

ОГЛАВЛЕНИЕ

Предисловие	3
Введение	6
1. Проблемы обеспечения информационной безопасности цифровой экономики. Задачи исследовательской работы	18
1.1. Истоки понятия «цифровая экономика»	18
1.2. Эволюция «цифровизации»	22
1.3. Программа «Цифровая экономика Российской Федерации»	24
1.4. Угрозы национальной безопасности России в связи с цифровой трансформацией и возможности их нейтрализации	27
1.5. Информационно-технологическая инфраструктура цифровой экономики	32
1.6. Проблема обеспечения доверия к ИТИЦЭ (ИТИВ) .	37
1.6.1. Прямое доказательство уровня защищённости	39
1.6.2. Косвенное доказательство уровня защищённости	40
1.7. Информационно-технологические инфраструктуры обеспечения безопасности на основе инфраструктуры открытых ключей	42
1.7.1. Электронная подпись	42
1.7.2. Доставка ключей	43
1.7.3. Согласование ключей	44
1.7.4. Инфраструктура открытых ключей	45
1.8. Национальная ИОК в Российской Федерации	46
1.9. Проблема уникальности параметров подлинности в рамках национальной инфраструктуры открытых ключей	49
1.10. Задачи исследовательской работы	51

Выводы по Главе 1	54
2. Анализ взаимосвязи доверия и безопасности в информационно-технологических системах	57
2.1. Обзор основных научных работ по теме исследований	58
2.2. Определение доверия с точки зрения нарушителя ...	60
2.3. Доверенная сторона	61
2.3.1. Доверие к клиенту («мыслящему субъекту»)	62
2.3.2. Доверие к логическому объекту	63
2.4. Доверяющая сторона	64
2.5. Доверительные взаимосвязи/взаимоотношения	66
2.6. Преступное намерение	68
2.7. Многообразие и взаимозависимость доверия	70
2.8. Доверие как знания о защищённости (безопасности) ..	72
2.9. Доверие как стратегическая игра	75
2.10. Сравнение защищённости (безопасности) и надёжности	77
2.11. Доверие и вероятность	79
2.12. Доверие в ИТС	81
2.12.1. Основы СЛ	81
2.12.2. Элементы СЛ	84
2.12.3. Понятие доверия в ИТС	92
2.12.4. Транзитивность доверия	99
2.12.5. Оператор понижения доверия	106
2.12.6. Слияние доверия	116
2.12.7. Переоценка доверия	120
Выводы по Главе 2	128
3 Инфраструктуры открытых ключей	134
3.1. Переход к электронному документообороту	134
3.2. Услуги по обеспечению безопасности	135
3.3. Инфраструктура обеспечения безопасности	136
3.4. Организация и компоненты ИОК	138
3.4.1. Компоненты ИОК	140
3.5. Архитектуры открытых ключей	146
3.5.1. Основные типы ИОК в организациях	146
3.5.2. Современные типы ИОК-архитектур	149

3.5.3. Форматы данных, используемые в ИОК	151
3.5.4. Дополнительные ИОК-услуги	160
3.6. Североамериканская модель организации ИОК	161
3.6.1. Состав участников национальной ИОК США	162
3.6.2. Обязанности федеральных ведомств США	167
3.6.3. Модель доверия национальной ИОК США	167
3.7. Западноевропейская модель организации ИОК	173
3.7.1. Основные концепции и иерархическая структура ИОК Евросоюза	173
3.7.2. Модель федеративной ИОК ЕС	176
3.7.3. Реестр состояния доверенных служб (услуг)	179
3.8. Проблемы и риски функционирования ИОК	184
3.8.1. Проверка параметров подлинности	185
3.8.2. Содержание и структура сертификатов	186
3.8.3. Формирование и распределение сертификатов и их доступность	187
3.8.4. Обеспечение цифровыми сертификатами	188
3.9. Проблемы и риски пользователей ИОК	193
3.9.1. Кому или чему доверяют пользователи ИОК?	195
3.9.2. Кто использует ключ пользователя ИОК?	196
3.9.3. Каков уровень защищённости проверяющего компью- тера?	197
3.9.4. Кто такой Иван Иванович Иванов?	198
Выводы по Главе 3	199
4 Модели доверия на основе ИОК	205
4.1. Системы обеспечения параметрами подлинности	205
4.2. Субъекты/объекты, параметры подлинности и иден- тификаторы	206
4.3. Изолированная система обеспечения параметрами подлинности	208
4.3.1. Архитектура изолированной СОПП	208
4.3.2. Проблемы доверия в изолированной СОПП	210
4.4. Федеративная система обеспечения параметрами под- линности	211
4.4.1. Архитектура федеративной СОПП	211
4.4.2. Проблемы доверия в федеративной СОПП	212
4.5. Централизованная система обеспечения параметрами подлинности	215

