**Лукин А.П.**

Senulukun@mail.ru,

Россия, Санкт-Петербург

Международный банковский институт имени Анатолия Собчака

**Пискунова Т.Г**, доцент – научный руководитель.

Аннотация: способы кибератак,варианты защиты.

Ключевые слова: кибербезопасность,атака,уязвимость.

Кибербезопасность банковских систем

Кибербезопасность банковской системы

Введение

Со времени своего появления банки неизменно вызывали преступный интерес. И этот интерес был связан не только с хранением в кредитных организациях денежных средств, но и с тем, что в банках сосредотачивалась важная и зачастую секретная информация о финансовой и хозяйственной деятельности многих людей, компаний, организаций и даже целых государств. В настоящее время в результате повсеместного распространения электронных платежей, пластиковых карт, компьютерных сетей объектом информационных атак стали непосредственно денежные средства как банков, так и их клиентов. Совершить попытку хищения может любой -- необходимо лишь наличие компьютера, подключенного к сети Интернет. Именно эта проблема является сейчас наиболее актуальной и наименее исследованной. Если в обеспечении физической и классической информационной безопасности давно уже выработаны устоявшиеся подходы (хотя развитие происходит и здесь), то в связи с частыми радикальными изменениями в компьютерных технологиях методы безопасности автоматизированных систем обработки информации банка (АСОИБ) требуют постоянного обновления. Как показывает практика, не существует сложных компьютерных систем, не содержащих ошибок. А поскольку идеология построения крупных АСОИБ регулярно меняется, то исправления найденных ошибок и "дыр" в системах безопасности хватает ненадолго, так как новая компьютерная система приносит новые проблемы и новые ошибки, заставляет по-новому перестраивать систему безопасности.

Каждая вторая атака на финансовый сектор осуществляется с использованием шифровальщика

В [Positive Technologies](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:Positive_Technologies" \o "Positive Technologies) проанализировали динамику защищенности кредитно-[финансового](https://www.tadviser.ru/index.php/%D0%A4%D0%B8%D0%BD%D0%B0%D0%BD%D1%81%D1%8B) сектора. Каждая вторая [атака](https://www.tadviser.ru/index.php/%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B8) на этот сектор осуществляется с использованием [вредоносного ПО](https://www.tadviser.ru/index.php/%D0%92%D1%80%D0%B5%D0%B4%D0%BE%D0%BD%D0%BE%D1%81%D0%BD%D0%BE%D0%B3%D0%BE_%D0%9F%D0%9E) — [шифровальщика](https://www.tadviser.ru/index.php/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BB%D1%8C%D1%89%D0%B8%D0%BA). Кроме этого, эксперты фиксируют двукратный рост [продаж](https://www.tadviser.ru/index.php/%D0%A2%D0%BE%D1%80%D0%B3%D0%BE%D0%B2%D0%BB%D1%8F) доступов к корпоративным сетям финансовых организаций в [дарквебе](https://www.tadviser.ru/index.php/%D0%94%D0%B0%D1%80%D0%BA%D0%BD%D0%B5%D1%82" \o "Даркнет) на фоне снижения их стоимости в 4 раза. Об этом 10 ноября 2022 года сообщила компания Positive Technologies.

Как сообщается в исследовании, по итогам трех первых кварталов 2022 года общее число продаж доступов к корпоративным сетям [банков](https://www.tadviser.ru/index.php/%D0%91%D0%B0%D0%BD%D0%BA%D0%B8) в дарквебе выросло в два раза по сравнению с аналогичным периодом 2021 года. Стоимость варьируется от 250 до 30 000 [долл. США](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%94%D0%BE%D0%BB%D0%BB%D0%B0%D1%80_%D0%A1%D0%A8%D0%90) в зависимости от организации и привилегий в сети, которые получает покупатель. По мнению экспертов, такой рост активности может быть обусловлен четырехкратным снижением минимальной цены: с 1000 до 250 долл. [США](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A1%D0%BE%D0%B5%D0%B4%D0%B8%D0%BD%D0%B5%D0%BD%D0%BD%D1%8B%D0%B5_%D1%88%D1%82%D0%B0%D1%82%D1%8B_%D0%90%D0%BC%D0%B5%D1%80%D0%B8%D0%BA%D0%B8_(%D0%A1%D0%A8%D0%90)).

