МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «МЭИ»

«Утверждаю»
Директор ИнЭИ
А. Ю. Невский

ПРОГРАММА ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ ДЛЯ ПОСТУПАЮЩИХ В МАГИСТРАТУРУ
(общая часть)

Разработано:
Профессор. каф. БИТ Минзов А.С.

Москва, 2022 год

1. Основные требования и содержание политики информационной безопасности организации. Какие исходные данные необходимы для её разработки и как оценить ее корректность?

Назначение и роль политики в системе менеджмента информационной безопасности (СМИБ). Основные требования к политике и ее содержание. Исходные данные для разработки политики информационной безопасности. Цели политики информационной безопасности и сфера ее действия. Связь стратегии развития организации и текущего состояния СМИБ с целями политики.

Определение сферы действия политики информационной безопасности и ее отличие от политики СМИБ. Определение требований к результатам оценки и обработки рисков, выбору мер и средств контроля и управления.

Требования по соответствию нормативно-правовым требованиям и договорным обязательствам.

Требования по осведомленности, обучению и тренингам для сотрудников организации.

Требования по обеспечению непрерывности бизнеса.

Документы, дополняющие политику информационной безопасности (частные политики, процедуры безопасности, инструкции, планы, положения).

Ответственность должных лиц и персонала за соблюдение требований политики информационной безопасности.

Пересмотр политики информационной безопасности: условия пересмотра, ответственный исполнитель, организация процесса пересмотра политики. Главное условие определения корректности политики информационной безопасности – это соответствие содержания политики требуемым мерам защиты информации в организации на основе оценки существующего ее состояния, нормативно-правовых требований и стратегического плана развития этой организации и ее информационной инфраструктуры.

Используемые источники:

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

2. Системы управления событиями информационной безопасности (SIEM): назначение, решаемые задачи и общая структура системы.

Проактивная защита в системе информационной безопасности: назначение, составные части и механизмы их действия в системе защиты информации. Классификация задач, решаемых в SIEM. Структура SIEM и их основные характеристики. Примеры отечественных и зарубежных систем. Тенденции развития SIEM.

Используемый источник:

Минзов А.С., Баронов О.Р., Минзов С.А., Осипов П.А.

Управление событиями информационной безопасности: Учебное пособие / Под редакцией профессора, д-ра техн. наук А.С. Минзова. — М.: ВНИИгеосистем, 2020. — 97 с. : ил.

3. Каналы утечки конфиденциальной акустической информации: классификации каналов, краткие характеристики и среда распространения информативного сигнала, технические средства обнаружения и защиты.

Определение понятия «канал утечки информации». Основные термины канала утечки информации. Классификации каналов утечки информации и их краткие характеристики. Единицы измерения параметров акустической информации. Технические средства обнаружения и защиты: классификация, область применения.

Используемый источник:

Бузов Г.А., и др. Защита от утечки информации по техническим каналам. Учебное пособие. М.: Горячая линия-Телеком, 2005.

4. Побочные электромагнитные излучения и наводки (ПЭМИН): краткая характеристика канала утечки конфиденциальной информации, технические средства обнаружения и защиты.

Определение понятия «ПЭМИН». Основные термины и определения для этого канала утечки информации. Классификации каналов утечки информации ПЭМИН и их краткие характеристики. Определение понятия «зона R2». Единицы измерения параметров электромагнитного излучения. Технические средства обнаружения и защиты от ПЭМИН: классификация, область применения.

Используемые источники:

Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. Технические средства и методы защиты информации. М.: Горячая линия-Телеком, 2014.

Бузов Г.А., и др. Защита от утечки информации по техническим каналам. Учебное пособие. М.: Горячая линия-Телеком, 2005.

5. Организация инженерно-технической защиты территорий и помещений с использованием технических средств охраны.

Назначение инженерно-технической защиты, ее место и роль в системе защиты информации. Классификация методов и средств инженерно-технической защиты территорий и помещений. Требования к инженерно-технической защите информации. Классификация технических средств охраны и их назначение.

Используемые источники:

Невский А.Ю., Баронов О.Р. Технические средства охраны. М.: ВНИИгеосистем, 2015;

ГОСТ Р 53195.1-2008 Национальный стандарт Российской Федерации. Безопасность функциональная связанных с безопасностью зданий и сооружений систем. Часть 1. Основные положения;

ГОСТ Р 53709-2009. Национальный стандарт Российской Федерации. Системы безопасности комплексные и интегрированные. Общие технические требования;

ГОСТ Р 51241-2008. Национальный стандарт Российской Федерации. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний;

ГОСТ Р 51558-2008. Национальный стандарт Российской Федерации. Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний.