4.5.1. Архитектура централизованной СОПП	215
4.5.2. Проблемы доверия в централизованных СОПП	219
4.6. Системы персональной аутентификации	220
4.6.1. Архитектура системы персональной аутентификации	220
4.6.2. Проблемы доверия в системах персональной аутентификации	225
4.7. Сравнение моделей обеспечения пользователей ПП .	225
4.8. Системы обеспечения ПЭУ параметрами подлинности	227
4.8.1. Архитектуры систем обеспечения ПЭУ ПП	228
4.8.2. Проблемы доверия в системах обеспечения ПЭУ ПП	233
4.9. Параметры подлинности в сертификатах ИОК	235
4.10. Структуры доверия на основе ИОК	239
4.10.1. Одиночная иерархическая ИОК-инфраструктура ...	246
4.10.2. Многоиерархическая ИОК	247
4.10.3. Избираемое прямое доверие	251
4.10.4. Взаимная сертификация нескольких корневых ЦС .	253
4.10.5. ИОК-модель со связующим ЦС	253
4.10.6. PGR-модель доверия	255
4.10.7. ИОК с центром подтверждения подлинности сертификатов	257
4.10.8. Простая ИОК (простая распределённая инфраструктура обеспечения безопасности) и делегирование сертификатов	259
4.10.9. ИОК на основе защищённой DNS-системы	261
4.11. Семантика доверия и параметра подлинности	265
4.12. Дальнейшее развитие ИОК	268
Выводы по Главе 4	270
5. Модель национальной системы доверия на основе ИОК	275
5.1. Синтез сетей субъективного доверия в СЛ	275
5.1.1. Графы сетей доверия	276
5.1.2. Выходное-входное множество	277
5.1.3. Анализ сетей доверия, отображаемых в форме ППОГ	280
5.1.4. Анализ сложных сетей доверия, не отображаемых в форме ППОГ	286
5.2. Синтез национальной системы доверия на основе инфраструктуры открытых ключей	298

5.2.1. Ретроспектива	298
5.2.2. Исходные условия и синтез национальной системы доверия на основе ИОК	305
5.2.3. Усовершенствованная модель национальной системы доверия на основе ИОК	311
5.3. Функционально-структурная модель национальной системы доверия на основе ИОК	313
5.3.1. ЦПП федерального уровня	318
5.3.2. ЦПП федерального окружного уровня	318
5.3.3. ЦПП регионального уровня	319
5.3.4. ЦПП муниципального уровня	319
5.4. Методы защиты пользователей ИОК	319
5.4.1. Противодействие изданию фальсифицированных СЕРТ _{ОК}	320
5.4.2. Распознавание поддельных (мошеннических) web-сайтов	325
5.5. Использование IPv6-адресов в качестве национальных (глобальных) ПП	330
5.5.1. Свойства логической характеристики IPv6-протокола	330
5.5.2. Международный стандарт ISO 3166	331
5.5.3. Структура данных для информационного обеспечения Интернет-сети	332
5.5.4. Описание метода	333
5.5.5. Противоречие с положениями стандартов RFC-3587 и RFC-4291	334
5.5.6. Расширение предлагаемого метода на локальные IPv6-адреса	335
5.5.7. Обоснование и следствия	337
5.5.8. Реализационные аспекты	339
Выводы по Главе 5	342
Заключение	346
Перечень сокращений и обозначений	350
Словарь терминов	354
Литература	356
Приложения	373
Приложение 1. Директива президента США «Public Encryption Management»	373
Приложение 2. Операторы, используемые в СЛ	377