также требуется описать.

·Ответственность (роли и обязанности).

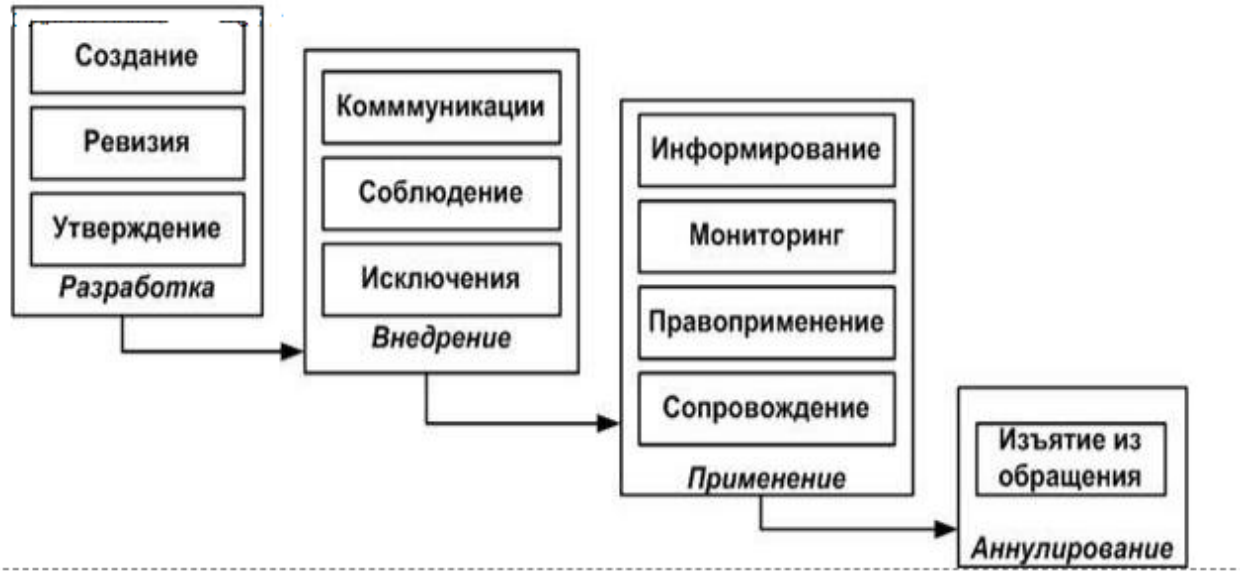
Ответственность (роли и обязанности). В этом разделе ПолИБ точно устанавливается, кто и за что отвечает. Фраза «За ОИБ несут ответственность все сотрудники организации» на практике мало что означает.

·Соблюдение ПолИБ.

Соблюдение ПолИБ. Это выражается в соблюдении двух видов соответствий.

20. Назовите основные стадии жизненного цикла ПолИБ? Из каких шагов они состоят?

Ответ:




21.Дайте определения «ОИБ», «управления ИБ» и «СУИБ» организации.

Ответ:

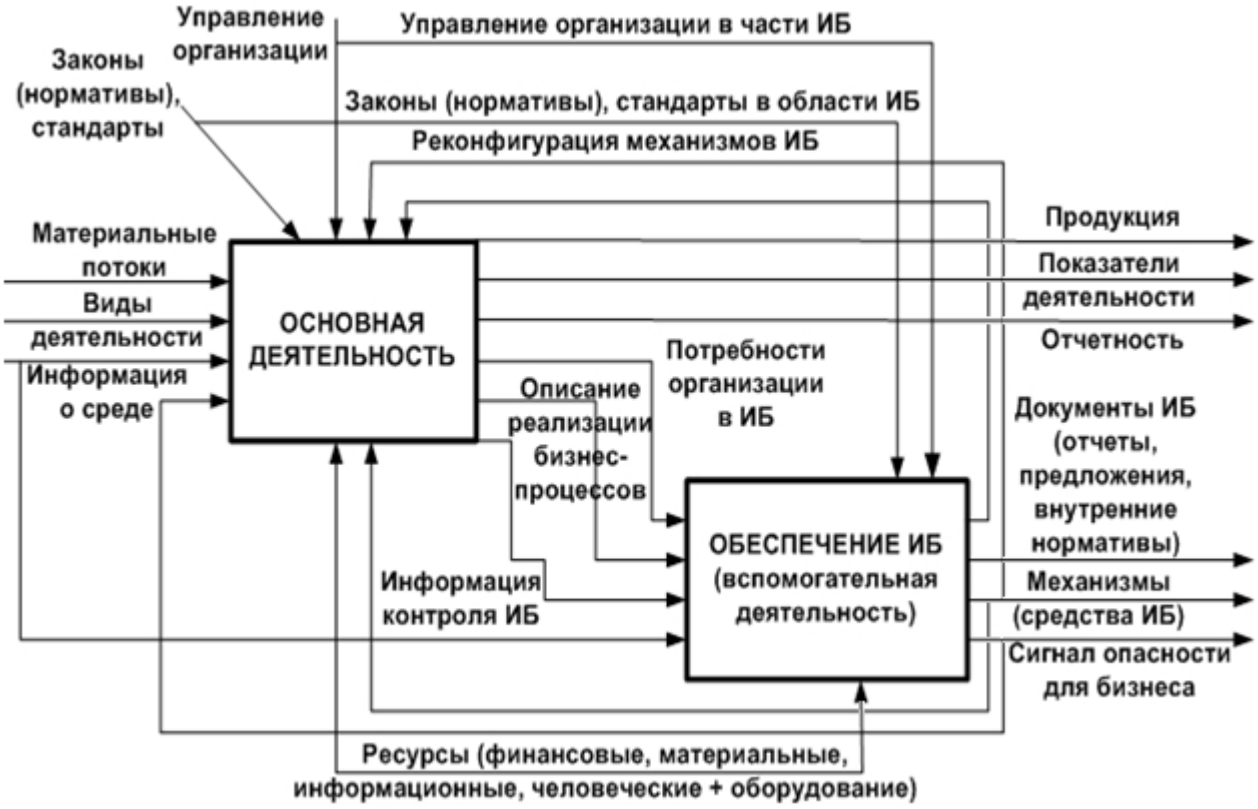
ОИБ - обеспечение информационной безопасности

