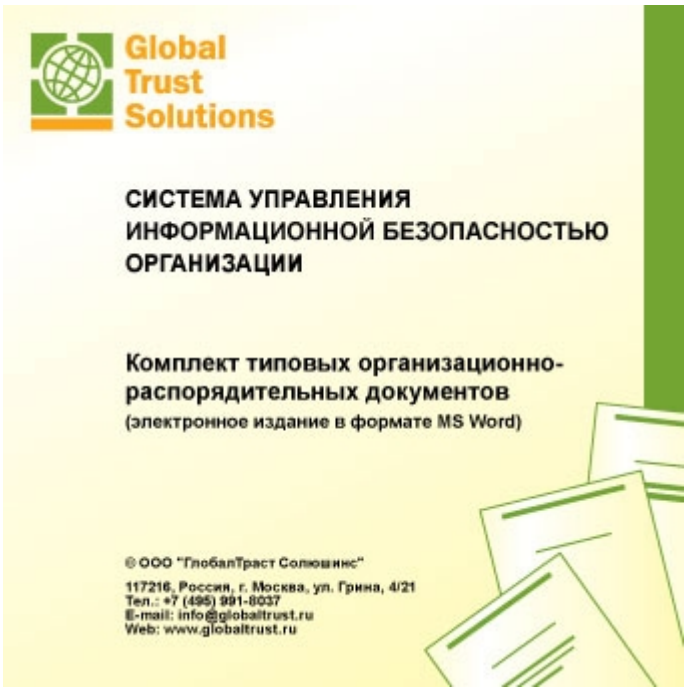
Универсальный комплект типовых документов по информационной безопасности

написано GlobalTrust.ru | 20.08.2023



GTS 1035v2 — Наиболее полный и универсальный комплект документов, предоставляющий средства для документирования всех ключевых областей обеспечения информационной безопасности (содержит более 80 документов по 36 областям ИБ) и подходит для любой организации осуществляющей документирование вопросов защиты информации в соответствии с требованиями международных стандартов, законодательства и нормативной базы. В том числе, он позволяет обеспечить соответствие ISO 27001, СТО БР ИББС, PCI DSS, СТР-К, 382-П, 161-ФЗ и прочим нормативам, актуальным для российских компаний.

Содержание комплекта GTS 1035 v2

1. GTS 0001 Политика информационной безопасности
2. GTS 0002 Концепция обеспечения информационной безопасности

3. GTS 0003 Положение о службе информационной безопасности
4. GTS 0004 План защиты информационных активов от несанкционированного доступа
5. GTS 0005 Правила обеспечения безопасности при работе пользователей в корпоративной сети
6. GTS 0006 План обеспечения непрерывности бизнеса и Аварийные процедуры
7. GTS 0007 Политика резервного копирования и восстановления данных
8. GTS 0008 Политика управления доступом к ресурсам корпоративной сети
9. GTS 0009 Политика управления инцидентами информационной безопасности
10. GTS 0010 Политика обеспечения безопасности удаленного доступа
11. GTS 0011 Политика обеспечения безопасности при взаимодействии с сетью Интернет
12. GTS 0012 Политика антивирусной защиты
13. GTS 0013 Парольная политика
14. GTS 0014 Политика аудита информационной безопасности
15. GTS 0015 Политика контроля состояния СУИБ со стороны руководства
16. GTS 0016 Политика контроля эффективности СУИБ
17. GTS 0017 Процедура планирования и реализации превентивных и корректирующих мер
18. GTS 0018 Политика обеспечения безопасности платежных систем организации
19. GTS 0019 Политика установки обновлений программного обеспечения
20. GTS 0020 Руководство по защите конфиденциальной информации
21. GTS 0021 Процедура управления документами и записями
22. GTS 0022 Регламент использования мобильных устройств
23. GTS 0023 Регламент работы с цифровыми носителями конфиденциальной информации
24. GTS 0024 Политика контроля защищенности корпоративной сети
25. GTS 0025 Политика инвентаризации информационных активов
26. GTS 0026 Политика обеспечения физической безопасности помещений и оборудования
27. GTS 0027 Политика обеспечения пропускного и внутриобъектового режима

