А.М. Сычев, П.В. Ревенков, А.Б. Дудка

БЕЗОПАСНОСТЬ ЭЛЕКТРОННОГО БАНКИНГА

Банк Воронеж PayPal

БЭСТ CREDIT PILOT ДЕНЕЖНЫЕ ПЕРЕВОДЫ

АССОЦИАЦИЯ ФИНАНСОВЫХ ИННОВАЦИЙ

Москва
2017

УДК 004.56
ББК 32.971.353
С95

Сычев А.М., Ревенков П.В., Дудка А.Б.

С95 Безопасность электронного банкинга / А.М. Сычев, П.В. Ревенков, А.Б. Дудка. — М.: Интеллектуальная литература, 2017. — 318 с.

ISBN 978-5-9908133-4-2

Книга «Безопасность электронного банкинга» посвящена вопросам, связанным с обеспечением безопасного функционирования систем электронного банкинга.

А.М. Сычев, П.В. Ревенков, и А.Б. Дудка описывают в ней основные принципы управления рисками электронного банкинга и риски, возникающие в кредитных организациях при внедрении ими систем интернет-банкинга, а также организация внутреннего контроля при использовании систем электронного банкинга, обеспечение информационной безопасности электронного банкинга с учетом требований стандартов Банка России по обеспечению информационной безопасности, а также приводятся уникальные для российской аудитории примеры влияния «теневого Интернета» на безопасность электронного банкинга.

Издание предназначено для банковских специалистов, практикующих консультантов и аудиторов, преподавателей, аспирантов и студентов, обучающихся финансовым специальностям в вузах.

УДК 004.56
ББК 32.971.353

ISBN 978-5-9908133-4-2

СОДЕРЖАНИЕ

Вступительное слово 7
Предисловие 9
Список авторов 11
Список сокращений 12
Введение 13

1. Электронный банкинг и риски недостаточного обеспечения информационной безопасности 15
1.1. Интернет и банковский бизнес 15
1.2. Основные виды мошенничества в сети Интернет 24
1.3. Актуальные направления регулирования в условиях электронного банкинга 39

2. Кибербезопасность в условиях применения систем электронного банкинга 51
2.1. Парадигмы построения системы кибербезопасности 51
2.2. Методология анализа рисков недостаточного обеспечения кибербезопасности 54
2.3. Информационное общество и кибербезопасность 59
2.4. Электронные финансы — в Интернет вещей 63
2.5. Кибербезопасность в условиях развития Интернета вещей и электронного банкинга 67

3. Принципы управления рисками электронного банкинга 72
Введение 72
3.1. Проблемы, связанные с управлением рисками электронного банкинга 74
3.2. Основные принципы управления рисками электронного банкинга 76
3.2.1. Наблюдение со стороны совета директоров и высшего руководства банка (Принципы 1–3) 78
3.2.2. Средства обеспечения безопасности (Принципы 4–10) 90

3.2.3. Управление правовым и репутационным рисками (Принципы 11–14). 102

4. Возможные риски при использовании технологии интернет-банкинга 110
Введение. 110
4.1. Развитие интернет-банкинга. 112
4.2. Типы интернет-банкинга 115
4.3. Риски интернет-банкинга 116
4.3.1. Кредитный риск 117
4.3.2. Процентный риск 118
4.3.3. Риск ликвидности. 118
4.3.4. Ценовой риск 119
4.3.5. Валютный риск 119
4.3.6. Операционный риск. 120
4.3.7. Риск несоответствия 122
4.3.8. Стратегический риск 122
4.3.9. Репутационный риск 124
4.4. Управление рисками. 125
4.5. Внутренний контроль 127

5. Организация внутреннего аудита и внутреннего контроля в кредитных организациях при использовании систем электронного банкинга 128
5.1. Качество корпоративного управления в части развития и применения систем электронного банкинга 128
5.1.1. Ориентированность кредитной организации на развитие технологий электронного банкинга. 128
5.1.2. Роль совета директоров кредитной организации в организации внутреннего контроля 131
5.1.3. Общие процедуры организации внутреннего аудита и внутреннего контроля. 134
5.1.3.1. Документарное обеспечение системы внутреннего контроля 134
5.1.3.2. Особенности подбора кадров в службу внутреннего аудита и службу внутреннего контроля 137

5.1.3.3. Методологическое обеспечение службы внутреннего аудита и службы внутреннего контроля 140
5.1.3.4. Организация работы службы внутреннего аудита и службы внутреннего контроля с результатами проверок применения технологий электронного банкинга. 142
5.1.4. Организация управления рисками, связанными с использованием системы электронного банкинга 145
5.2. Организация (адаптация) процедур внутреннего аудита и контроля в части системы электронного банкинга 151
5.2.1. Организация процедур внутреннего аудита и контроля на этапе обоснования нового проекта системы электронного банкинга 153
5.2.2. Организация процедур внутреннего контроля на этапе принятия решения о новом проекте системы электронного банкинга 157
5.2.3. Организация (адаптация) процедур внутреннего аудита и контроля на этапе планирования реализации системы электронного банкинга 162
5.2.4. Организация (адаптация) процедур внутреннего аудита и контроля на этапе проектирования системы электронного банкинга 164
5.2.5. Организация (адаптация) процедур внутреннего аудита и контроля на этапе разработки системы электронного банкинга 170
5.2.6. Организация (адаптация) процедур внутреннего аудита и контроля на этапе испытаний, сдачи и приемки в эксплуатацию системы электронного банкинга 187
5.2.7. Организация (адаптация) процедур внутреннего контроля на этапе эксплуатации системы электронного банкинга 202

6. Обеспечение информационной безопасности электронного банкинга с учетом требований стандартов Банка России по обеспечению информационной безопасности 209

7. О средствах и способах защиты информации . . . 235

Введение . . . 235

7.1. Наложенные средства защиты информации . . . 237

7.1.1. Аппаратный модуль доверенной загрузки . . . 240

7.1.2. Защита клиентских рабочих мест . . . 243

7.1.2.1. Классические тонкие клиенты . . . 246

7.1.2.2. Работа с ЦОДом как эпизодическая задача . . . 248

7.1.2.3. Работа с ЦОДом как задача руководителя . . . 251

7.2. Устройства с правильной архитектурой . . . 252

7.2.1. Компьютеры . . . 253

7.2.1.1. Пример целесообразного использования микрокомпьютера новой гарвардской архитектуры . . . 258

7.2.2. Служебные носители (флешки, ключевые носители, средства хранения журналов) . . . 271

7.2.2.1. Флешки . . . 272

7.2.2.2. Ключевые носители . . . 278

7.2.2.3. Другие служебные носители . . . 289

8. Влияние «теневого интернета» на безопасность электронного банкинга . . . 290

Введение . . . 290

8.1. Проблемы политического характера . . . 292

8.2. Проблема «теневого Интернета» на примере системы TOR и идентификации злоумышленников . . . 294

8.3. Проблемы законодательного характера . . . 302

8.4. Проблемы обеспечения информационной безопасности на местах в банковском секторе . . . 305

8.5. Проблемы обеспечения информационной безопасности на стороне клиента . . . 308

Заключение . . . 310

Список использованных источников и литературы . . . 312

Нормативные правовые акты . . . 312

Книги и статьи . . . 313

Электронные ресурсы . . . 316

Документы, размещенные на официальном сайте Базельского комитета по банковскому надзору (bis.org) . . . 317