СУИБ - система управления информационной безопасностью

Управление информационной безопасностью (управление ИБ): циклический процесс, состоящий из совокупности целенаправленных действий, осуществляемых для достижения заявленных бизнес-целей организации посредством обеспечения защищенности ее информационной сферы, и включающий осознание необходимости обеспечения ИБ (ОИБ), постановку задачи по ОИБ, оценку текущей ситуации и состояния объекта управления, планирование мер по обработке рисков

ИБ, реализацию, внедрение и оценку эффективности соответствующих защитных мероприятий и средств управления, распределение ролей и ответственности в области ОИБ, обучение и мотивацию сотрудников, выбор управляющих и корректирующих воздействий и их реализацию.

22. Опишите деятельность по ОИБ организации как процесс. Каковы его входные и выходные данные?




Входные данные для процесса ОИБ:

- информация о среде ведения бизнеса организации;
- информационные модели основной деятельности организации – описания бизнес-процессов, реализуемых технологий и т.д.;
- потребности организации в ИБ;
- информация, используемая для контроля успешности деятельности по ОИБ.

Выход (результат) деятельности по ОИБ в организации:

- документы по ОИБ (отчеты, предложения, в том числе по обучению персонала, внутренние нормативные документы и т.д.);
- механизмы (средства, защитные меры) ОИБ;
- заказы на приобретение, поставку и регламентацию использования средств ОИБ на объекты и системы в организации, которые далее могут эксплуа-

тироваться другими вспомогательными или основными подразделениями, и порядок их использования;

· сигнал опасности для основной деятельности (бизнеса) организации.

23. Как процесс ОИБ в организации связан с процессами основной деятельности организации?

Ответ:

Для ОИБ необходимы исходные данные, ресурсы и управляющие воздействия. Результаты ОИБ непосредственно влияют на эффективность основных бизнес-процессов организации.

С учетом описания структуры типового процесса можно сделать вывод о том, что ОИБ необходимо

рассматривать как процесс.

Входные данные для процесса ОИБ:

•информация о среде ведения бизнеса организации;

•информационные модели основной деятельности организации – описания бизнес-процессов, реализуемых технологий и т.д.;

•потребности организации в ИБ;

•информация, используемая для контроля успешности деятельности по ОИБ.

Информационные модели основной деятельности организации определяют акцент и контекст всей деятельности по ОИБ, т.к. позволяют понять, где в структуре ведения бизнеса организации в части ИТ имеются уязвимости, где и при каких условиях могут проявиться те или иные угрозы ИБ и действия нарушителей ИБ, где находятся требующие защиты активы, какие защитные меры – организационные, административные, программно-аппаратные, технические – могут потребоваться и какие из них могут быть наиболее эффективными в каждом конкретном случае.

24. Определение процесса УИБ.

Ответ:

Управление ИБ организации как циклический процесс, состоящий из совокупности целенаправленных действий, осуществляемых для достижения заявленных бизнес-целей организации посредством обеспечения защищенности ее информационной сферы, и включающий осознание необходимости ОИБ, постановку задачи по ОИБ, оценку текущей ситуации и состояния объекта управления, планирование мер по обработке рисков ИБ, реализацию, внедрение и оценку эффективности соответствующих защитных мероприятий и средств управления, рас-

пределение ролей и ответственности в области ОИБ, обучение и мотивацию сотрудников, выбор управляющих и корректирующих воздействий и их реализацию.

25. Что является хорошей практикой при выборе области действия СУИБ? Какие стратегии выбора области действия СУИБ существуют?

Ответ:

Области действия СУИБ. Это область и границы применения СУИБ в терминах характеристик бизнеса, организации, ее расположения, ресурсов и технологий

Хорошей практикой при определении области действия будущей СУИБ является выбор одного из ключевых бизнес-процессов организации.

26. Какие факторы необходимо учитывать при выборе области действия СУИБ?

Ответ:

При выборе области действия СУИБ, в которой силами специально созданной рабочей группы будут внедряться процессы СУИБ, учитываются следующие факторы:

- деятельность и услуги (продукция), предоставляемые организацией своим партнерам и клиентам;
- целевая информация, ИБ которой должна быть обеспечена;
- бизнес-процессы, обеспечивающие обработку целевой информации;
- подразделения и сотрудники организации, задействованные в данных бизнес-процессах;
- программно-аппаратные и технические средства, обеспечивающие функционирование данных бизнес-процессов;
- территориальные площадки организации, в рамках которых происходят сбор, обработка и передача целевой информации.

27. Что входит в документальное обеспечение СУИБ? Каковы этапы его жизненного цикла?

Управление документами и записями составляет важную часть процесса управления рисками ИБ, которая должна реализоваться параллельно с другими процессами управления ИБ.

В документацию СУИБ обычно включаются следующее документы:

- политика СУИБ;
- руководства по процессам управления ИБ;
- документированные процедуры;
- рабочие инструкции;

- формы и шаблоны;
- планы работ;
- спецификации;
- внешние документы (международные стандарты, ГОСТы и т.п.);
- отчетные документы и т.п.

Тогда по аналогии с иерархией документов по ОИБ организаций БС РФ иерархия документов СУИБ может быть представлена так, как показано на рисунке.

Документы СУИБ первого уровня включают Политику СУИБ и, возможно, детализирующие ее подполитики (например, обработки рисков ИБ, обработки инцидентов ИБ и т.п.).

Второй уровень представлен двумя типами документов СУИБ.

