Global Trust Solutions

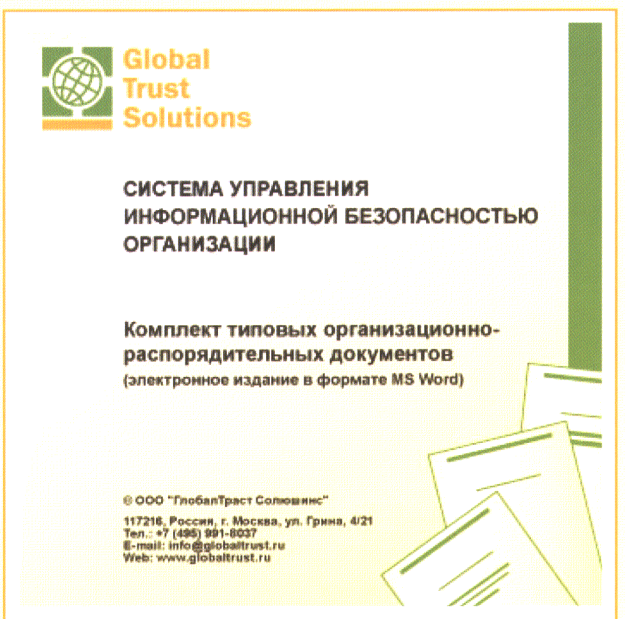
ПОЛИТИКА БЕЗОПАСНОСТИ

ШАБЛОНЫ ТИПОВЫХ ОРГАНИЗАЦИОННО-РАСПОРЯДИТЕЛЬНЫХ ДОКУМЕНТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ГлобалТраст, опираясь на существующую практику обеспечения информационной безопасности в современных российских организациях, успешный мировой опыт и консалтинговые проекты по подготовке российских компаний к сертификации по международному стандарту ISO 27001, разработал и постоянно совершенствует наиболее полную коллекцию типовых организационно-распорядительных документов по информационной безопасности. Эти документы необходимы любой организации для разработки локальной нормативной базы в области информационной безопасности (политик, процедур, инструкций, концепций, положений, стандартов, регламентов, планов, протоколов и т.п.) при внедрении системы управления информационной безопасностью, документировании процессов и требований безопасности, распределении ролей и назначении ответственных за безопасность. Все разрабатываемые ГлобалТраст документы в обязательном порядке проходят практическую апробацию и являются завершенными рабочими документами.

GTS 1035 - КОМПЛЕКТ ТИПОВЫХ ДОКУМЕНТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Предоставляет средства для документирования более 20 ключевых областей обеспечения информационной безопасности. Количество документов в Комплекте постоянно увеличивается.



Содержание:

1. GTS 1036 Концепция обеспечения информационной безопасности организации
2. GTS 1037 Правила обеспечения информационной безопасности при работе пользователей в корпоративной сети организации
3. GTS 1038 Политика и Регламент резервного копирования и восстановления данных
4. GTS 1039 План обеспечения непрерывности бизнеса, Аварийные процедуры, Программа и Протокол тестирования плана
5. GTS 1040 Комплексный план защиты информационных ресурсов организации от несанкционированного доступа
6. GTS 1041 Политика обеспечения безопасности удаленного доступа к ресурсам корпоративной сети организации
7. GTS 1042 Политика обеспечения безопасности при взаимодействии с сетью Интернет
8. GTS 1043 Антивирусная политика, Инструкция по защите от компьютерных вирусов, Стандарт на антивирусное ПО
9. GTS 1044 Политика обеспечения безопасности платежных систем организации
10. GTS 1045 Парольная политика
11. GTS 1046 Политика управления доступом к ресурсам корпоративной сети
12. GTS 1047 Политика, Процедура и План аудита информационной безопасности
13. GTS 1048 Соглашение о соблюдении режима информационной безопасности, заключаемое со сторонними организациями
14. GTS 1049 Политика установки обновлений программного обеспечения
15. GTS 1050 Процедура планирования и реализации превентивных и корректирующих мер по обеспечению ИБ
16. GTS 1051 Руководство по защите конфиденциальной информации, Перечень сведений, составляющих конфиденциальную информацию, Соглашение о конфиденциальности
17. GTS 1052 Процедура управления документами и Процедура управления записями
18. GTS 1053 Регламент использования мобильных устройств
19. GTS 1054 Регламент работы с цифровыми носителями конфиденциальной информации
20. GTS 1055 Политика информационной безопасности

GTS 1056 - КОМПЛЕКТ ТИПОВЫХ ДОКУМЕНТОВ ДЛЯ УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Позволяет в максимальной степени упростить внедрение системы управления рисками информационной безопасности в организации. Мы обобщили накопленный опыт проведения подобных работ и разработали законченный комплект документов, которые достаточно универсальны и в максимальной степени приближены к реальной практике. Используемая качественная методология оценки рисков находится в полном соответствии с требованиями стандартов ISO 27001 и ISO 27005 (BS 7799-3), а также опирается на известные методы оценки рисков CRAMM и OCTAVE.

Для управления рисками в организации недостаточно приобрести какой-либо программный инструментарий, не удастся также напрямую воспользоваться существующими методологиями и стандартами. Ведь, в конечном итоге, каждая организация должна разработать и внедрить свои собственные процессы управления рисками, а на практике это означает создание соответствующей организационной структуры, проведение обучения и осуществление контроля.

Ключевым моментом является разработка документации для управления рисками. Без этого дальше разговоров дело не пойдет. Только грамотно написанная документация, адекватная текущему положению дел, культуре и потребностям бизнеса организации, позволит перейти к внедрению эффективных и измеримых процессов управления рисками.

Содержание:

1. Общее описание
2. Инструкция по внедрению системы управления рисками информационной безопасности в организации
3. Политика управления рисками информационной безопасности
4. Методология оценки рисков информационной безопасности
5. Приложение 1: Определение ценности активов
6. Приложение 2: Модель угроз информационной безопасности
7. Приложение 3: Оценка уровней угроз и уязвимостей
8. Приложение 4. Определение величины рисков
9. Приложение 5: Декларация о применимости механизмов контроля
10. Приложение 6: План обработки рисков
11. Приложение 7: Реестр информационных рисков

Совершенно новое и уникальное предложение для российского рынка. Перейдите на следующий уровень зрелости, внедрив систем управления рисками информационной безопасности в вашей организации!

ПРИОБРЕТЕНИЕ КОМПЛЕКТОВ ДОКУМЕНТОВ

Приобрести данный Комплект документов, а также стандарты, руководства, книги, инструменты и методики, которые легли в основу его разработки, можно в интернет-магазине shop.GlobalTrust.ru.

ПОДДЕРЖКА ВНЕДРЕНИЯ

GlobalTrust обеспечивает полную поддержку внедрения процессов управления рисками информационной безопасности и системы управления информационной безопасностью организации, предоставляя услуги по обучению, консалтингу, аудиту и аутсорсингу. Подробное описание услуг можно найти на корпоративном сайте ГлобалТраст.

ООО "ГлобалТраст Солюшинс"
117216, Россия, г. Москва, ул. Грина, 4/21
Тел.: +7 (495) 991-8037; Тел./Факс: +7 (495) 711-8776
E-mail: info@globaltrust.ru
Интернет-представительство: http://www.globaltrust.ru
Интернет-магазин: http://www.gtrust.ru