



**Уральский
федеральный
университет**

имени первого Президента
России Б.Н.Ельцина

**Институт экономики
и управления**



**Ural Federal
University**

named after the first President
of Russia B.N.Yeltsin

УРАЛЬСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ
имени первого Президента России Б.Н.Ельцина

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ В «СБЕРБАНК РОССИИ»

Сероусова
Мезенина
Демидова
Носкова
Зайцев



Общая характеристика Сбербанк

ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО «СБЕРБАНК»

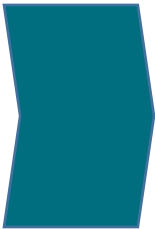
— российский государственный финансовый конгломерат, крупнейший транснациональный и универсальный банк Российской Федерации — России, Центральной и Восточной Европы.



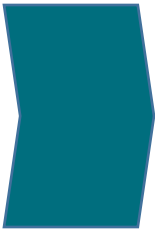
СБЕРБАНК

- Клиентами Сбербанка РФ по состоянию на 2019 год являются **110 млн физических лиц и более 1 млн предприятий**.
- В 2018 году ценность бренда «Сбербанка России» составила **670,4 млрд рублей** (самый дорогой бренд России).

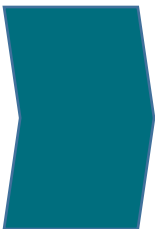
Общая характеристика Сбербанк



Доля Правительства России в уставном капитале ПАО Сбербанк 52,32 % голосующих акций.



Остальными акционерами «Сбербанка» являются более 8273 юридических и физических лиц.



Доля физических лиц в уставном капитале банка составляет около 2,84 %, а доля иностранных инвесторов — более 45 %.

Общая характеристика Сбербанк

Председатели правления Сбербанка России

- Жихарев, Павел Иванович (март 1991 — март 1993)
- Яшин, Олег Владимирович (март 1993 — январь 1996)
- Казьмин, Андрей Ильич (январь 1996 — ноября 2007)
- Греф, Герман Оскарлович (с ноября 2007 года)



Сбербанк



Общая характеристика Сбербанк



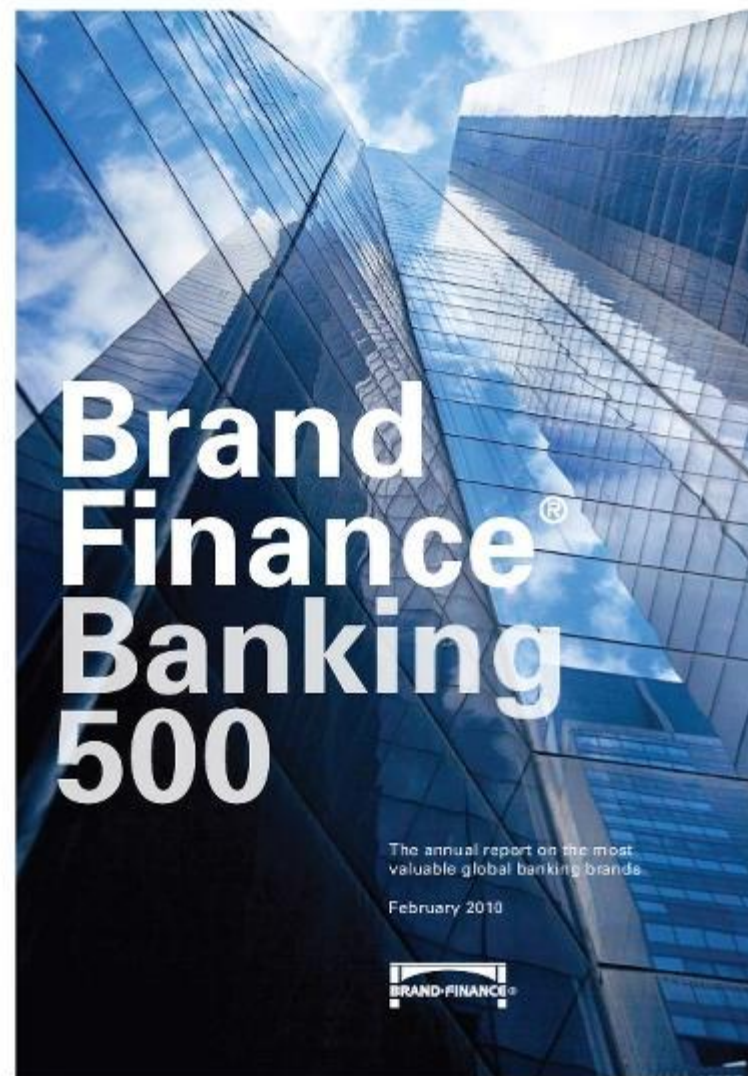


Общая характеристика Сбербанк

В июле 2019 года Сбербанк возглавил список самых дорогих брендов России по версии Brand Finance.