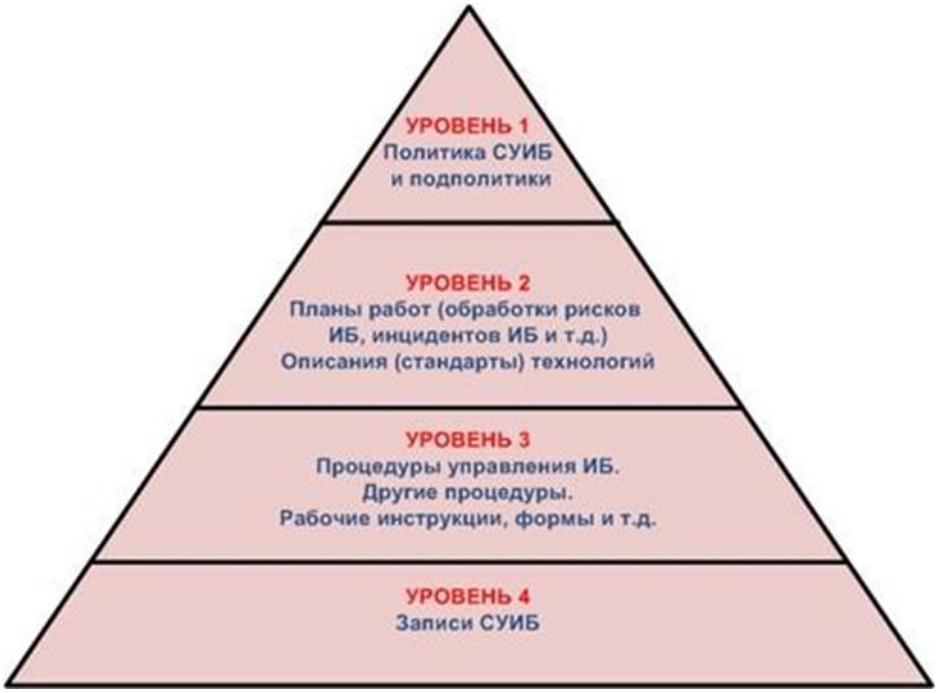
1. Планы работ по управления ИБ. В состав планов входят

- планы мероприятий по обеспечению деятельности в рамках управления ИБ, реализации и внедрению процедур, требований и мер по ОИБ, управлению документами, связанными с СУИБ;
- планы обработки рисков ИБ;
- планы мероприятий на случаи возможных инцидентов ИБ;
- планы работ по обслуживанию аппаратных средств и программных систем, используемых для ОИБ, обучению и повышению осведомленности работников организации и т.д.

В них описывается перечень, порядок (последовательность), объем (в той или иной форме), сроки выполнения работ, а также руководители, исполнители и ответственность за выполнение работ.

Третий уровень документов СУИБ – наиболее объемная часть документации, описывающая конкретные действия каждого участника процесса управления ИБ. Этот уровень составляют документы СУИБ, содержащие требования к процедурам управления ИБ, выполняемым как структурными подразделениями организации, так и ее сотрудниками в рамках технологических процессов, реализующих технологии, которые определены в различных ПолИБ организации и Политике СУИБ.

Четвертый уровень составляют документы СУИБ, содержащие свидетельства – записи о результатах реализации деятельности по управлению ИБ, регламентированной документами верхних уровней иерархии.




28. Какие уровни документов включает в себя иерархия документов СУИБ? Какие виды конкретных документов создаются на каждом из уровней?

Ответ:

В организационной документации (положение о предприятии, устав компании, стандарты, положения, инструкции, правила планирования, учета и т.д.) не указываются конкретные лица и конкретные даты исполнения. В распорядительной документации (приказ, распоряжение, инструктаж) указываются конкретные исполнители и сроки выполнения.

По уровню управления документация компании подразделяется на три уровня. Причем документы более низкого уровня не могут отменять либо противоречить положениям документов более высокого уровня. Эта структура облегчает рассылку, поддержание и понимание документации.

29. В чем состоит основное отличие между понятиями документ и запись?

Ответ:

Хотя документ и запись имеют одинаковое значение в общем использовании, они имеют определенные значения в области информации. Документ - это часть письма, которая содержит информацию, тогда как запись - это документ, который можно использовать в качестве доказательства. И документы, и записи предоставляют информацию, но записи также служат доказательством. Это главное отличие между документом и записью.

30. В чем заключается процесс управления документами и записями?

Ответ:

Стандарт ИСО 15489 устанавливает, что к процессам управления документами относятся:

- включение документов в систему;
- регистрация;
- классификация;
- классификация доступа и защиты;
- установление порядка и сроков хранения;
- хранение;
- использование;
- обеспечение сохранности.

31. На каких этапах руководство организации должно продемонстрировать свою приверженность к разработке, реализации, эксплуатации, мониторингу, анализу, сопровождению и совершенствованию СУИБ?

Ответ:

Руководство должно продемонстрировать свою приверженность созданию, внедрению, эксплуатации, мониторингу, анализу, сопровождению и совершенствованию СУИБ, путем:

a) создания политики СУИБ;

b) обеспечения наличия целей и планов СУИБ;

c) определения ролей и ответственности за информационную безопасность;

d) сообщения организации о важности достижения целей информационной безопасности и соответствия политике информационной безопасности, ее ответственности перед законом и необходимости непрерывного совершенствования;

e) выделения достаточных ресурсов для разработки, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования СУИБ;

f) принятия решения о критериях принятия рисков и допустимом уровне риска;

g) обеспечения проведения внутренних аудитов СУИБ;

h) проведения анализа СУИБ со стороны руководства.

32. В чем состоит основная необходимость участия высшего руководства в жизненном цикле СУИБ?