Анализ Positive Technologies показал, что в атаках на финансовые организации злоумышленники чаще всего используют методы [социальной инженерии](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A1%D0%BE%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%B8%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D0%B8%D1%8F) (47% случаев) и реже прибегают к эксплуатации уязвимостей, чем при атаках на другие отрасли. По мнению экспертов, это связано с лучшей защищенностью сетевого периметра организаций финансовой отрасли. Преступникам дешевле и проще найти нелояльных сотрудников банков, которые готовы предоставить им доступ к системам или конфиденциальную информацию, чем взламывать периметр компании путем эксплуатации [уязвимостей](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A3%D1%8F%D0%B7%D0%B2%D0%B8%D0%BC%D0%BE%D1%81%D1%82%D0%B8_%D0%B2_%D0%9F%D0%9E_%D0%B8_%D0%BE%D0%B1%D0%BE%D1%80%D1%83%D0%B4%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B8).

По итогам первых трех кварталов 2022 года общее количество атак на финансовые организации снизилось на 16% по сравнению с аналогичным периодом 2021 года. Доля кибератак на финансовую отрасль в последние годы в целом сокращалась и на ноябрь 2022 года составляет около 5% от числа всех кибернападений на организации. Эксперты объясняют это тем, что банки традиционно вкладываются в безопасность и следуют отраслевым стандартам [ИБ](https://www.tadviser.ru/index.php/%D0%98%D0%91).

Рост вредоносных программ на 428%

3 февраля 2022 года компания [Eset](https://www.tadviser.ru/index.php/Eset) сообщила о том, что количество обнаружений вредоносных программ для [Android](https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:Android" \o "Android)-банкинга выросло на 428% в 2021 году по сравнению с 2020 годом. В пятёрку [стран](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A1%D1%82%D1%80%D0%B0%D0%BD%D1%8B_%D0%BC%D0%B8%D1%80%D0%B0)-лидеров по активности угроз вошли [Турция](https://www.tadviser.ru/index.php/%D0%A2%D1%83%D1%80%D1%86%D0%B8%D1%8F), [Россия](https://www.tadviser.ru/index.php/%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D1%8F), [Испания](https://www.tadviser.ru/index.php/%D0%98%D1%81%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F), [Украина](https://www.tadviser.ru/index.php/%D0%A3%D0%BA%D1%80%D0%B0%D0%B8%D0%BD%D0%B0) и [Япония](https://www.tadviser.ru/index.php/%D0%AF%D0%BF%D0%BE%D0%BD%D0%B8%D1%8F).

[Банковские](https://www.tadviser.ru/index.php/%D0%91%D0%B0%D0%BD%D0%BA%D0%B8) угрозы для Android развиваются быстрее большинства [вирусного](https://www.tadviser.ru/index.php/%D0%92%D0%B8%D1%80%D1%83%D1%81) [ПО](https://www.tadviser.ru/index.php/%D0%9F%D0%9E). Более того, нежелательные программы активно распространяются через официальный магазин приложений [Google Play](https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:Google_Play): в период с сентября по декабрь 2021 года их скачали более 300 тыс. раз.

Функционал вредоносных приложений позволяет злоумышленникам красть банковские [данные](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%94%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5) пользователей и впоследствии совершать несанкционированные покупки, снятие наличных, а также переводить средства на сторонние счета.

Аналитики ESET прогнозируют, что в 2022 году [вредоносных программ](https://www.tadviser.ru/index.php/%D0%97%D0%BB%D0%BE%D0%B2%D1%80%D0%B5%D0%B4) для компрометации онлайн-банкинга станет ещё больше.

