Большая библиотека по информационной безопасности и защите ИТ-систем

Автор-разработчик

Ф.И.О.	Исаев Роман Александрович
Должность	Российский эксперт по организационному развитию, управлению бизнес-процессами и операционными рисками, информационным технологиям в бизнесе. Руководитель проектов, бизнес-тренер.
Контакты	www.isaevroman.ru, mail@isaevroman.ru

Общие сведения

Версия	**2.0** Список изменений и дополнений https://orgstudio.ru/files/BBIB2-Whats_new.pdf Свидетельство о государственной регистрации https://orgstudio.ru/certificate/ Отзывы (рецензии) пользователей https://orgstudio.ru/reviews1/
Области применения	Организации любых отраслей и сфер деятельности
Краткое описание	**109 файлов**: образцы документов, модели, практические и учебные материалы, которые требуются в работе сотрудникам и руководителям в области информационной безопасности и информационных технологий.
Обновления	Пользователи Библиотеки получают **бессрочную бесплатную подписку** на все следующие версии. Для получения обновлений необходимо предоставить отзыв (рецензию) на применяемую в работе версию.
Технические требования	Поставка выполняется в виде архива файлов форматов: Word, Excel, PDF, Visio. Для открытия файлов необходимы соответствующие программные продукты (актуальных версий).
Обучение	Проводится вебинар «Операционные риски и операционная надёжность организаций: процессы, технологии, практика»
Другие Библиотеки	Предлагаем также ознакомиться с другими нашими продуктами. - Большая библиотека бизнес-аналитика и специалиста по бизнес-процессам - Большая библиотека системного аналитика и ИТ-архитектора - Большая библиотека риск-менеджера и специалиста по операционным рискам - Сборник типовых моделей процессов для организаций всех отраслей - Сборник стратегий развития организаций (для всех отраслей)
Стоимость	**89 000 руб.** **Скидка 10%** предоставляется (не суммируются): - при одновременной покупке двух Библиотек и Сборников автора - для действующих пользователей Библиотек и Сборников - для физических лиц

Описание

«**Большая библиотека по информационной безопасности и защите ИТ-систем**» (далее Библиотека) включает документы и материалы, требующиеся многим сотрудникам и руководителям, которые работают в следующих областях.

1. Информационная безопасность и кибербезопасность (как подраздел)
2. Риски информационных систем (ИТ-риски)
3. Операционные риски (в широком определении)
4. Обеспечение непрерывности деятельности (business continuity management) и операционная надёжность (киберустойчивость) организации
5. Управление персональными данными (хранение, обработка, защита)
6. Внутренний аудит, внутренний контроль
7. Управление ИТ-проектами

Библиотека предназначена для решения следующих практических задач

1. Разработка и развитие системы управления информационной безопасностью, включая всю необходимую документацию.
2. Защита информационных активов и ИТ-систем организации, а также обрабатываемых персональных данных.
3. Проектирование и оптимизация бизнес-архитектуры, ИТ-архитектуры, бизнес-процессов и технологических процессов организации с точки зрения информационной безопасности.
4. Обеспечение исполнения внутренних регламентов в области информационной безопасности, выполнение процедур аудита и контроля.
5. Систематизация и распространение знаний в организации, обучение и вовлечение сотрудников.
6. Исполнение государственных и международных стандартов и требований в области информационной безопасности, киберустойчивости и защиты информации.
7. Применение лучших профессиональных практик и инноваций в данной области.
8. Организация эффективной работы подразделения (управления) информационной безопасности.

Внедрение и использование Библиотеки имеет следующие экономические эффекты и выгоды для организации

1. Снижение трудозатрат на разработку документов, выполнение проектов, обучение сотрудников. Быстрое внедрение изменений и нововведений на практике.
2. Возможность выполнить большой объём задач собственными силами без привлечения внешних консультантов, т.е. без дополнительных расходов.
3. Минимизация рисков и ошибок за счёт готовых проверенных на практике материалов и решений.
4. Улучшение показателей KPI бизнес-процессов и ИТ-систем, безопасности и надёжности работы организации в целом. Снижение операционных убытков (потерь).

Пользователи

Библиотека будет полезна для всех подразделений организации, в первую очередь для следующих: управление информационной безопасности, управление экономической безопасности, управление операционных рисков, управление информационных технологий, управления внутреннего контроля и внутреннего аудита, управление процессов (процессный офис).

Структура и материалы Библиотеки

1. Нормативные документы

Общие документы (код IB) 29 документов

- Инструкция категорирования информационных ресурсов (конфиденциальность, целостность)
- Методика проведения анализа рисков информационной безопасности
- Памятка сотруднику по правилам обеспечения информационной безопасности
- Политика информационной безопасности
- Политика тестирования информационной безопасности
- Положение о бесперебойной и безопасной работе информационно-вычислительной сети
- Положение о ролях по обеспечению информационной безопасности

- Положение о системе менеджмента информационной безопасности
- Положение о технических средствах защиты информации
- Положение об анализе и улучшениях системы обеспечения информационной безопасности
- Положение об информационной безопасности
- Положение об информационной безопасности при обеспечении непрерывности бизнеса
- Положение об обучении и проверке знаний сотрудников по информационной безопасности
- Положение об оценке рисков нарушения информационной безопасности
- Порядок проведения аудитов и самооценок информационной безопасности
- Порядок проведения интервью при самооценке информационной безопасности
- Регламент тестирования информационной безопасности
- Методика оценки и анализа рисков информационной безопасности и ИТ-рисков
- Положение о защите конфиденциальной информации
- Положение о конфиденциальном документообороте
- Политика информационной безопасности по работе в сети Интернет
- Политика информационной безопасности по работе с электронной почтой
- Положение об обучении и проверки знаний по информационной безопасности
- Положение об управлении информационными потоками для обеспечения безопасности
- Порядок мониторинга и контроля защитных мер в области ИТ и ИБ
- Порядок обеспечения информационной безопасности при работе в Интернет и с электронной почтой
- Порядок организации расследования инцидентов информационной безопасности
- Процедура поиска несанкционированно функционирующих беспроводных точек доступа
- Рекомендации по обеспечению безопасной работы за компьютером