Ответ:

Организация должна определить и выделить ресурсы, убедиться в том, что весь персонал, на который возложена определяемая в СУИБ ответственность, обладает необходимой компетенцией для решения требуемых задач, убедиться в том,

что весь имеющий отношение к СУИБ персонал осведомлен о важности и необходимости принятия мер по обеспечению информационной безопасности, а также о своем вкладе в достижение целей СУИБ.

33. Каким образом при использовании циклической модели РОСА применительно к СУИБ требования и ожидания к результатам ОИБ преобразуются в управляемую ИБ?

Ответ:

| | |
|---|---|
| Планируй (создание СУИБ) | Определение политики СУИБ, целей, процессов и процедур, существенных для управления рисками и улучшения информационной безопасности с целью предоставления результатов, соответствующих политикам и целям компании |
| Делай (внедрение и функционирование СУИБ) | Внедрение и функционирование СУИБ, обеспечение и управление политикой, средствами контроля, процессами и процедурами |
| Проверяй (мониторинг и пересмотр СУИБ) | Оценка и (при необходимости) анализ функционирования процессов в соответствии с политикой СУИБ, целей и практического опыта, а также предоставление отчетов о результатах проведения проверок руководству компании |
| Действуй (поддержание и улучшение СУИБ) | Выполнение корректирующих и превентивных действий, основанных на результатах внутреннего аудита СУ И Б, проверок руководством компании или на другой информации, с целью достижения постоянного улучшения СУИБ |

34. Дайте определение «процесс управления ИБ» организации.

Ответ:

Это циклический процесс, включающий осознание степени необходимости защиты информации и постановку задач; сбор и анализ данных о состоянии информационной безопасности в организации; оценку информационных рисков; планирование мер по обработке рисков; реализацию и внедрение соответствующих механизмов контроля, распределение ролей и ответственности, обучение и мотивацию персонала, оперативную работу по осуществлению защитных мероприятий; мониторинг функционирования механизмов контроля, оценку их эффективности и соответствующие корректирующие воздействия.

35. Какие действия и процессы выполняются на стадии планирования СУИБ?

Ответ:

Процесс планирования включает следующие этапы:

1) Определение перечня информационных ресурсов компании. Автоматизированное средство помогает хранить данные об информационных ресурсах и всех их изменениях, помимо этого, оно может упростить процесс сбора данных.

2) Оценка критичности видов информации. Здесь автоматизированное средство может только хранить данные, сведения анкет.

3) Оценка защищенности информационной системы (ИС), то есть выявление угроз и уязвимостей информационных ресурсов. Интеграция с базами уязвимостей (например, OSVDB) и встроенные базы угроз (например, DSEC-CT) помогают оптимизировать данный процесс и обеспечить его полноту. Кроме того, возможна интеграция с различными сканерами уязвимостей.

4) Определение информационных рисков, используя имеющиеся данные об информационной системе. Встроенный алгоритм рассчитывает информационные риски на основе внесенных (или собранных автоматически) данных. Результат оформляется в виде отчета.

5) Выбор стратегии обработки рисков, определение мер по снижению рисков. Автоматизированное средство позволяет максимально гибко и удобно моделировать различные варианты внедрения средств защиты, оценить эффективность планируемых средств, выбрать наилучшую стратегию защиты.

36. Специалистов каких подразделений необходимо включать в рабочую группу по построению СУИБ?

Ответ:

Подразделения ИБ, подразделения по работе с персоналом.

37. Какие действия и процессы выполняются на стадии реализации и внедрения СУИБ? Каковы задачи данного этапа?

Ответ?

Внедрение процедур системы управления ИБ, средств повышения защищенности подразумевает их реализацию в информационной системе компании. В данном процессе автоматизированное средство может аккумулировать информацию, осуществлять общение между специалистами по ИБ, исполнять роль планировщика задач.

На данном этапе основная роль автоматизированного средства - сохранять документы системы управления ИБ:

- регламентирующие документы (политики, регламенты, инструкции);
- записи, подтверждающие выполнение существующих процедур в ИС компании.

Это позволяет хранить всю документацию системы управления ИБ в одном централизованном месте и в случае необходимости без промедления предоставлять ее заинтересованным лицам (например, внутренним или внешним аудиторам).

38. Какие действия и процессы выполняются на стадии проверки СУИБ?

Ответ:

Проверка функционирования процедуры системы управления ИБ необходима для того, чтобы гарантировать их правильную и эффективную работу или в случае выявления каких-либо нарушений определить, какие требуются совершенствования. На данном этапе автоматизированное средство может выполнять, например, следующие роли:

- Ведение статистики и анализ инцидентов. Анализ инцидентов является основным критерием эффективности и достаточности обеспечения безопасности ИС, а также эффективности всей системы управления ИБ в целом. На основе информации об инцидентах определяются меры по совершенствованию средств защиты ИС. Автоматизированное средство может предоставлять возможность структурированного хранения данных обо всех инцидентах ИБ, собирать их статистику по различным параметрам, помечать объекты, часто фиксируемые в качестве объектов инцидентов.
- Сбор метрик оценки эффективности И Б. Результаты и частота инцидентов информационной безопасности - наиболее очевидная метрика оценки ее эффективности. Кроме того, автоматизированное средство может анализировать, например, следующие данные: уязвимости ИС (найденные, закрытые), эффективность внедряемых контрмер, количество проведенных курсов по ИБ и т.п.

39. Какие действия и процессы выполняются на стадии совершенствования СУИБ? Каковы задачи данного этапа?

Ответ:

На основе собранных и проанализированных метрик оценки эффективности определяются корректирующие действия и план их внедрения. Как правило, корректирующие действия являются либо изменениями в процедурах, документах, либо новыми средствами защиты, то есть изменениями в самой ИС компании. Автоматизированное средство помогает отражать результаты, хранить данные и вести контроль изменений защищенности ИС.

По завершении последнего этапа PDCA-модели весь процесс заново переходит на этап планирования и циклически повторяется в течение всего жизненного цикла системы управления ИБ.