28. GTS 0028 Политика в области обучения и повышения осведомленности персонала по ИБ
29. GTS 0029 Политика обеспечения ИБ при взаимодействии с третьими сторонами
30. GTS 0030 Политика предотвращения утечки информации по каналам связи
31. GTS 0031 Политика обеспечения безопасности электронного документооборота
32. GTS 0032 Политика обеспечения целостности информационных активов
33. GTS 0033 Технический стандарт безопасности ИТ-инфраструктуры
34. GTS 0034 Политика регистрации и мониторинга событий ИБ
35. GTS 0035 Политика обеспечения безопасности при разработке ПО
36. GTS 0036 Политика обеспечения безопасного хранения защищаемой информации
37. GTS 0037 Регламент администрирования сетевого оборудования
38. GTS 0038 Политика менеджмента соответствия в области ИБ
39. GTS 0039 Разрешительная система доступа к АС

Типовые документы для внедрения системы управления информационной безопасностью организации

В основе организационных мер защиты информации лежат политики безопасности. В современной практике термин «политика безопасности» может употребляться как в широком, так и в узком смысле слова. В широком смысле, политика безопасности определяется как система документированных управленческих решений по обеспечению безопасности организации. В узком смысле под политикой безопасности обычно понимают локальный нормативный документ, определяющий требования безопасности, систему мер, либо порядок действий, а также ответственность сотрудников организации и механизмы контроля для определенной области обеспечения безопасности. Примерами таких документов могут служить «Политика управления паролями», «Политика управления доступом к ресурсам корпоративной сети», «Политика обеспечения безопасности при

взаимодействии с сетью Интернет» и т.п.

Разработка политик безопасности собственными силами – длительный и трудоемкий процесс, требующий высокого профессионализма, отличного знания нормативной базы в области безопасности и, помимо всего прочего, писательского таланта. Этот процесс обычно занимает многие месяцы и не всегда завершается успешно. Большинство организаций не располагают собственными людскими ресурсами, необходимыми для квалифицированной разработки и внедрения политик безопасности. Отыскать готовые политики безопасности, которые бы оказались применимыми в вашей организации, соответствовали бы ее структуре и требованиям безопасности нереально. Несмотря на доступность соответствующих, в основном англоязычных, ресурсов в сети Интернет, они зачастую являются непригодными для практического использования.

Мы предоставляем набор регулярно обновляемых шаблонов типовых организационно-распорядительных документов в формате MS Word, которые могут использоваться для разработки локальной нормативной базы организации в области информационной безопасности (политик, инструкций, концепций, положений, стандартов, регламентов и т.п.). Все предлагаемые документы успешно прошли стадию практического внедрения.

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 GlobalTrust документы в обязательном порядке проходят практическую апробацию и являются завершенными рабочими документами.

Поддержка внедрения

Мы обеспечиваем поддержку внедрения организационно-распорядительной документации и соответствующих процессов СМИБ организации, предоставляя услуги по обучению, консалтингу, аудиту и аутсорсингу.

Правила лицензирования

Лицензирование шаблонов типовых документов по информационной безопасности производится по количеству систем управления информационной безопасностью (СМИБ), в рамках которых производится использование этих шаблонов. Одна лицензия дает право использования шаблонов в одной организации в рамках одной СМИБ.

Компаниям, предполагающим использование шаблонов документов для оказания услуг другим организациям, требуется приобрести специальную консалтинговую лицензию, либо отдельно приобретать лицензии для каждой организации с учетом скидки на количество приобретаемых лицензий.

Поставка документов осуществляется в электронном виде в формате MS Word на CD-ROM или по e-mail.

Заказ документов

- по телефону: +7 (925) 203-95-11
- по e-mail: info@globaltrust.ru
- через web-форму