После установки [финансового](https://www.tadviser.ru/index.php/%D0%A4%D0%B8%D0%BD%D0%B0%D0%BD%D1%81%D1%8B) [приложения](https://www.tadviser.ru/index.php/%D0%9C%D0%BE%D0%B1%D0%B8%D0%BB%D1%8C%D0%BD%D0%BE%D0%B5_%D0%BF%D1%80%D0%B8%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5) изучите разрешения программы. Необходимо деактивировать функции работы поверх других открытых приложений — так вы обезопасите себя от незаметной активности онлайн-банкинга в случае его взлома. Обязательно выставляйте запрет на права администрирования устройства и отключайте разрешения на внешний доступ к [смартфону](https://www.tadviser.ru/index.php/%D0%A1%D0%BC%D0%B0%D1%80%D1%82%D1%84%D0%BE%D0%BD) или [планшету](https://www.tadviser.ru/index.php/%D0%9F%D0%BB%D0%B0%D0%BD%D1%88%D0%B5%D1%82). Эффективной мерой защиты является использование дополнительных [антивирусных](https://www.tadviser.ru/index.php/%D0%90%D0%BD%D1%82%D0%B8%D0%B2%D0%B8%D1%80%D1%83%D1%81) программ класса Mobile Security.

Треть взломов ИТ-систем российских банков происходит из-за действий сотрудников

Примерно в 30% случаев взлома ИТ-систем российских банков в 2021 году виноваты были сотрудники - они допустили [утечку данных](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A3%D1%82%D0%B5%D1%87%D0%BA%D0%B8_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85), проявили халатность или участвовали в мошеннических схемах. Такие данные в середине февраля 2022 года были обнародованы компанией [RTM Group](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:RTM_Group), предоставляющей услуги в области [информационной безопасности](https://www.tadviser.ru/index.php/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C).

На внешние [хакерские атаки](https://www.tadviser.ru/index.php/%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B8) пришлось 15% проникновений в банковские ИТ-системы в [России](https://www.tadviser.ru/index.php/%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8) по итогам 2021 года. Эта доля, по мнению экспертов, в 2022 году упадет до 3%, тогда как процент инцидентов, связанных с действиями сотрудников банков, напротив, ощутимо вырастет и достигнет 50%.

Раньше такой значительной динамики по числу инцидентов с участием внутренних инсайдеров не наблюдалось, отмечают в RTM Group, и она может быть связана с повышением сложности внешних взломов и ростом стоимости внутренних данных. Главной целью злоумышленников будут счета компаний, клиентов и любая информация о них, а также документы и внутренняя переписка, полагают аналитики.

Руководитель отдела аналитики [SearchInform](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:SearchInform_(%D0%A1%D1%91%D1%80%D1%87%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC)" \o "SearchInform (СёрчИнформ)) [Алексей Парфентьев](https://www.tadviser.ru/index.php/%D0%9F%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0:%D0%9F%D0%B0%D1%80%D1%84%D0%B5%D0%BD%D1%82%D1%8C%D0%B5%D0%B2_%D0%90%D0%BB%D0%B5%D0%BA%D1%81%D0%B5%D0%B9) в разговоре с «[Коммерсантом](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:%D0%98%D0%94_%D0%9A%D0%BE%D0%BC%D0%BC%D0%B5%D1%80%D1%81%D0%B0%D0%BD%D1%82%D1%8A)» пояснил, что злоумышленникам дешевле и безопаснее использовать инсайдеров, а не внешние схемы. Он отметил, что по закону [банки](https://www.tadviser.ru/index.php/%D0%91%D0%B0%D0%BD%D0%BA%D0%B8) не обязаны устанавливать программы для защиты от утечек данных и других инсайдерских рисков. По оценке Парфентьева, такое [ПО](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5) есть пока в трети банков.