40. В чем разница и сходство между понятиями корректирующего и предупреждающего действия?

Ответ:

Корректирующие действия (КД) и предупреждающие действия (ПД) - основные элементы функционирования и улучшения систем менеджмента качества. Их необходимо планировать на основе проведенных технических аудитов, инспекционного обследования, экспертных оценок текущего и прогнозируемого состояния объекта и направлять на устранение причин возникновения несоответствий и потенциальных опасностей.

Стандарт ИСО 9001:2008 устанавливает два вида действий в случае выявления несоответствий – коррекция и корректирующие действия. Коррекция – это действия, предпринимаемые для устранения возникшего несоответствия. Корректирующие действия – это действия, предпринимаемые для устранения причин несоответствия. Источники для КД: - жалобы, - отчеты о несоответствиях, - предписания, акты. Предупреждающие действия – действия, предпринимаемые для предотвращения возникновения несоответствия. Источники для ПД: - анализ потребностей ожидания потребителей, - анализ рынка, - измерение заинтересованности заинтересованных сторон.

Методы проведения КД и ПД выбираются применительно к осуществляемым предприятием процессам и продукции этих процессов.

Разработка процедуры КД и ПД – необходимая деятельность организаций, где происходят отказы оборудования и инциденты, присутствуют различные несоответствия, потенциальные опасности (возможность возникновения отказа и его развития в крупные аварии с негативными последствиями для здоровья людей, окружающей среды, имущества, бизнеса и т.д.).

Эти несоответствия – следствие несовершенства техники и организации производства, человеческих ошибок, природно-климатических воздействий и других факторов. Организация работ по устранению и предупреждению несоответствий, ввиду высоких трудовых и финансовых затрат, требует эффективного расходования ресурсов, необходимых для реализации КД и ПД, которые должны быть адекватны несоответствиям и соразмерны значимости своего воздействия, т.е. измеряемы и количественно связаны с уровнем безопасности.

41. Что такое «угроза ИБ», «уязвимость», «источник угрозы ИБ»? Как взаимосвязаны эти понятия?

Ответ:

Угроза информационной безопасности — совокупность условий и факторов, создающих опасность нарушения информационной безопасности.

Уязвимость – любой фактор, делающий возможным реализацию угрозы.

источник угрозы ИБ - это субъект (физическое лицо, материальный объект или физическое явление), активизирующий угрозу ИБ и переводящий ее из разряда потенциальной опасности нарушения свойств ИБ (конфиденциальности, доступности, целостности и т. д.) активов организации в реально происходящее нарушение этих свойств. Уязвимость создает потенциальные условия для реализации угрозы ИБ.  Угроза ИБ, для реализации которой в системе нет уязвимости, не актуальна для этой системы и не влечет за собой риска ИБ.

42. Каким образом возможно формировать каталоги угроз ИБ и уязвимостей, которые будут использоваться для оценки рисков ИБ?

Ответ:

Важно применять в новых условиях и собственный опыт произошедших ранее инцидентов ИБ и прошлых оценок угроз ИБ, но помня, что в среде ведения бизнеса и в ИС и в ИТ происходят постоянные изменения. Также стоит обратиться к другим каталогам и статистикам угроз ИБ (возможно, специфичным для организации или ее бизнеса), что поможет создать наиболее полный список угроз ИБ, применимых к организации.

43. В чем может состоять преимущество использования каталогов угроз ИБ, характерных для организации, в которой проводится оценка рисков ИБ, по сравнению с использованием типовых каталогов угроз ИБ?

Ответ:

Это поможет создать наиболее полный список угроз ИБ, применимых к организации.

44. Какие подходы к анализу рисков ИБ выделяются в стандартах?

Ответ:

В стандартах ISO/IEC TR 13335-3:1998 и ГОСТ Р ИСО/МЭК 13335- 3-2007 рассматриваются четыре вида анализа рисков ИБ [7, 10]:

1) базовый (англ, baseline risk analysis) с низкой степенью риска и выбором стандартных защитных мер;

2) неформальный (англ, informal risk analysis) для активов организации, которые, как представляется, подвергаются наибольшему риску;

3) детальный (англ, detailed risk analysis) с использованием формального подхода ко всем активам организации;

4) комбинированный (англ, combined risk analysis) — сначала высокоуровневый анализ для выбора подхода к анализу рисков ИБ с последующим проведением детального анализа для наиболее критичных выделенных систем (если прекращение их функционирования может при-чинить ущерб или принести убытки органи-

зации, отрицательно повлиять на ее бизнес или активы) и базового для всех остальных.

45. В чем состоят сходства и различия подходов базового и детального анализа рисков ИБ?

Ответ:

Детальный анализ рисков ИБ может быть очень ресурсоемким процессом, и поэтому требуется тщательное определение границ бизнес- среды, операций, активов в области действия СУИБ. Кроме того, подобный подход требует постоянного внимания со стороны руководства.

Такой анализ рисков ИБ отличается от базового тем, что выполняется более детальный анализ активов и требований по ОИБ

Цель ОИБ на основе базового подхода состоит в том, чтобы подобрать для организации минимальный набор защитных мер для всех или отдельных активов. Используя базовый подход, можно применять соответствующий ему базовый уровень ИБ в организации и, кроме того, дополнительно использовать результаты детального анализа риска ИБ для ОИБ активов с высоким уровнем риска или систем, играющих важную роль в бизнесе организации. Применение базового подхода позволяет снизить инвестиции организации на исследование результатов анализа рисков ИБ.

Требуемая защита при таком подходе обеспечивается за счет использования справочных материалов (каталогов) и лучших практик по защитным мерам, в которых можно подобрать набор средств для защиты активов от наиболее часто встречающихся угроз. Базовый уровень ИБ устанавливается в соответствии с потребностями организации, при этом в проведении детальной оценки угроз ИБ, уязвимостей и рисков ИБ для систем нет необходимости. При наличии в системе установленных защитных мер их сравнивают с рекомендуемыми в каталогах. Защитные меры, которые отсутствуют в системе, но могут быть в ней использованы, должны быть реализованы.