Его стоимость за год выросла на 25,6 % и составила 842,1 млрд рублей.

Сбербанк возглавляет данный рейтинг с 2017 года, опережая компании нефтегазового сектора.





SWOT Анализ

<p><u>S (STRENGTHS – СИЛЬНЫЕ СТОРОНЫ)</u></p> <ol style="list-style-type: none">1. Репутация банка2. Филиалы по всей стране3. Выход в другие страны Центральной и Восточной Европы4. Высококвалифицированные и опытные работники.	<p><u>W (WEAKNESSES – СЛАБЫЕ СТОРОНЫ)</u></p> <ol style="list-style-type: none">1. Невозможность принятия оперативных решений в филиалах.2. Большие комиссии3. Сложное взаимодействие системы «Банк-Клиент».
<p><u>O (OPPORTUNITIES – ВОЗМОЖНОСТИ)</u></p> <ol style="list-style-type: none">1. Расширение международных сетей2. Расширение рынка кредитования малообеспеченным слоям населения3. Создание более удобных приложений для мобильных телефонов и планшетов,4. Сохранение небольших процентных ставок по ипотеке	<p><u>T (THREATS – УГРОЗЫ)</u></p> <ol style="list-style-type: none">1. Экономический кризис в России2. Сокращение рентабельности операций.3. Мировой финансовый кризис4. Усиление конкуренции на российском финансовом рынке

Нормативно-правовая основа

Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ

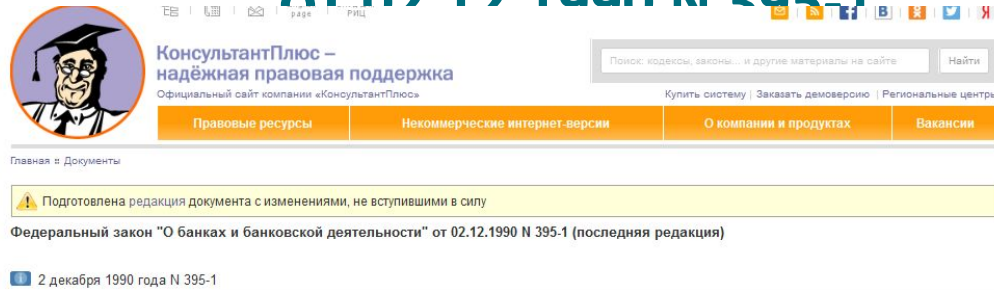
Статья 16. Защита информации

1. Защита информации представляет собой комплекс организационных и технических мер, направленных на:
- 1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
 - 2) соблюдение конфиденциальности информации ограниченного доступа;
 - 3) реализацию права на доступ к информации.
2. Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.
3. Требования о защите общедоступной информации могут устанавливаться только для достижения целей, указанных в пунктах 1 и 3 части 1 настоящей статьи.
4. Владелец информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:
- 1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
 - 2) своевременное обнаружение фактов несанкционированного доступа к информации;
 - 3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
 - 4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
 - 5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
 - 6) постоянный контроль за обеспечением уровня защищенности информации;
 - 7) нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации.
- (п. 7 введен Федеральным законом от 21.07.2014 N 242-ФЗ)
5. Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.
6. Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

Нормативно-правовая основа

Федеральный закон "О банках и банковской деятельности"

от 02.12.1990 N 395-1



The screenshot shows the website of Consultant Plus. At the top, there is a search bar with the text "Поиск: кодексы, законы... и другие материалы на сайте" and a "Найти" button. Below the search bar, there are navigation links: "Правовые ресурсы", "Некоммерческие интернет-версии", "О компании и продуктах", and "Вакансии". A yellow warning banner indicates: "Подготовлена редакция документа с изменениями, не вступившими в силу". Below this, the title of the law is displayed: "Федеральный закон 'О банках и банковской деятельности' от 02.12.1990 N 395-1 (последняя редакция)". The date "2 декабря 1990 года N 395-1" is also visible.

