SBERBANK
CYBER SECURITY TEAM
SECURITY DEPARTMENT
SCST

Развитие системы законодательного обеспечения информационной безопасности на национальном и международном уровнях

I Международная конференция по информационной безопасности **«Инфофорум-Югра»**

Ханты-Мансийск
июнь 2017

Содержание

Актуальные направления в сфере информационной безопасности в части оптимизации регулирования

Законодательство РФ в сфере обработки и обмена банковской тайной	Предоставление банкам инициативного права передачи сведений, составляющих банковскую тайну в ПОО, субъектам ОРД, CERT, сообществу
Законодательство в сфере международного сотрудничества и обмена информацией об инцидентах ИБ и фактах совершенных киберпреступлений	Координация действий между международными и национальными, государственными и коммерческими CERT
Уголовное и уголовно-процессуальное законодательство РФ	Проект ФЗ №47571-7 «О безопасности критической информационной инфраструктуры» Законопроект № 186266-7 "О внесении изменений в УК РФ в части усиления ответственности за хищение ДС с банковского счета..."
Стандартизация и гармонизация международных и национальных законодательных актов	Ратификация Россией Конвенции (2001г) Совета Европы о кибербезопасности или продвижение альтернативной Конвенции по противодействию преступлениям в сфере ИКТ (*)
Законодательство РФ в сфере обработки и защиты персональных данных	Легализация обмена ПДн о кибер преступниках Вывод из под регулирования «технологических» ПДн
GDPR - Регламент ЕС о защите персональных данных 2016/679	Гармонизация положений GDPR 2016/679 и ФЗ-152

(*) проект был представлен в июле 2016г в СПб на XV Совещании руководителей спецслужб государств-партнеров ФСБ РФ