Защита ИТ-систем (код IB-IS) 22 документа
- Модель угроз безопасности и ИТ-рисков для устройств удаленного доступа
- Модель угроз и нарушителей безопасности информации в ИТ-системах
- Политика по внесению изменений в ИТ-системы в части информационной безопасности
- Политика по обеспечению информационной безопасности технологических процессов и систем
- Политика по управлению доступом к информационным ресурсам и системам
- Положение о защите информации в информационных системах
- Положение о категорировании ИТ-систем и ресурсов в целях защиты
- Положение о механизмах идентификации, аутентификации и авторизации в ИТ-системах и ресурсах
- Положение о проведении контроля защищённости ИТ-систем
- Положение о распределении доступа к ИТ-системам и базам данных
- Положение об обеспечении информационной безопасности процессов в ИТ-системах
- Порядок осуществления контроля за состоянием ИТ-системы и её безопасности
- Порядок предоставления прав доступа к конфиденциальной информации и ИТ-системам
- Порядок проведения тестирования защищенности ИТ-систем
- Порядок разработки систем защиты информации в ИТ-системах
- Порядок эксплуатации систем защиты информации в ИТ-системах
- Типовая детальная модель защиты информационной системы
- Инструкция пользователя по защите информации при работе в ИТ-системах
- Порядок проведения инструментального анализа защищенности ИТ-систем
- Специальные требования и рекомендации по защите конфиденциальной информации от утечки
- План защиты ИТ-системы от несанкционированного доступа и вмешательства
- Регламент мониторинга и контроля защитных мер для ИТ-систем организации

Антивирусная защита, кибератаки (код AV) 15 документов
- Методика обнаружения и противодействия атакам на ИТ-системы организации
- Политика антивирусной защиты
- Положение об антивирусной защите
- Положение об организации антивирусной защиты локальной вычислительной сети
- Положение об управлении уязвимостями информационных ресурсов и систем
- Порядок контроля уязвимостей программного обеспечения в организации
- Инструкция по антивирусной защите (вариант 1)
- Инструкция по антивирусной защите (вариант 2)

- Инструкция по защите от воздействия вредоносных программ (приложений)
- Концепция создания и функционирования системы антивирусной защиты
- Памятка по вопросам антивирусной безопасности для сотрудников
- Политика по обеспечению информационной безопасности средствами антивирусной защиты
- Политика управления системой обнаружения вторжений
- Порядок организации антивирусной защиты
- Регламент обеспечения антивирусной защиты

Криптографическая защита и ЭЦП (код CR) 9 документов
- Инструкция по администрированию средств криптографической защиты информации (СКЗИ)
- Политика использования средств криптографической защиты информации
- Положение об организации криптографической защиты информации
- Положение по работе со средствами криптографической защиты информации и ключевой информацией
- Положение по учету, хранению и использованию носителей ключевой информации (ЭЦП)
- Регламент использования электронной цифровой подписи (ЭЦП) в организации
- Положение по организации и обеспечению безопасности применения криптографических средств
- Порядок обращения с шифровальными средствами (криптографической защиты информации)
- Порядок учета и хранения носителей ключевой информации

Защита персональных данных (код PD) 11 документов
- Классификация информационных систем для обеспечения безопасности персональных данных
- Методы и способы защиты персональных данных от несанкционированного доступа
- Модель угроз информационной системы персональных данных
- Положение о защите персональных данных работников
- Положение о персональных данных
- Порядок доступа к персональным данным, обрабатываемым в ИТ-системах
- Регламент тестирования информационной системы персональных данных
- Система защиты персональных данных - техническое задание 1
- Система защиты персональных данных - техническое задание 2
- Политика обеспечения безопасности персональных данных в ИТ-системах
- Регламент обработки и защиты персональных данных

2. Положения о подразделениях и должностные инструкции (8 файлов)
- Должностная инструкция Начальника отдела по защите информации
- Должностная инструкция Специалиста отдела по защите информации
- Положение о Комитете по информационной безопасности
- Положение об Органе криптографической защиты
- Положение об Отделе безопасности информационных технологий
- Положение об Отделе информационной безопасности
- Положение об Управлении информационной безопасности
- Положение об Удостоверяющем центре

3. Формы документов (12 файлов)
- Акт проверки безопасности информационной инфраструктуры
- Анализ соответствия ИТ-системы требованиям безопасности и рекомендации
- Информационная безопасность и операционная надёжность ИТ-оборудования
- Информационная безопасность и операционная надёжность ИТ-систем
- Отчёт о проверке безопасности информационной системы (ИС)
- Отчёт о результатах обследования процессов обработки персональных данных
- Отчёт о результатах проверки обеспечения защиты персональных данных в ИС
- Отчёт об уровне зрелости системы информационной безопасности
- План действий при возникновении внештатных ситуаций в ИТ-инфраструктуре
- План защиты от несанкционированного доступа к электронным базам данных и сетевым ресурсам
- Программа оценки системы информационной безопасности

- Техническое задание - разработка комплексной системы обеспечения безопасности в ИТ-системе

4. Разные материалы (3 файла)

- Модель процесса «Управление информационной безопасностью» (Information Security Management)
- Показатели KPI процесса «Обеспечение безопасности»
- Статья «Операционная надёжность и операционные риски»