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О БАНКАХ И БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ

[Список изменяющих документов](#)

(см. Обзор изменений данного документа)

• Глава I. Общие положения

- Статья 1. Основные понятия настоящего Федерального закона
- Статья 2. Банковская система Российской Федерации и правовое регулирование банковской деятельности
- Статья 3. Союзы и ассоциации кредитных организаций
- Статья 4. Банковская группа и банковский холдинг
- Статья 5. Банковские операции и другие сделки кредитной организации
- Статья 5.1. Особенности осуществления банком с базовой лицензией банковских операций и сделок
- Статья 6. Деятельность кредитной организации на рынке ценных бумаг
- Статья 7. Фирменное наименование кредитной организации
- Статья 8. Раскрытие информации об органах управления кредитной организации и о деятельности кредитной организации, банковской группы и банковского холдинга
- Статья 9. Отношения между кредитной организацией и государством
- Статья 10. Учредительные документы кредитной организации
- Статья 11. Уставный капитал кредитной организации
- Статья 11.1. Органы управления кредитной организации
- Статья 11.1-1. Особенности компетенции и организации деятельности совета директоров (наблюдательного совета) кредитной организации
- Статья 11.1-2. Требования к системам управления рисками и капиталом, внутреннего контроля кредитной организации

Нормативно-правовая основа

Раскрытие информации и конфиденциальность



Информационная политика

https://www.sberbank.com/common/img/uploaded/files/pdf/normative_docs/informatsionnaya_politika_rus.pdf



Соглашение о конфиденциальности

https://www.sberbank.com/common/img/uploaded/files/pdf/normative_docs/confidentiality_agreement.pdf



Договор о нераспространении информации (Соглашение о конфиденциальности)



Политика обработки персональных данных



1. Общие положения	4
2. Цели и задачи Информационной политики	5
3. Основные принципы Информационной политики	6
4. Раскрытие информации	7
4.1. Раскрытие информации о финансовой деятельности Банка по РПБУ	7
4.2. Раскрытие информации о финансовой деятельности Банка по МСФО	8
4.3. Информация, раскрываемая Банком как кредитной организацией	8
4.4. Раскрытие информации о принимаемых рисках, процедурах их оценки, процедурах управления рисками и капиталом	9
4.5. Информация, раскрываемая Банком как эмитентом ценных бумаг	9
4.6. Информация, раскрываемая Банком как профессиональным участником рынка ценных бумаг	10
4.7. Предоставление информации акционерам при подготовке к общему собранию акционеров	11
4.8. Предоставление доступа к информации по требованию акционеров и иных правомочных лиц	12
4.9. Раскрытие информации в соответствии с требованиями иностранных регуляторов рынка ценных бумаг и иностранных бирж, на которых осуществляется обращение депозитарных расписок	14
4.10. Раскрытие информации о системе корпоративного управления Банка	15
4.11. Состав информации, добровольно (дополнительно) раскрываемой Банком, и способы ее раскрытия	15
5. Коммуникации	16
5.1. Лица, имеющие право раскрывать информацию от имени Банка	16
5.2. Коммуникации с акционерами, инвесторами, аналитиками	17
5.3. Коммуникации с сотрудниками	18
5.4. Взаимодействие со СМИ	19
5.5. Присутствие Банка в социальных медиа	19
6. Инсайдерская информация	20
7. Конфиденциальная информация	20
8. Раскрытие существенной информации	21
9. Ответственность за раскрытие информации	22
10. Контроль за соблюдением Информационной политики	22

ИНФОРМАЦИОННАЯ ПОЛИТИКА ПАО СБЕРБАНК

2.2. Информационная политика направлена на решение следующих основных задач:

- повышение уровня открытости и доверия в отношениях Банка с различными целевыми аудиториями (акционерами, клиентами и другими заинтересованными лицами);
- поддержание профессиональных и доверительных отношений со средствами массовой информации (далее – СМИ), основанных на свободном обмене достоверной информацией;
- улучшение и/или расширение существующих каналов коммуникаций для более полного информирования акционеров, клиентов и иных заинтересованных лиц;
- защита информации о Банке, разглашение и/или использование которой может нанести ущерб интересам Банка, его акционерам, клиентам и контрагентам, или повлечь преимущества одних заинтересованных лиц перед другими.