46. Какой из подходов к анализу рисков ИБ предпочтительнее применять в небольшой организации, в которой эксплуатируются критичные системы, поддерживающие предоставление организацией услуг внешним заказчикам?

Ответ?

Базовый.

При данном подходе организация может применить базовый уровень ИБ для всех защищаемых активов за счет выбора стандартных защитных мер

47. В какой ситуации и для какой организации целесообразно применять комбинированный подход к анализу рисков ИБ?

Ответ:

Подходит практически для всех организаций и любых ситуаций при наличии у организации достаточного количества ресурсов.

48. Какие подходы к оценке рисков ИБ выделяются в стандартах?

Ответ:

В стандартах ISO/IEC 27005:2018 и ГОСТ Р ИСО/МЭК 27005-2010 выделяются два основных типа оценки рисков ИБ и упоминается их комбинация:

- высокоуровневая (англ, high-level IS risk assessment);
- детальная (англ, detailed IS risk assessment).

49. Как осуществляются качественная, количественная и полуколичественная оценка рисков ИБ?

Ответ:

Для проведения качественной оценки рисков ИБ выполняются шесть процедур:

1) Определение и документальная фиксация перечня типов активов, для которых выполняются процедуры оценки рисков ИБ (далее - область оценки рисков ИБ). Область оценки рисков ИБ может быть определена как перечень типов активов организации в целом, ее отдельного подразделения или отдельного процесса деятельности организации в целом или ее подразделения. Для каждого из типов активов определяется перечень основных и дополнительных свойств ИБ, поддержание которых необходимо обеспечивать в рамках СОИБ организации.

2) Определение и документальная фиксация перечня типов объектов среды, соответствующих каждому из типов активов области оценки рисков ИБ. При составлении данного перечня рассматриваемые типы объектов среды разделяются по уровням информационной инфраструктуры организации.

3) Определение на основе модели угроз ИБ организации и документальная фиксация источников угроз ИБ, воздействие которых может привести к потере свойств ИБ соответствующих типов активов для каждого из определенных в рамках выполнения процедуры 2 типов объектов среды. Типы объектов среды и выявляемые для них источники угроз должны соответствовать друг другу в рамках иерархии информационной инфраструктуры организации. При этом возможно расширение первоначального перечня источников угроз ИБ, зафиксированных в модели угроз организации (или же его дополнительная структуризация путем составления новых моделей угроз для некоторых из выделенных типов объектов

среды или отдельных объектов среды). При формировании перечня источников угроз рекомендуется рассматривать возможные способы их воздействия на объекты среды, в результате чего возможна потеря свойств ИБ соответствующих типов активов (способы реализации угроз ИБ). Степень детализации и порядок группировки для рассмотрения способов реализации угроз ИБ определяются организацией.

4) Определение СВР угроз ИБ применительно к выделенным типам объектов среды и анализ возможности потери каждого из свойств ИБ для каждого из типов активов в результате воздействия на соответствующие им типы объектов среды выделенных источников угроз ИБ. Для оценки СВР угроз ИБ в РС БР ИББС-2.2-2009 используется следующая качественная шкала степеней «нереализуемая - минимальная - средняя - высокая - критическая». Основными факторами для оценки СВР угроз ИБ является информация соответствующих моделей угроз ИБ, в частности: данные о расположении источника угрозы ИБ относительно соответствующих типов объектов среды; информация о мотивации источника угрозы ИБ антропогенного характера (связанного с человеком); предположения о квалификации и (или) ресурсах источника угрозы ИБ; статистические данные о частоте реализации угрозы ИБ ее источником в прошлом; информация о способах реализации угроз ИБ; информация о сложности обнаружения реализации угрозы ИБ рассматриваемым источником; данные о наличии у рассматриваемых типов объектов среды организационных, технических и прочих защитных мер, эксплуатация которых сокращает качественно или количественно существующие уязвимости объектов защиты активов, тем самым снижая вероятность реализации соответствующих угроз ИБ [например, средства защиты от несанкционированного доступа (НСД)].

5) Определение СТП нарушения ИБ для типов активов области оценки рисков ИБ и анализ последствий потери каждого из свойств ИБ для каждого из типов активов в результате воздействия на соответствующие им типы объектов среды выделенных источников угроз ИБ. Для оценки СТП нарушения ИБ вследствие реализации угроз ИБ в РС БР ИББС-2.2- 2009 используется следующая качественная шкала степеней «минимальная - средняя - высокая - критическая». Основными факторами для оценки СТП нарушения ИБ являются: степень влияния на непрерывность бизнеса и репутацию организации; объемы финансовых и материальных потерь, финансовых, материальных и временных затрат, а также людских ресурсов, необходимых для восстановления свойств ИБ для активов рассматриваемого типа и ликвидации последствий нарушения ИБ; степень нарушения законодатель-

ных требований и (или) договорных обязательств организации, требований регулирующих и контролирующих (надзорных) органов в области ИБ, а также требований внутренних нормативных актов организации; объем хранимой, передаваемой, обрабатываемой, уничтожаемой информации, соответствующей рассматриваемому типу объекта среды; данные о наличии у рассматриваемых типов объектов среды организационных, технических и прочих защитных мер, эксплуатация которых сокращает СТП нарушения свойств ИБ активов (например, средства резервного копирования и восстановления информации).

6) Оценка рисков ИБ, результаты которой документально фиксируются. Качественная оценка рисков ИБ проводится для всех свойств ИБ выделенных типов активов и всех соответствующих им комбинаций типов объектов среды и воздействующих на них источников угроз ИБ на основании сопоставления оценок СВР угроз ИБ и оценок СТП нарушения ИБ вследствие реализации соответствующих угроз ИБ. Для оценки рисков ИБ в РС БР ИББС-2.2-2009 используется следующая качественная шкала «допустимый - недопустимый».

