

Информационная безопасность банковских безналичных платежей. Часть 5 — 100+ тематических ссылок про взломы банков



Обновлено: 20.08.2018

При подготовке материалов для следующих статей набралась довольно обширная коллекция ссылок на темы:

- хакерских атак на банки,
- технического анализа банковских взломов,
- обзора типовых уязвимостей в банковских сетях,
- судебной практики,
- аналитики, прогнозов и других статей по банковской безопасности.

В какой-то момент времени количество подобранных материалов переросло в качество, так что данная подборка может заинтересовать уже сама по себе.

Публикации в СМИ о хакерах и инцидентах

2015

1. [“Хакеры из Горного Алтая украли из банка десятки миллионов”, –altapress.ru, 2015](http://altapress.ru)

2. [“Хакерам из Москвы грозит по 10 лет за хищение 20 млн у банка”, – sobesednik.ru, 2015](#)

2016

3. [“Хакеры украли у четырёх банков миллиард рублей с помощью бота”, – Life.ru, 2016](#)

4. Сюжет: «Кража из Русского международного банка (РМБ)»

а) [“С корсчета в ЦБ хакеры похитили свыше полумиллиарда рублей», — interfax.ru, 2016](#)

б) [“Русский международный банк назвал сумму похищенных хакерами средств”, — rbc.ru, 2016](#)

5. Сюжет: «Кража из Металлинвестбанка»

а) [“Хакеры вывели 677 млн руб. со счетов Металлинвестбанка”, – rbc.ru, 2016](#)

б) [“Из-за хакерской атаки Металлинвестбанк потерял 200 млн рублей”, — ria.ru, 2016](#)

в) [“Пресс-релиз Металлинвестбанка по факту кражи”, — metallinvestbank.ru, 2016](#)

г) [“Ограбление по-хакерски”, — kommersant.ru, 2017](#)

6. [“АБС не сработала”, – kommersant.ru, 2016](#)

7. [“Хакеры украли у банков почти 2 млрд руб. с помощью «писем от ЦБ” – RBC.ru, 2016](#)

8. [“Миллион за пару минут. Как хакеры грабят банки по всему миру”, — 21.by, 2016](#)

9. [“В Свердловской области перед судом предстанут «хакеры», обвиняемые в хищении более 2,6 млн рублей со счетов банков в различных регионах страны”, — Генеральная Прокуратура РФ, 2016](#)

10. Сюжет: Хакерская группа Lurk

а) [“Банковский троянец Lurk: специально для России”, — Securelist.ru, 2016](#)

б) [“Сотрудники МВД России и ФСБ России задержали интернет-хакеров”, — МВД России, 2016](#)

в) [“Охота на Lurk”, — Securelist.ru, 2016](#)

11. [“Суд взыскал 470 млн рублей с процессинговой компании UCS”, — vedomosti.ru, 2016](#)

2017

12. [“От Юты до Енисея: хакеры атакуют банки США и России”, — Газета.ru, 2017](#)

13. [“Group-IB оценила масштаб деятельности русскоязычных хакеров MoneyTaker”, — rbc.ru, 2017](#)

14. [“Сооснователь Group-IB рассказал о совершивших кибератаку на банки России”, — rbc.ru, 2017](#)

15. Сюжет: „Кража из банка “Глобэкс»

а) [“Хакеры прибежали на SWIFT”, — kommersant.ru, 2017](https://kommersant.ru)

б) [“Хакеры пришли в “Глобэкс”, — kommersant.ru, 2017](https://kommersant.ru)

в) [“Хакеры украли из дочернего банка ВЭБа \\$1 млн”, — vedomosti.ru, 2017](https://vedomosti.ru)

16. [“Хакерские атаки собрали в группировку”, — Коммерсант.ru, 2017](https://kommersant.ru)

17. [“Digital Security опровергает связь участника Zeronights с MoneyTaker”, — anti-malware.ru, 2017](https://anti-malware.ru)

18. Сюжет: Группа из 14 хакеров, грабившая банки

а) [“Боксёр с Украины возглавлял группировку хакеров, укравших 1 млрд рублей у банков”, — Life.ru, 2016](https://life.ru)

б) [“У хакера сработала программа раскаяния”, — kommersant.ru, 2017](https://kommersant.ru)

в) [“Суд взламывает хакерскую сеть”, -kommersant.ru, 2017](https://kommersant.ru)