ИНФОРМАЦИОННАЯ ПОЛИТИКА ПАО СБЕРБАНК

7.2. Банк принимает меры к **охране** конфиденциальной информации и поддержанию режима ее неразглашения:

- работа с конфиденциальной информацией осуществляется строго в соответствии с требованиями законодательства Российской Федерации и внутренних документов Банка;
- передача (предоставление, доступ) персональных данных третьим лицам осуществляется в соответствии с требованиями законодательства Российской Федерации;
- работники Банка, вступая в трудовые отношения с Банком, принимают на себя обязательство о неразглашении конфиденциальной информации Банка;
- работникам Банка запрещается сообщать кому-либо личные пароли доступа в корпоративную информационную сеть, программы и рабочие файлы;
- члены Наблюдательного совета обязаны не разглашать и не использовать в личных интересах или в интересах третьих лиц, ставшие им известными сведения, составляющие конфиденциальную информацию Банка;
- разглашение конфиденциальной информации влечет за собой наступление ответственности в соответствии с правилами внутреннего трудового распорядка Банка или законодательством Российской Федерации.

ИНФОРМАЦИОННАЯ ПОЛИТИКА ПАО СБЕРБАНК

3. Обязательства по сохранению конфиденциальной информации

3.1. Получающая сторона обязана постоянно сохранять в тайне, не раскрывать и не разглашать конфиденциальную информацию, принять для обеспечения сохранности конфиденциальной информации Передающей стороны меры, не меньшие, чем те, которые Получающая сторона принимает для обеспечения сохранности своей собственной конфиденциальной информации, а именно:

3.1.1. Обеспечить хранение полученной конфиденциальной информации в условиях строгой и полной секретности, исключая несанкционированный доступ к ней третьих лиц;

3.1.2. Не раскрывать, не копировать конфиденциальную информацию, не предоставлять доступ к ней как в целом, так и в части, любым третьим лицам, а также препятствовать возможной несанкционированной передаче;

3.1.3. Не делать никаких официальных объявлений, публикаций, а также заявлений третьим лицам в отношении каких-либо выводов, сделанных на основе полученной конфиденциальной информации.

3.2. Ни одна из Сторон не будет разглашать факт существования Соглашения без предварительного согласия другой Стороны.

3.3. При обнаружении фактов разглашения конфиденциальной информации третьим лицам Получающая сторона незамедлительно должна проинформировать Передающую сторону о данных фактах и предпринятых мерах по уменьшению ущерба.

ИНФОРМАЦИОННАЯ ПОЛИТИКА ПАО СБЕРБАНК

5. Ответственность

5.1. Получающая сторона, не исполнившая свои обязательства по Соглашению, обязана возместить Передающей стороне убытки, причиненные разглашением или неправомерным использованием конфиденциальной информации. Убытки возмещаются в соответствии с законодательством Российской Федерации.

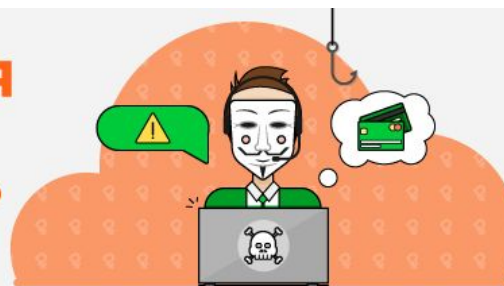


«МОШЕННИЧЕСТВО В БАНКОВСКОЙ СФЕРЕ»



«МОШЕННИЧЕСТВО В БАНКОВСКОЙ СФЕРЕ»

Ситуация 1. «Звонок из службы безопасности банка»

**КАК УБЕРЕЧЬСЯ
ОТ АТАК
МОШЕННИКОВ?**

Чтобы не попадать в неприятные ситуации, всегда придерживайтесь простых правил безопасности:



Запишите номера своего банка в телефонную книгу телефона. Даже если мошенники попытаются использовать при разговоре похожие номера, они все равно отобразятся на экране, как неизвестные.



Не нужно следовать инструкциям неизвестных лиц, особенно, если они касаются ваших счетов, банковских кабинетов и т.д.



Завершайте разговор немедленно, если на том конце провода у вас выпрашивают данные по карте, либо информацию из SMS по операциям на счете



Всегда проверяйте свои счета, баланс карты, чтобы держать ситуацию с деньгами под контролем



«МОШЕННИЧЕСТВО В БАНКОВСКОЙ СФЕРЕ»

Ситуация 2. «Перевод по ошибке»



(4)

+7 (900) 556-92-31

Контакт

Сообщение
Вт, 12 мая, 22:23

Зачислен платеж
150.00руб через
Мобильный платеж
системы оплаты QIWI.