Для формирования резервов на возможные потери, связанные с ин¬цидентами ИБ, риски ИБ могут быть оценены в количественной (де¬нежной) форме. Это определяется на основании количественных оце¬нок СВРкол угроз ИБ, выраженной в процентах, и СТПкол нарушения ИБ, выраженной в денежной форме.

Оценки СВРкол угроз ИБ формируются экспертно путем перевода качественных оценок СВР угроз ИБ, полученных в рамках выполнения процедуры 4, в количественную форму в соответствии со следующей рекомендуемой шкалой:

- нереализуемая - 0 %;
- минимальная - от 1 до 20 %;
- средняя - от 21 до 50 %;
- высокая - от 51 до 100%;
- критическая - 100 %.

50. В чем суть процесса оценивания рисков ИБ?

Ответ:

Риски ИБ заключаются в возможности утраты свойств ИБ активов в результате реализации угроз ИБ, вследствие чего организации может быть нанесен ущерб. Оценка рисков ИБ проводится для типов активов, входящих в предварительно определенную область оценки.

51. Какова роль процесса управления инцидентами ИБ в рамках СУИБ?

Ответ:

Процесс управления инцидентами ИБ связан со многими другими процессами, например, управлением рисками ИБ, мониторингом/ауди- том, управлением изменениями, доступом и НБ. Следовательно, он является своеобразным «мотором» жизненного цикла СУИБ.

52. Какова взаимосвязь между процессами управления рисками ИБ и управления инцидентами ИБ?

Ответ:

Результат процесса управления инцидентами ИБ и полученная в ходе этого информация является единственным объективным источником определения вероятности реализации угроз ИБ при анализе рисков ИБ.

53. Каковы основные этапы работы процесса управления инцидентами ИБ?

Ответ:

Обнаружение, идентификация и регистрация произошедших инцидентов ИБ

Оценка, классификация и приоритезация инцидентов ИБ

Сохранение информации об инциденте ИБ и сбор доказательств его осуществления

Всестороннее исследование инцидента ИБ

Разрешение и закрытие инцидентов ИБ

Извлечение уроков из инцидентов ИБ

Подготовка к усовершенствованию процесса управления инцидентами ИБ

54. Какие подпроцессы включают в себя деятельность по управлению инцидентами ИБ?

Ответ:

- обнаружение уязвимостей, событий ИБ и инцидентов ИБ;
- оповещение об уязвимостях, событиях ИБ и инцидентах ИБ;
- обработка сообщений об уязвимостях, событиях ИБ и инцидентах ИБ;
- реагирование на инциденты ИБ;
- анализ инцидентов ИБ;
- расследование инцидентов ИБ;
- анализ эффективности процесса управления инцидентами ИБ.

55. Каковы основные цели и задачи управления инцидентами ИБ?

Ответ:

Как для всякой деятельности, в первую очередь определяются цели организации по эффективному управлению инцидентами ИБ. Итоговый список, конечно, будет разным для разных организаций. Ниже приведен один из возможных вариантов такого списка:

- гарантировать целостность критически важных систем;
- сохранить и восстановить данные;
- сохранить и восстановить сервисы;
- выяснить, почему инцидент ИБ стал возможен;
- предотвратить развитие атак и будущие инциденты ИБ;
- избежать нежелательной огласки информации об инциденте ИБ;
- найти виновников инцидента ИБ;
- наказать нарушителей ПолИБ организации.

Для достижения этих целей организация решает основные задачи управления инцидентами ИБ:

- координация сбора сведений об инцидентах ИБ, реагирования на них и дальнейшего анализа причин их возникновения;
- минимизация нарушения порядка работы и повреждения актива организации, восстановление в кратчайшие сроки работоспособности организации в результате инцидента ИБ;
- минимизация последствий нарушения ИБ (конфиденциальности, целостности и доступности) активов организации;
- обеспечение сохранности и целостности доказательств того, что инцидент ИБ имел место, накопление и хранение точной информации об имевших место инцидентах ИБ;
- защита прав организации, установленных законом;
- защита репутации организации и ее активов;
- быстрое обнаружение и/или предупреждение подобных инцидентов ИБ в будущем;
- обучение персонала организации действиям по обнаружению, устранению последствий и предотвращению инцидентов ИБ.

56. От чего зависит эффективность процесса управления инцидентами ИБ? В чем она выражается?

Ответ:

Как показывают лучшие практики в области управления ИБ, эффективность процесса управления инцидентами ИБ зависит от следующих факторов:

- координации и согласованности действий всех вовлеченных в него лиц;
- имеющихся возможностей по получению и анализу информации, связанной с инцидентом ИБ;
- оперативности и корректности полученных результатов.

Эффективность управления инцидентами ИБ обычно выражается в измеряющихся и оценивающихся показателях, например:

- тенденции в изменении общего количества инцидентов ИБ;
- среднее фактическое время, затраченное на разрешение инцидента ИБ;
- процент инцидентов ИБ, обработанных в рамках согласованного времени реакции;
- средние затраты на полную обработку инцидента ИБ;
- процент инцидентов ИБ, закрытых без обращения к специализированным группам поддержки;
- количество и процент инцидентов ИБ, разрешенных удаленно.

57. Опишите основные этапы работы процесса управления инцидентами ИБ.

Ответ:

Обнаружение, идентификация и регистрация произошедших инцидентов ИБ - осуществляется на основании показаний систем мониторинга доступности ИТ-сервисов и обращений пользователей, а полученная информация фиксируется в системе регистрации и обработки инцидентов ИБ.

Оценка, классификация и приоритезация инцидентов ИБ - производится идентификация причин возникновения инцидента ИБ и соответствующих действий для его разрешения, а также определяется критичность инцидента ИБ для бизнеса организации.