6. Цель, задачи и общая характеристика мероприятий специального обследования защищаемого помещения.

Определение цели мероприятий специального обследования защищаемого помещения, задачи специального обследования, характеристика мероприятий подготовки к проведению специального обследования, выполнения поисковых мероприятий и подготовка отчетных материалов

Используемый источник:

Бузов Г.А., и др. Защита от утечки информации по техническим каналам. Учебное пособие. М.: Горячая линия-Телеком, 2005.

7. Цель, задачи и общая характеристика мероприятий специальной проверки технического средства приема, обработки, хранения и передачи информации.

Определение цели мероприятий специальной проверки технических средств, задачи специальной проверки технических средств, характеристика мероприятий проведения специальной проверки технических средств, типового набора операций при проведении технических проверок и подготовка отчетных материалов

Используемый источник:

Бузов Г.А., и др. Защита от утечки информации по техническим каналам. Учебное пособие. М.: Горячая линия-Телеком, 2005.

8. Какие цели и задачи решаются при разработке плана обработки рисков информационной безопасности и как они связаны с конечными целями организации и ограничениями? Методы и способы реализации этих задач.

Цели плана обработки рисков – обоснование требуемых мер защиты и управления в соответствии с оценками значений рисков информационный безопасности для различных угроз, активов и их уязвимостей с учетом принятых ограничений на допустимый уровень принятия рисков. Две группы задач решаемых с использованием рисков. Связь второй группы задач с конечными целями организации и оценкам эффективности принятых решений по управлению рисками информационной безопасности. Решения по управлению рисками в условиях ограничений на бюджет по защите информации.

Используемые источники:

Минзов А.С., Невский А.Ю., Баронов О.Р. Управление рисками информационной безопасности: Монография/ Под редакцией А.С. Минзова. — М.: ВНИИгеосистем, 2019. — 110 с. : ил.

ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

9. ценции защиты информации, изложенные в стандартах COBIT 5.0 и ГОСТ Р ИСО/МЭК 27001?

Определить следующие различия в концепциях стандартов ГОСТ Р ИСО/МЭК 27001 и COBIT 5.0.:

- в определении места и роли системы защиты информации в структуре информационной системе организации;
- в учете при построении СМИБ дополнительных факторов влияния на эффективность асе информационной системы организации;
- применения единой методологии управления различными факторами;
- в ориентация системы защиты информации в ИС на конечные цели функционирования организации;
- применение риск-ориентированного подхода к построению системы защиты информации на основе оценки ее эффективности.
- Применение цикла управления СМИБ, ориентированного на более глубокие процессы управления этапами работ.

Используемые источники:

Минзов А.С., Невский А.Ю., Баронов О.Р. Управление рисками информационной безопасности: Монография/ Под редакцией А.С. Минзова. — М.: ВНИИгеосистем, 2019. — 110 с. : ил.

ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности.

10. Определить перечень исходных данных при оценке актуальных угроз информационной безопасности как при проектировании

систем и сетей, так и в ходе их эксплуатации. В какой логической последовательности проводится анализ и оценка угроз?

Определение исходных данных для оценки актуальных угроз безопасности информации:

а) общий перечень угроз безопасности информации, содержащийся в банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), модели угроз безопасности информации, разрабатываемые ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;

б) описания векторов компьютерных атак, содержащихся в базах данных и иных информационных источниках, опубликованных в сети «Интернет» (CAPEC, ATT&CK, OWASP, STIX, WASC и др.);

в) негативные последствия от реализации (возникновения) угроз безопасности информации, определенные в соответствии с настоящей Методикой;

г) объекты воздействия угроз безопасности информации и виды воздействий на них, определенные в соответствии с настоящей Методикой;

д) виды и категории актуальных нарушителей, которые могут реализовывать угрозы безопасности информации, в том числе непреднамеренные угрозы, и их возможности, определенные в соответствии с настоящей Методикой;

е) актуальные способы реализации (возникновения) угроз безопасности информации.

Используемые источники:

Методический документ "Методика оценки угроз безопасности информации" (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.)

Программу составили:

Руководитель
магистерской программы
д.т.н., профессор

А.С. Минзов