2018

19. [“Хакеры похитили сотни миллионов у банков Мексики”, — SecurityLab.ru, 2018](https://securitylab.ru)

20. Сюжет: «Преступная группа из Волжского»

а) [“В Волжском задержан похищавший средства с банковских карт хакер”, - SecurityLab.ru, 2018](https://securitylab.ru)

б) [“Хакеры зарабатывали до полумиллиона в день”, — Коммерсант.ru, 2018](https://kommersant.ru)

21. Сюжет: «Подготовка к атаке на российские платежные системы»

а) [“В Северске хакера осудили за подготовку атаки на российские платежные системы”, — SecurityLab.ru, 2018](https://securitylab.ru)

б) [“Кибератаку на российские электронные платежные системы предотвратили в Томске”, — ib-bank.ru, 2018](https://ib-bank.ru)

22. [“В Ставропольском крае задержан хакер за взлом банкоматов и хищение средств”, -SecurityLab.ru, 2018](https://securitylab.ru)

23. [“В Саратове хакер похитил более 380 тыс. рублей с помощью фишингового сайта”, — SecurityLab.ru, 2018](https://securitylab.ru)

24. [“Питерский хакер похищал средства с банковских карт”, — SecurityLab.ru, 2018](https://securitylab.ru)

25. [“Деньги из ЦБ крадут призрачные хакеры”, — dailystorm.ru, 2018](https://dailystorm.ru)

26. [“У начинающих хакеров появились учителя по взлому банкоматов”, — dni24.com, 2018](https://dni24.com)

27. Сюжет: «Арест лидера преступной группы Carbanak / Anunak / Cobalt»

а) [“Mastermind behind eur 1 billion cyber bank robbery arrested in spain”, — Европол, 2018](https://eur1.billion.cyber.bank.robbery.arrested.in.spain) + ([тут](#))

б) [“Арестован украинский хакер, предположительно являющийся лидером Carbanak”, - SecurityLab.ru, 2018](https://securitylab.ru)

в) [“Лидер Carbanak попался на нежелании вовремя заплатить за машину”, — SecurityLab.ru, 2018](https://securitylab.ru)

28. Сюжет: «Продолжение активности преступной группы Cobalt после ареста ее лидера»

а) [“Group-IB: несмотря на арест лидера, группа Cobalt продолжает атаки на банки”, — Group-IB, 2018](#)

б) [“Арест лидера не прекратил деятельность группы Cobalt: хакеры атаковали крупные банки России и СНГ”, — хакер.ru, 2018](#)

29. [«В Москве осуждены киберпреступники, похищавшие средства у клиентов банков», — SecurityLab.Ru, 2018](#)

30. [«ПИР Банк лишился более 58 млн рублей в результате кибератаки», — SecurityLab.Ru, 2018](#)

31. [«Следственными органами МВД России направлено в суд дело о хищении денежных средств с банковских карт граждан», — МВД России, 2018](#)

32. [“Кибермошенники осуждены в Москве за кражу денег через интернет-кабинеты банков”, — ИА Интерфакс, 2018](#)

33. Сюжет: «Кража из „ПИР Банка“

а) [“ПИР для хакеров”, — kommersant.ru, 2018](#)

б) [“Как тебе такое, Carbanak?”, — Gorup-ib.ru, 2018](#)

34. [“Прокуратура Республики Башкортостан направила в суд уголовное дело по факту хищения хакерами свыше 8 млн. рублей”, — Генеральная Прокуратура РФ, 2018](#)

35. [»В США суд выдвинул обвинения 3 членам хакерской группировки Carbanak”, — SecurityLab.ru, 2018](#)

36. [«Екатеринбургские хакеры похитили у банков 1,2 млрд руб.», — SecurityLab.ru, 2018](#)

Технический анализ инцидентов

2014

1. [Доклад: «COMPUTER FORENSIC INVESTIGATION OF {mobile} BANKING TROJAN», — Zeronights 2014, Иванов Борис](#)

2015

2. [Отчет: “Технический отчет о деятельности преступной группы, занимающейся целевыми атаками — Anunak”, — Group-IB, 2015 \(+ статья\)](#)

3. [Отчет: “Атаки на брокерские и расчетные системы”, — Group-IB, 2015](#)

4. [Большое банковское ограбление: APT-кампания Carbanak, — securelist.ru, 2015 \(+ отчет english\)](#)