Сохранение информации об инциденте ИБ и сбор доказательств его осуществления, включая область действия, развитие событий и используемый подход.

Всестороннее исследование инцидента ИБ при поддержке ИТ- подразделения, партнеров и персонала организации, а также соответствующих специалистов, занимающихся сбором свидетельств и доказательств инцидента ИБ.

Разрешение и закрытие инцидентов ИБ - осуществляется своевременная обработка и разрешение инцидента ИБ, и восстановление ИТ- сервисов за счет реконфигурации, переустановки или установки обновлений для систем, сервисов и сетей.

Извлечение уроков из инцидентов ИБ - с подробным описанием произошедшего инцидента ИБ, документированием выявленных событий ИБ, предоставлением отчетов руководству, анализом полученных

уроков, контролем качества разрешения инцидентов ИБ с целью выявления несоответствий и разработки плана усовершенствования и рекомендаций по управлению инцидентами ИБ.

Подготовка к усовершенствованию процесса управления инцидентами ИБ, включающая предотвращение, повышение осведомлённости, обучение, создание группы реагирования на инциденты ИБ (ГРИИБ), разработку политик и процедур и выбор средств.

58. Какой из подпроцессов управления инцидентами ИБ является наиболее объемным и трудоемким?

Ответ:

Реагирование на инцидент ИБ Организации важно заранее определить приоритеты действий, совершаемых во время инцидента ИБ. Бывают столь сложные случаи, когда невозможно одновременно принять все необходимые ответные меры и без учета приоритетов для конкретной организации не обойтись.

59. Что понимают под системой управления инцидентами ИБ?

Ответ:

Система управления инцидентами ИБ (СУИИБ) - часть общей системы управления организации, предназначенная для обнаружения и регистрации, оценки, классификации и приоритезации, всестороннего исследования, обработки, извлечения уроков и предотвращения инцидентов ИБ в дальнейшем и включающая организационную структуру, политику, планирование действий, обязанности, установившийся порядок, процедуры, процессы и ресурсы в области реагирования на инциденты ИБ.

60. Что необходимо принимать во внимание для создания оптимальной СУИИБ?

Ответ:

При внедрении СУИИБ организациям следует избегать возникновения таких потенциальных проблем, как, например, отсутствие «полезных» результатов ее функционирования, которыми можно было бы воспользоваться. Все заинтересованные стороны должны знать, что для предотвращения появления таких проблем были предприняты определенные шаги.

Контрольные вопросы:

1. Какой стандарт (серия стандартов) стал основоположником стандартизации систем управления ИБ?

2. Для организации какой сферы применимы стандарты серии ISO/IEC 27000?

3. Каковы отличительные черты серии стандартов ISO/IEC 27000?

4. Какой из стандартов серии ISO/IEC 27000 содержит требования к созданию, внедрению, эксплуатации, мониторингу, анализу, сопровождению и совершенствованию СУИБ?

5. Какие показатели необходимо рассчитать для построения модели угроз?

6. Что обозначает коэффициент реализуемости угрозы?

7. Какие угрозы являются актуальными?

8. В соответствии с каким нормативным документом строится модель угроз?

9. Какие показатели необходимо рассчитать для построения модели нарушителя?

10. В соответствии с каким нормативным документом, и в каких случаях строится модель нарушителя?

11. Что понимается под информационной безопасностью?

12. Назовите основные способы защиты информации.

13. Назовите способы несанкционированного получения конфиденциальной информации.

14. Какие задачи решаются в ходе разработки и внедрения КСЗИ?

15. Назовите этапы создания системы защиты.

16. Дайте определение политики информационно безопасности.

17. Что включает в себя политика пользования электронной почтой?

18. Назовите общее содержание политика подготовки, обмена и хранения документов.

19. Что включает в себя политика информационно-технической подде1ржки?

20. Что включает в себя политика серверной безопасности?

21. Что называется системой управления информационной безопасностью?

22. Какие стадии включает в себя процесс контроля целостности системы защиты информации?

23. Назовите основные компоненты системы управления информационной безопасностью.

24. Перечислите основные методы защиты систем управления информационной безопасностью.

25. Назовите порядок проведения испытаний системы защиты.

26. Назовите порядок разработки методики испытаний.

27. Какой нормативный документ устанавливает 7 классов защищенности средств защиты информации?

28. Назовите порядок тестирования функций МЭ.

29. Каким рядом заметных достоинств обладает программный комплекс «Сканер-ВС»?

30. Какие этапы включает в себя процесс оценки рисков ИБ?

32. Каковы основные методологические недостатки традиционных подходов к оценке рисков ИБ? Применение каких инновационных подходов позволит устранить эти недостатки?

33. Какие этапы включает в себя процесс анализа рисков ИБ?

34. На каких этапах оценки рисков ИБ может потребоваться участие владельцев бизнес-процессов и почему?

35. Целесообразно ли вести реестр активов организации на регулярной основе и как это может повлиять на процесс оценки рисков ИБ?

36. Какое место процесс оценки рисков ИБ занимает в СУИБ?

37. Каковы наиболее значимые для организации результаты, получаемые в результате работы процесса оценки рисков ИБ?

38. Какова роль процесса управления инцидентами ИБ в рамках СУИБ?

39. Какова взаимосвязь между процессами управления рисками ИБ и управления инцидентами ИБ?

40. Каковы основные этапы работы процесса управления инцидентами ИБ? На каких этапах процесса может потребоваться участие владельцев бизнес- процессов и почему?

41 Какие подпроцессы включает в себя деятельность по управлению инцидентами ИБ?

42. Каковы основные цели и задачи управления инцидентами ИБ?

43. Назовите основные задачи SOC-центров.

44. Какие средства SIEM-систем управления инцидентами информационной безопасности применяются на практике?

Составил
к.т.н., доцент кафедры
«Информационная безопасность» _____ Ю.М. Кузьмин