В самих [банках](https://www.tadviser.ru/index.php/%D0%A4%D0%B8%D0%BD%D0%B0%D0%BD%D1%81%D0%BE%D0%B2%D1%8B%D0%B5_%D1%83%D1%81%D0%BB%D1%83%D0%B3%D0%B8,_%D0%B8%D0%BD%D0%B2%D0%B5%D1%81%D1%82%D0%B8%D1%86%D0%B8%D0%B8_%D0%B8_%D0%B0%D1%83%D0%B4%D0%B8%D1%82) по-разному относятся к прогнозам об усилении атак со стороны инсайдеров. В [Росбанке](https://www.tadviser.ru/index.php/%D0%A0%D0%BE%D1%81%D0%B1%D0%B0%D0%BD%D0%BA) «не ожидают роста внутренних утечек», заявил газете директор департамента информационной безопасности банка [Михаил Иванов](https://www.tadviser.ru/index.php/%D0%9F%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0:%D0%98%D0%B2%D0%B0%D0%BD%D0%BE%D0%B2_%D0%9C%D0%B8%D1%85%D0%B0%D0%B8%D0%BB.). При этом в кредитной организации ждут, что, «скорее всего, расти будут и внешние, и внутренние риски», признал он.

В каждом втором мобильном банке в России мошенники могут красть деньги

В каждом втором мобильном банке мошенники могут красть деньги, говорится в исследовании, проведённом компанией [Positive Technologies](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:Positive_Technologies" \o "Positive Technologies).

Эксперты изучили 14 популярных российских приложений для операционных систем [Android](https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:Android" \o "Android) и [iOS](https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:Apple_iOS" \o "Apple iOS), которые были загружены более 500 тыс. раз из каталогов [Google Play](https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:Google_Play) и [App Store](https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:App_Store" \o "App Store).

По итогам анализа специалисты пришли к выводу, что в 13 из 14 приложений возможен доступ к их персональным данным. 76% уязвимостей в мобильных [банках](https://www.tadviser.ru/index.php/%D0%A4%D0%B8%D0%BD%D0%B0%D0%BD%D1%81%D0%BE%D0%B2%D1%8B%D0%B5_%D1%83%D1%81%D0%BB%D1%83%D0%B3%D0%B8,_%D0%B8%D0%BD%D0%B2%D0%B5%D1%81%D1%82%D0%B8%D1%86%D0%B8%D0%B8_%D0%B8_%D0%B0%D1%83%D0%B4%D0%B8%D1%82) могут быть использованы злоумышленниками без физического доступа к устройству.

При этом каждое второе мобильное банковское приложение имеет недостаток, позволяющий мошенникам красть денежные средства. Для использования ряда уязвимостей в клиентских частях мобильных банков злоумышленнику достаточно установить на устройство жертвы [вредоносное ПО](https://www.tadviser.ru/index.php/%D0%92%D1%80%D0%B5%D0%B4%D0%BE%D0%BD%D0%BE%D1%81%D0%BD%D0%BE%D0%B5_%D0%9F%D0%9E), например, в ходе [фишинговой атаки](https://www.tadviser.ru/index.php/%D0%A4%D0%B8%D1%88%D0%B8%D0%BD%D0%B3).

Приложения, разработанные для iOS, содержали меньше уязвимостей, чем приложения для Android: так, недостатки в первых были не выше среднего уровня риска, в то время как 29% вторых содержали уязвимости высокого уровня риска (cоздателям Android-приложений предоставляется больше возможностей при разработке, объясняют такую разницу эксперты). Все они связаны с технологией deep linking, благодаря которой пользователь может перемещаться между приложениями: именно она выступает точкой входа в приложение для хакеров.