Ср, 13 мая, 8:45

По ошибке положила
вам 150р.Прошу верните
дочке на Билайн
[89607386085](tel:89607386085)





«МОШЕННИЧЕСТВО В БАНКОВСКОЙ СФЕРЕ»

Ситуация 3. «Опрос от Сбербанка»

Опросы Сбербанка с номера 9000

Наша ссылка
в SMS безопасна



Екатерина
13.11.2018

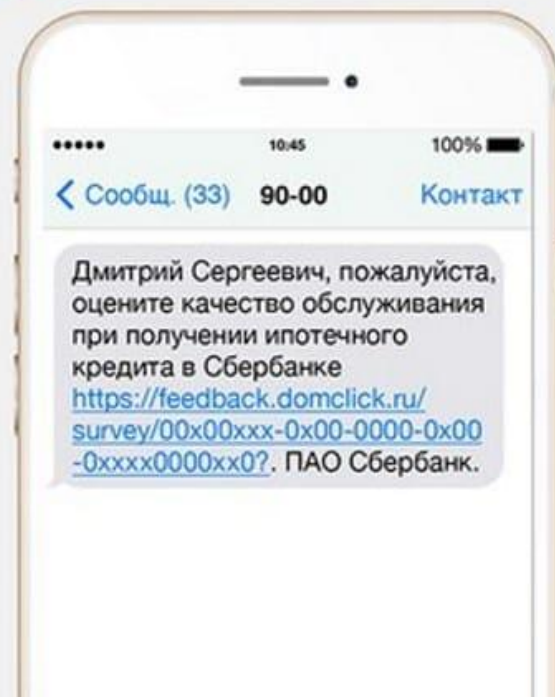


ПРОХОДИ ОПРОС от *СБЕРБАНКА* и
ПОЛУЧИ ВЫПЛАТУ от 15 тыс. до 140
тыс. руб! *СПЕШИ!* [http://sberbank-
opros.com/sberbank](http://sberbank-opros.com/sberbank). Добрый день. Это
ваш опрос?

✓ 17:49



Сбербанк





СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ ПО ОТРАСЛЯМ

- **Экономическая**
- **Информационная**
- **Защита средств на банковских картах**
- **Организация обработки и защита персональных данных**

Экономическая безопасность

За отчетный период предотвращено **325** попыток использования поддельных документов, удостоверяющих личность (годом ранее предотвращено 100 прецедентов)

- В Сбербанке внедрена система мониторинга, выявляющая факт внесения в устройство самообслуживания суррогатных купюр. При активном содействии подразделений экономической безопасности сотрудниками полиции задержано **16 лиц**, причастных к такому правонарушению.
- Сбербанк содействует внесению изменений в законодательство, предусматривающих введение уголовной ответственности за незаконный оборот составных и суррогатных купюр путем включения в УК РФ новой **статьи 186.1**.
- В рамках фрод-процедуры «Красная кнопка – Ар» предотвращена выдача кредитов корпоративным клиентам по поддельным документам на сумму **10.3 млрд рублей**.



Информационная безопасность

За 2018 год было пресечено более 300 тыс. попыток хищения средств физических и юридических лиц, предотвращен ущерб на сумму более 40 млрд руб.



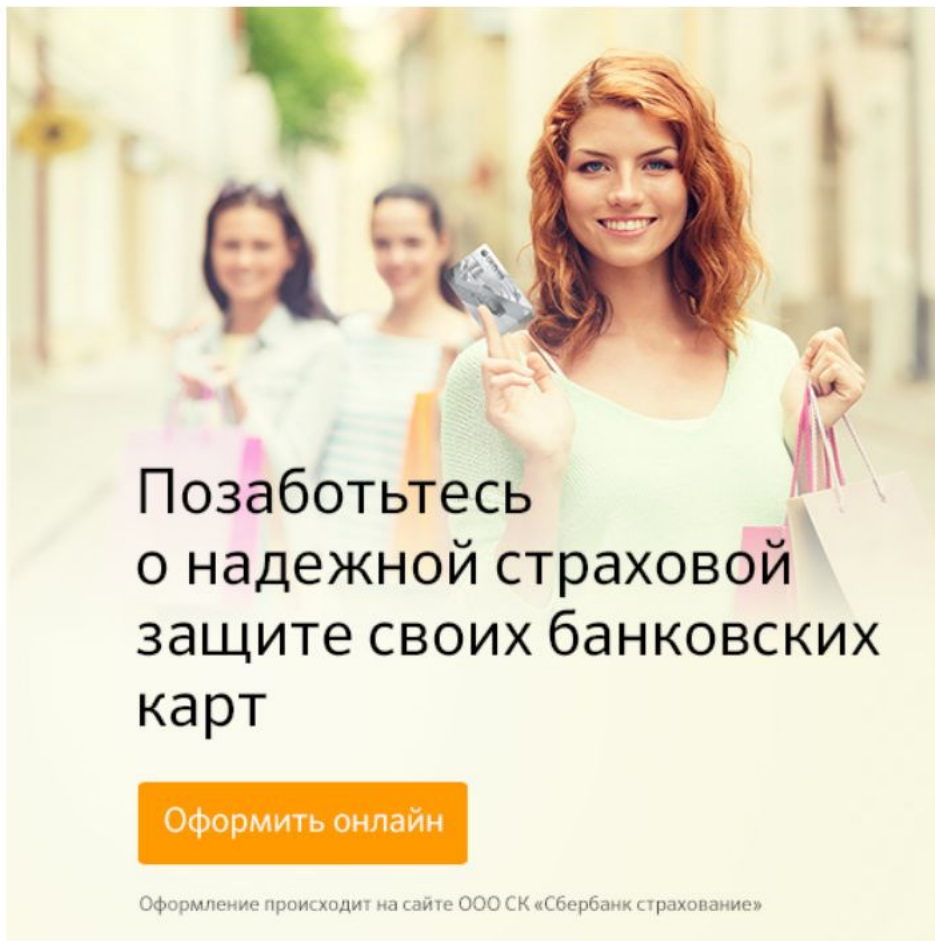
Проект Сбербанка «Фрод-мониторинг для удаленных каналов обслуживания физических лиц» стал бронзовым призером международного конкурса IPMA International Project Excellence Award 2017.