2016

5. [“Увеличивается количество АРТ-ограблений банков с использованием атак Metel, GCMAN и Carbanak 2.0”, – securelist.ru, 2016](#)
6. [Отчет: “Buhtrap: эволюция целенаправленных атак на банки”, – Group-IB, 2016](#)
7. [Отчет: “Cobalt snatch”, — Positive Technologies, 2016](#)

2017

8. [Отчет: “Cobalt strikes back: новые атаки на финансовые организации”, — Positive Technologies, 2017](#)
9. [“По следу Cobalt: тактика логической атаки на банкоматы в расследовании Group-IB”, — Блог компании Group-IB на habr.com, 2017](#)
10. [“Секреты Cobalt Как группа Cobalt преодолевает средства защиты”, — Group-IB, 2017](#)
11. [“MoneyTaker: охота на невидимку Group-IB рассекретила хакеров, атакующих банки в США и России”, — Group-IB, 2017](#)
12. [“Lazarus Технологии шпионажа и целевых атак проправительственных хакеров из Северной Кореи и неизвестные подробности их операций в отчете Group-IB «Lazarus: архитектура, инструменты, атрибуция», — Group-IB, 2017](#)
13. [Атаки на банкоматы на примере GreenDispenser: организация и технологии”, — Positive Technologies, 2017](#)
14. [“The Silence — новая целевая атака на финансовые организации”, — Securelist.ru, 2017](#)
15. [“Финансовая кампания TwoBee”, — Securelist.ru, 2017](#)

2018

16. [“Большая разница: Cobalt vs MoneyTaker Чем отличаются две самые активные преступные группы”, — Group-IB, 2018](#)
17. [“Новые атаки на банки”, — Positive Technologies, 2018](#)
18. [Вебинар: “Исследование целенаправленных атак на финансовые организации”, — Positive Technologies, 2018 \(+ презентация\)](#)
19. [»Атаки на промышленные предприятия с использованием RMS и TeamViewer“, — Securelist.ru, 2018](#)

Прогнозы и обзоры

2016

1. [“Обзор финансовой стабильности II—III кварталы 2016 г.”](#), — Банк России, 2016

2017

2. [“Hi-Tech Crime Trends 2017”](#), — Group-IB, 2017 (+ [данный отчет на внешнем ресурсе](#))
3. [“Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России: 1 июня 2016 – 1 сентября 2017”](#), — ФинЦЕРТ ЦБ РФ, 2017
4. [“Основные типы атак в кредитно-финансовой сфере в 2017 году”](#), — ФинЦЕРТ ЦБ РФ, 2017
5. [“Обзор несанкционированных переводов денежных средств за 2017 год”](#), — ФинЦЕРТ ЦБ РФ, 2017
6. [“Киберпреступники против финансовых организаций: чего ждать в 2018 году”](#), — Securelist.ru, 2017
7. [Вебинар: “Актуальные киберугрозы – 2017: тренды и прогнозы”](#), — Positive Technologies, 2018 (+ [отчет](#))

2018

8. [“Финансовые киберугрозы в 2017 году”](#), — Securelist.ru, 2018

Судебная практика

1. “Материалы судебных разбирательств между АО «Кемсоцинбанк» и другими банками, через которые были обналичены украденные у него деньги”, — Арбитражные и апелляционные суды, 2017-18 ([тут](#) и [тут](#))

Регулярные обзоры и тематические ресурсы

1. [«Преступления в банковской сфере»](#), — amulet-group.ru
2. [“Архив securelist.ru, рубрика “Атака на банки”](#), — securelist.ru
3. [“ФинЦЕРТ Банка России”](#), — Банк России

4. [“Расследования высокотехнологичных преступлений”, — Рубрикатор на сайте Group-IB.ru](#)
5. [Сюжет “Хакерские атаки на российские банки”, — РИА Новости](#)
6. [Threat Actor Map](#)
7. [Рубрика: «Стража со взломом», — Komersant.ru](#)
8. [«Рубрикатор: Киберпреступность официального сайта МВД России», — МВД России](#)
9. [Периодические отчеты: «Состояние преступности» — МВД России](#)

Уязвимости

2013

1. [“Анализ безопасности мобильных банковских приложений за 2012 год”, — Digital Security, 2013](#)

2014

2. [“Безопасность мобильного банкинга: возможность реализации атаки MitM”, — Digital Security, 2014](#)
3. [“VM escape: 101”, – Блог компании Digital Security на habr.com, 2014](#)