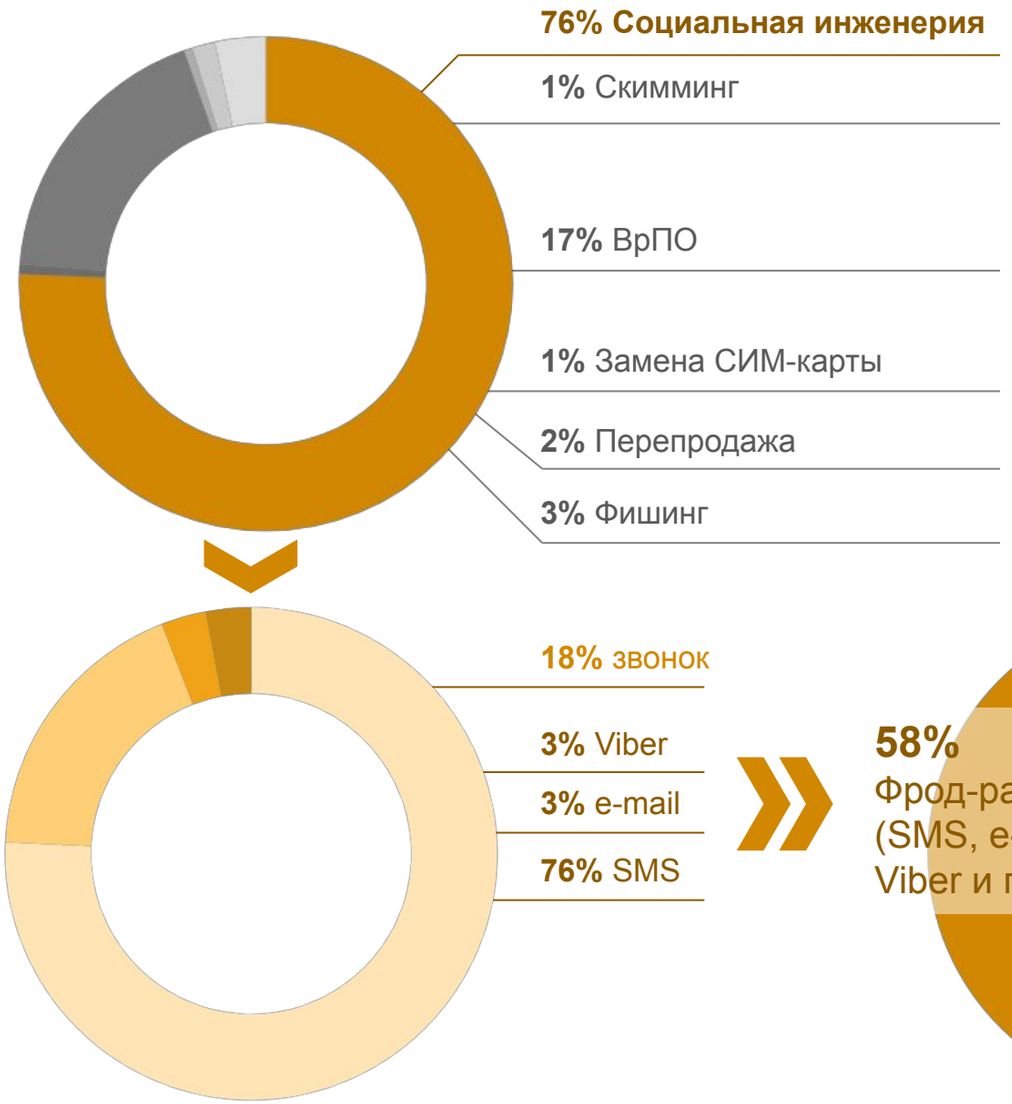
SCST

Текущая ситуация с регулированием в сфере информационной безопасности банковской системы РФ

GDPR – Регламент ЕС о защите персональных данных 2016/679 от 27 апреля 2016 г, отменяет Директиву ЕС о защите персональных данных 95/46/ЕС от 1995г с 01.01.2018 г

ФЗ РФ обязательны к исполнению, как и НПА/ОРД регуляторов, стандарты – «де юре» носят рекомендательный характер, «де факто» – императивный по требованиям МПС VISA/MC

Фактическая структура способов реализации кибератак на клиентов Сбербанка и корневые причины успеха злоумышленников



Корневые причины:

- Низкий уровень осведомленности клиентов в вопросах ИБ
- Простота и доступность реализации фрод-рассылок на клиентов Банка при их дешевизне для мошенников
- Массовость проникновения услуг Банка среди населения РФ
- Мошенничество в «промышленном масштабе» на потоке: ОПГ, мошеннические КоллЦентры, бизнес в «зонах»
- Безнаказанность злоумышленников из-за бюрократичности уголовно-процессуального законодательства при возрастающей технологичности реализации киберпреступлений

Текущее регулирование в уголовном законодательстве РФ в сфере противодействия киберпреступлениям

Ст.УК	Определение	Ущерб	Сроки наказания
272	Неправомерный доступ к компьютерной информации	Крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает 1 млн. руб.	Максимальный срок наказания – до 7 лет
273	Создание, использование и распространение вредоносных компьютерных программ		
274	Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и инфо-телеком сетей		Максимальный срок наказания – до 5 лет
183	Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую и банковскую тайну	Крупный ущерб > 2,25 млн рублей Особо крупный > 9 миллиона рублей	Максимальный срок наказания – до 7 лет при тяжких последствиях или 5 лет или штраф до 1,5 млн рублей в случае крупного ущерба
158	Кража	Крупный ущерб > 250 тысяч рублей Особо крупный > 1 миллиона рублей	Максимальный срок наказания – до 10 лет со штрафом в размере до 1 миллиона рублей
159.1	Мошенничество в сфере кредитования	Крупный ущерб > 1,5 млн. рублей Особо крупный > 6 миллиона рублей	Максимальный срок наказания – до 10 лет лишения свободы
159.2	Мошенничество при получении выплат	Крупный ущерб > 250 тысяч рублей Особо крупный > 1 миллиона рублей	Максимальный срок наказания – до 10 лет лишения свободы
159.3	Мошенничество с использованием платежных карт	крупный ущерб > 1,5 млн. рублей Особо крупный > 6 миллиона рублей	Максимальный срок наказания – до 10 лет лишения свободы
159.4	Мошенничество в сфере предпринимательской деятельности – утратила силу		
159.5	Мошенничество в сфере страхования	крупный ущерб > 1,5 млн. рублей Особо крупный > 6 миллиона рублей	Максимальный срок наказания – до 10 лет лишения свободы
159.6	Мошенничество в сфере компьютерной информации	крупный ущерб > 1,5 млн. рублей Особо крупный > 6 миллиона рублей	Максимальный срок наказания – до 10 лет лишения свободы

По данным аналитического обзора Следственного Департамента МВД за 2016г по уголовным делам, связанным с киберпреступлениями в РФ, **75% были приостановлено** за не установлением лица, подлежащего привлечению к уголовной ответственности в качестве обвиняемого, только **7% дел было направлено в суд**.