Защита средств на банковских картах

Оформить онлайн

Оформить в отделении



Позаботьтесь
о надежной страховой
защите своих банковских
карт

Оформить онлайн

Оформление происходит на сайте ООО СК «Сбербанк страхование»

Удобно

Вы просто выбираете подходящую
вам сумму страховой защиты



Быстро и выгодно

Экономия до 15% за бонусы
СПАСИБО



Все карты «под замком»

Одним полисом надежно
застрахованы все карты,
привязанные к вашему счету в
Сбербанке



Защита средств на банковских картах



Хотите быть уверенными в сохранности своих денег и защитить их от злоумышленников? С полисом «Защита карт» вы сможете спокойно совершать покупки и расплачиваться дебетовыми и кредитными картами по всему миру — в интернете, в магазинах, ресторанах и других местах.

Сумма страховой защиты и стоимость полиса в рублях

	Вариант 1*	Вариант 2	Вариант 3	Вариант 4
Общая сумма страховой защиты	60 000	120 000	250 000	350 000
Стоимость полиса на 1 год	1 161	1 710	3 510	5 310

Защита средств на банковских картах

Как оформить полис

- 1 Перейдите на страницу оформления и выберите сумму страховой защиты.
- 2 Укажите паспортные данные, адрес и контактную информацию.
- 3 Получите полис на e-mail.
- 4 Оплатите полис банковской картой.

Электронный полис равнозначен бумажному и имеет такую же юридическую силу. Преимущества электронного полиса состоят в удобстве его оформления, получения и хранения..

Срок страхования

15
дней

Полис вступает в силу на 15-й день после оплаты

1
год

Срок действия полиса после вступления его в силу

Этот продукт прежде всего для людей, которые активно пользуются банковской картой – снимают денежные средства в банкоматах, используют её для оплаты счета в кафе и ресторанах, интернете (например, коммунальные платежи)

Организация обработки и защита персональных

данных

В СОСТАВ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ВХОДЯТ:

- обеспечение контролируемой зоны, в пределах которой осуществляется функционирование автоматизированных систем Сбербанка;
- защита машинных носителей информации
- антивирусная защита;
- обнаружение и предотвращение вторжений;
- контроль и анализ защищенности персональных данных;
- обеспечение целостности автоматизированных систем Сбербанка и персональных данных;
- обеспечение доступности персональных данных;
- защита среды виртуализации;
- защита технических средств;
- защита автоматизированных систем, их средств, систем связи и передачи данных;
- выявление инцидентов



РЕКОМЕНДАЦИИ

Для защиты информации конфиденциального характера можно посоветовать определить возможных внутренних нарушителей и актуальных угроз, связанных с их действиями.