2015

4. [“Безопасность веб-ресурсов банков России”, — Digital Security, 2015](#)

2016

5. [Вебинар: “Подводные камни прикладной криптографии” — Positive Technologies, 2016 \(+ презентация\)](#)

2017

6. [“Уязвимости приложений финансовой отрасли”, – Positive Technologies, 2017](#)
7. [“Автоматизированный анализ кода: статистика уязвимостей веб-приложений за 2017 год”, — Positive Technologies, 2017](#)

8. [“Статистика атак на веб-приложения: IV квартал 2017 года”, — Positive Technologies, 2017](#)
9. [“Корпоративные информационные системы: тестирование на проникновение сценарии атак”, — Positive Technologies, 2017](#)
10. [Вебинар: “Типовые сценарии атак на беспроводные сети”, — Positive Technologies, 2017 \(+ презентация\)](#)
11. [Вебинар: “Типовые сценарии атак на корпоративную информационную систему”, — Positive Technologies, 2017 \(+ презентация\)](#)

2018

12. [“Исследование: больше половины систем дистанционного банковского обслуживания содержат критические уязвимости”, — Блог компании Positive Technologies на habr.com, 2018](#)
13. [Вебинар: “Продвинутые атаки на Microsoft Active Directory: способы обнаружения и защиты”, — Positive Technologies, 2018 \(+ презентация\)](#)
14. [“Уязвимости корпоративных информационных систем 2018”, — Positive Technologies, 2018](#)
15. [“Как социальная инженерия открывает хакеру двери в вашу организацию”, — Positive Technologies, 2018](#)
16. [Вебинар: “Анализ защищенности АТМ: логические атаки и уязвимости”, — Positive Technologies, 2018 \(+ презентация\)](#)
17. [«К купюрам пробрались через сейф», — kommersant.ru, 2018](#)
18. [«Низкоуровневый взлом банкоматов NCR», — Блог компании Positive Technologies на habr.com, 2018](#)

Аналитические статьи

2013

1. [“Обеспечение безопасности систем ДБО на всех этапах жизненного цикла”, — Аналитический банковский журнал, 2013](#)

2014

2. [“Атаки на автоматизированные банковские системы”, — BIS-journal, 2014](#)

2015

3. [“АБС под прицелом”, — Аналитический банковский журнал, 2015](#)
4. [“Ограбление XXI века: хакерам удалось украсть \\$1 млрд”, — Лаборатория Касперского, 2015](#)
5. [“Russian financial cybercrime: how it works”, — securelist.com, 2015](#)

2016

6. [“Десятки российских банков потеряли миллионы долларов из-за атак киберпреступников”, — Лаборатория Касперского, 2016](#)
7. [“Банкер, который может украсть все”, — securelist.com, 2016](#)
8. [«Хакеры против банков: самые громкие преступления последних лет», — Rbc.ru, 2016](#)

2017

9. [“Как хакеры готовят атаки на банки”, — Блог компании Positive Technologies на habr.com, 2017](#)
10. [“Целевые атаки на банки России как тестовый полигон”, — Group-IB, 2017](#)
11. [“Ограбление по-хакерски”, — Kommersant.ru, 2017](#)

2018

12. [“Новостные сайты в Рунете распространяли банковского троянца”, — Securelist.ru, 2018](#)
13. [“3000 долларов за вечер. Как работают киберпреступники, которые могут ограбить любого”, — tut.by, 2018](#)
14. [“Кибератаки — наша повседневность. Хакеры нацелились на мобильные банки и промышленность”, — 360tv.ru, 2018](#)
15. [“Атаки на банки”, — Positive Technologie, 2018](#)
16. [«Схемы хищений в системах ДБО и пять уровней противодействия им», — Блог компании Group-IB на habr.com, 2018](#)
17. [«Pegasus подкрался незаметно», — Kommersant.ru, 2018](#)
18. [«Рынок преступных киберуслуг 2018», — Positive Technology, 2018](#)
19. [«Трояны множатся в мобильном банке», — Kommersant.ru, 2018](#)
20. [«APT Trends Report Q2 2018», — Securelist.com, 2018](#)
21. [«О преступлениях, совершаемых с использованием современных информационно-коммуникационных технологий», — Генеральная Прокуратура РФ,](#)

2018

Разное

1. “ИНСТРУКЦИЯ по реагированию на инциденты, связанные с системами дистанционного банковского обслуживания”, — Group-IB, 2012 (анонс)