Также выяснилось, что в шести из семи веб-приложений банков содержатся уязвимости, связанные с недостаточными мерами по [аутентификации](https://www.tadviser.ru/index.php/%D0%98%D0%91_-_%D0%90%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F) пользователя. На практике недостатки мобильных приложений используются очень редко. Сегодня большинство мошеннических схем связаны с социальной инженерией, то есть психологическими методами выманивания у граждан необходимых сведений об их счетах.

ЦБ предписало банкам ускоренно перейти на отечественную криптозащиту

На состоявшемся 15 апреля 2022 года совещании [ЦБ РФ](https://www.tadviser.ru/index.php/%D0%A6%D0%91) с [банками](https://www.tadviser.ru/index.php/%D0%91%D0%B0%D0%BD%D0%BA%D0%B8) и отечественными производителями было принято решение о необходимости оперативной замены иностранных HSM-модулей на российские. Об этом пишет [«Коммерсантъ»](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:%D0%98%D0%94_%D0%9A%D0%BE%D0%BC%D0%BC%D0%B5%D1%80%D1%81%D0%B0%D0%BD%D1%82%D1%8A) со ссылкой на участников финрынка и советника CryptoPro Владимира Простова.

Аппаратный модуль безопасности (HSM) предоставляет защиту информационным системам от раскрытия данных с помощью [криптографии](https://www.tadviser.ru/index.php/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D0%B8). Выпуск модулей осуществляется в разных версиях: от простой карты расширения до отдельных устройств с антивандальной защитой. Правда, собираются они в основном из импортных деталей, по большей части китайских, а поставки из [КНР](https://www.tadviser.ru/index.php/%D0%9A%D0%B8%D1%82%D0%B0%D0%B9) к апрелю 2022 года затруднены из-за проблем с логистикой.

В публикации издания говорится, что для небольших банков замена может оказаться довольно серьезной финансовой нагрузкой, а полный переход на отечественные системы может занять практически год. По словам заместителя гендиректора [«ИнфоТеКС»](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D0%A2%D0%B5%D0%9A%D0%A1_(Infotecs)) [Дмитрия Гусева](https://www.tadviser.ru/index.php/%D0%9F%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0:%D0%93%D1%83%D1%81%D0%B5%D0%B2_%D0%94%D0%BC%D0%B8%D1%82%D1%80%D0%B8%D0%B9_%D0%9C%D0%B8%D1%85%D0%B0%D0%B9%D0%BB%D0%BE%D0%B2%D0%B8%D1%87), полный переход на отечественные HSM-модули для банков может занять несколько лет, так как необходимо не только произвести оборудование, «но и адаптировать его к работе с процессинговыми системами банков, а также поддержать российскую криптографию на конечном оборудовании: терминалах оплаты, банкоматах».

По данным собеседников издания, [Сбербанк](https://www.tadviser.ru/index.php/%D0%A1%D0%B1%D0%B5%D1%80%D0%B1%D0%B0%D0%BD%D0%BA_%D0%A0%D0%A4) и [ВТБ](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:%D0%92%D0%A2%D0%91_-_%D0%92%D0%BD%D0%B5%D1%88%D1%82%D0%BE%D1%80%D0%B3%D0%B1%D0%B0%D0%BD%D0%BA) будут менять модули самостоятельно, остальные банки — через вендоров. Всего в [России](https://www.tadviser.ru/index.php/%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D1%8F) нужно заменить несколько тысяч модулей. Стоимость таких устройств начинается от 3 млн [рублей](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%80%D1%83%D0%B1%D0%BB%D1%8C) за штуку для неплатежных модулей, тогда как платежные могут стоить в разы дороже.

Опрошенные газетой участники рынка считают, что ЦБ необходимо разработать отечественный аналог международному стандарту [PCI DSS](https://www.tadviser.ru/index.php/PCI_DSS) (комплексный стандарт безопасности платежных систем), так как получить сертификат отечественным вендорам в силу геополитических ограничений невозможно, даже при соответствии требованиям, при этом банки без такого сертификата обычно не хотят использовать оборудование от отечественных вендоров.