А - работники банковской сферы, обладающие доступом к информации конфиденциального характера в рамках реализации своих служебных обязанностей

Б – эксплуатационный персонал

В – технический и вспомогательный персонал

Г – лица, не являющиеся работниками банковской системы

		Вероятность угрозы	
		Высокая	Низкая
Угроза	Высокая	1	2
	Низкая	3	4

РЕКОМЕНДАЦИИ

- "ИНФОРМАЦИЯ КОНФИДЕНЦИАЛЬНОГО
- ХАРАКТЕРА" "ОТКРЫТАЯ ИНФОРМАЦИЯ"





РЕКОМЕНДАЦИИ

РЕКОМЕНДАЦИИ КЛИЕНТАМ БАНКА

по соблюдению мер информационной безопасности при использовании системы обмена электронными документами (для размещения на сайте Банка)

<http://www.capitalkredit.ru/media/5a82db30c96a7.pdf>





РЕКОМЕНДАЦИИ

1. Общие положения

- 1.1. Задачи защиты информации сводятся к минимизации ущерба и предотвращению воздействий со стороны злоумышленников. Для обеспечения надлежащей степени защищенности должен быть обеспечен комплексный подход, когда вопросам информационной безопасности уделяется достаточно внимания, как на стороне Банка, так и на стороне клиента.
- 1.2. Наиболее опасным является кража и их незаконное использование для клиента. Оптимальный способ распознавать способы этих злоумышленников.
- 1.3. Риски получения несанкционированных переводов денежных средств (использованием «фишингом») (использованием денежных средствами), а также во «фишинг» – попытка перехвата способов фишинга заключается в выдаются себя за представителей извощенников содержится ссылка на предлагается ввести свои личные безопасен, тогда как в действительности.
- 1.5. Антивирусная защита осуществляется персональных компьютерах, с которых вирусов и программ, направленных модификацию программного обеспечения паролей.
- 1.6. Средства и методы защиты информации необходимый уровень безопасности предотвратить мошеннический выполнения клиентами рекомендаций, изложенных в данном документе.

2. Рекомендации по защите информации от воздействия вредоносного кода.

- 2.1. При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.
- 2.2. Пользуйтесь персональными компьютерами с установленным лицензионным программным обеспечением.

3. Рекомендации по защите информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети Интернет

- 3.1. Мошеннический или поддельный web-сайт – это небезопасный web-сайт, на котором Вам предоставляется ввести конфиденциальную информацию. Зачастую web-сайтов известных компаний, которым Вы доверены для сбора конфиденциальной информации фальсифицированных WEB-сайтов – их доменные адреса содержат сайты Банка и содержат ложные банковские реквизиты, вступление в какие-либо деловые отношения с использованием подобных реквизитов, рискованно действиям. Ввод логина и пароля на таком сайте может быть использовано злоумышленниками, т.е. разглашению информации на сайты, визуально напоминающие сайт СДБО, для получения информации. В случае обнаружения несоответствия дизайна официального сайта или ДБО, сообщите об этом по контактным телефонам Банка. Не используйте фальсифицированных) ресурсов и программного интерфейса используемой Банком в системе ДБО, и (или) использующих зарегистрированные товарные знаки и наименование Банка, необходимо удостовериться, чтобы при подключении к СДБО защищенное SSL-соединение было установлено исключительно с официальным сайтом ДБО. Прежде чем ввести логин и пароль, Клиентам необходимо проверить по информации из SSL-сертификата подлинность сайта. Работу с ДБО рекомендуется осуществлять с использованием технических средств с индивидуальными дистанционно распознаваемыми идентификационными признаками (Приложение А), предоставленными в Банк;

1. Общие положения
2. Рекомендации по защите информации от воздействия вредоносного кода.
3. Рекомендации по защите информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети Интернет
4. Рекомендации по предотвращению получения несанкционированного доступа третьими лицами
5. Рекомендации по безопасности при использовании мобильных устройств для доступа к дистанционному банковскому обслуживанию.

РЕКОМЕНДАЦИИ

Регулярный **внутренний аудит информационной безопасности**, проводимый сотрудниками ревизионных структур Банка России и коммерческих банков, усиливает контроль за функционированием разных аспектов обеспечения информационной безопасности и регламентируется их внутренними документами.



РЕКОМЕНДАЦИИ

Оценка и проверка деятельности по обеспечению информационной безопасности — это элемент управления информационной безопасностью, который нужен для того, чтобы выявить признаки ухудшения используемых в организации защитных мер.

ДЛЯ ЭТОГО НЕОБХОДИМЫ:

- мониторинг информационной безопасности и контроль за используемыми защитными мерами;
- самооценка информационной безопасности (в пределах заданного интервала времени с программой и планом проведения);
- внутренний и внешний аудит функционирования системы управления информационной безопасностью (с заданной периодичностью)



РЕКОМЕНДАЦИИ

СТРАХОВАНИЕ КИБЕР-РИСКОВ ИЛИ УМНОЕ СТРАХОВАНИЕ

Умное страхование предусматривает страхование убытков от перерыва в хозяйственной деятельности и от несанкционированного списания денег со счета клиента в результате киберинцидента, а также страхование гражданской ответственности за вред, который может быть причинен третьим лицам, в результате киберинцидента.











ВЫВОД

При подготовке указанных рекомендаций были учтены лучшие практики российских кредитных организаций в этой сфере.

Мы считаем, что предлагаемая схема позволит рационально распределить усилия банка по организации информационной безопасности и, как следствие, повысить эффективность работы по информационной защите.

Топ 10 банков по надёжности

[ТОП 10](#)
[ТОП 20](#)
[ТОП 30](#)
[ТОП 40](#)
[ТОП 50](#)
[ТОП 100](#)

Рейтинг	Банк	Веб-сайт	Отзывы	Продукты	Филиалы
1	 Сбербанк Лицензия №1481	sberbank.ru	227 Отзывов ★ ★ ★ ★ ★	Кредиты ²⁴ Вклады ¹⁷	Отделения ⁶⁷²⁶ Банкоматы ²⁶⁰⁶¹
2	 Банк ВТБ Лицензия №1000	vtb.ru	151 Отзыв ★ ★ ★ ★ ★	Кредиты ⁴³ Вклады ⁸	Отделения ¹³⁷⁹ Банкоматы ⁸⁰⁸³
3	 Газпромбанк Лицензия №354	gazprombank.ru	74 Отзыва ★ ★ ★ ★ ★	Кредиты ¹² Вклады ¹⁶	Отделения ³⁸³ Банкоматы ³⁶⁶⁰
4 ⁻¹	 Национальный Клиринговый Центр Лицензия №3466	nationalclearingcentre.ru	Добавить отзыв		Отделения ¹
5 ⁻¹	 Альфа-Банк Лицензия №1326	alfabank.ru	122 Отзыва ★ ★ ★ ★ ★	Кредиты ⁹ Вклады ⁵	Отделения ⁶⁷³ Банкоматы ¹⁶²⁷
6	 Россельхозбанк Лицензия №3349	rshb.ru	56 Отзывов ★ ★ ★ ★ ★	Кредиты ³⁵ Вклады ¹⁴	Отделения ¹²⁷⁷ Банкоматы ³¹⁷⁸
7	 Банк «Открытие» Лицензия №2209	open.ru	216 Отзывов ★ ★ ★ ★ ★	Кредиты ¹⁶ Вклады ⁷	Отделения ⁷⁴⁴ Банкоматы ²⁸⁴⁶
8	 Московский Кредитный Банк Лицензия №1978	mkb.ru	22 Отзыва ★ ★ ★ ★ ★	Кредиты ¹⁰ Вклады ⁸	Отделения ¹⁵⁰ Банкоматы ⁸⁵³
9 ⁻¹	 ЮниКредит Банк Лицензия №1	unicreditbank.ru	10 Отзывов ★ ★ ★ ★ ★	Кредиты ¹⁹ Вклады ⁵	Отделения ⁹¹ Банкоматы ³⁶⁸
10 ⁻³	 Райффайзенбанк Лицензия №3292	raiffeisen.ru	36 Отзывов ★ ★ ★ ★ ★	Кредиты ¹⁶ Вклады ⁵	Отделения ¹⁷⁷ Банкоматы ¹³⁵⁶

место	название банка лицензия №, Регион	показатель, тыс. рублей		изменение	
		Март, 2020	Февраль, 2020	тыс. рублей	%
1	Сбербанк России лицензия № 1481, Москва и обл.	29 276 869 089	28 956 284 893	+320 584 196	+1,11%
2	ВТБ лицензия № 1000, Санкт-Петербург и обл.	14 115 988 836	14 121 403 057	-5 414 221	-0,04%
3	Газпромбанк лицензия № 354, Москва и обл.	6 700 683 954	6 651 137 698	+49 546 256	+0,74%
4 ⁺¹	Национальный Клиринговый Центр лицензия № 3466, Москва и обл.	3 941 010 034	3 714 752 967	+226 257 067	+6,09%
5 ⁻¹	Альфа-Банк лицензия № 1326, Москва и обл.	3 827 665 260	3 761 502 037	+66 163 223	+1,76%
6	Россельхозбанк лицензия № 3349, Москва и обл.	3 456 650 842	3 409 864 634	+46 786 208	+1,37%