SCST

Существующие проблемы в уголовном законодательстве РФ

1	Недостаточная эффективность действующего законодательства РФ в отношении противодействия кибермошенничеству. Статья 273 УК РФ на сегодняшний день не предполагает возможности привлечения к уголовной ответственности лиц за приобретение, посредническую деятельность по приобретению вирусной программы и её дальнейшему хранению, распространению
2	Уголовная ответственность за мошенничество по ст. 159.6 УК РФ наступает в случае, если преступлением причинен имущественный вред потерпевшему (обязательное условие). В отсутствие вреда, чаще всего содеянное квалифицируется по ст.272 УК РФ (максимальный срок наказания до 7 лет лишения свободы), что по своей суровости не соответствует уровню опасности деяния и тяжести последствий по данному виду преступлений.
3	Ответственность по статье «Покушение» не работает, т.к. если атака предотвращена - ущерба нет, ни клиент, ни банк не могут заявить об этом деянии в МВД.
4	Возбуждение УД по факту хищений денежных средств преимущественно возбуждаются по месту нахождения счетов мошенника, а не по месту нахождения кредитной организации или физ.лица, являющегося потерпевшим.
5	В случае возмещения средств клиенту Банком, организация автоматически не приобретает статус потерпевшей стороны и права требования компенсации убытков, при этом, у клиента исчезает мотивация в обращаться в правоохранительные органы.
6	В уголовном законодательстве ряда западных стран подробно описаны механизмы совершения преступления, а не набор признаков, как в УК РФ.

Предложения и инициативы Сбербанка направленные на повышение эффективности регулирования в уголовном и уголовно-процессуальном законодательстве РФ (до 2017)

1. **Введение в ст.158 УК РФ нового вида хищения - «кража с банковского счета или электронных денежных средств»**. Инициатива должна упростить возбуждение уголовных дел по заявлениям граждан по фактам кибермошенничества.

2. **Выравнивание ответственности по ст.158 и 159 УК РФ** - размер крупного и особо крупного ущерба для кражи (158) и мошенничества (159) разные, в ст.159 выше. Суть инициативы в увеличении срока наказания, при снижении размера ущерба за мошенничество.

3. **Дополнение ст.183 УК РФ таким способом незаконного сбора информации, как «путем обмана».** Поправка даст возможность привлекать к уголовной ответственности преступников, непосредственно осуществляющих воздействие на граждан методами социальной инженерии, без установления всех участников группы.

Вносится депутатами
Государственной Думы
А.Г. Аксаковым
И.Б. Дивинским
М.В. Емельяновым

Проект № 186266-7

ФЕДЕРАЛЬНЫЙ ЗАКОН

О внесении изменений в Уголовный кодекс Российской Федерации (в части усиления уголовной ответственности за хищение денежных средств с банковского счета или электронных денежных средств)

Внести в Уголовный кодекс Российской Федерации (Собрание законодательства Российской Федерации, 1996, № 25, ст. 2954; 2001, № 33, ст. 3424; 2003, № 50, ст. 4848; 2007, № 1, ст. 46; 2009, № 52, ст. 6453; 2011, №11, ст. 1495; 2011, № 50, ст. 7362; 2012, № 49, ст. 6752; 2015, № 27, ст. 3984; 2016, № 27, ст. 4256; 2016, № 27, ст. 4258) следующие изменения:

1) в статье 158:

а) в части третьей:

в пункте «в» слово «размере, -» заменить словом «размере;»;

дополнить пунктом «г» следующего содержания:

«г) с банковского счета, а равно электронных денежных средств, -»;

б) пункт 4 примечаний изложить в следующей редакции:

«4. Крупным размером в статьях настоящей главы, за исключением частей шестой и седьмой статьи 159, статей 159^1 и 159^5, признается стоимость имущества, превышающая двести пятьдесят тысяч рублей, а особо крупным - один миллион рублей.»;

2) в примечании к статье 159^1 слова «, а также в статьях 159^3, 159^5, 159^6 настоящей главы» заменить словами «и статье 159^5 настоящего Кодекса»;

3) в статье 159^3:

а) наименование изложить в следующей редакции:

«Статья 159^3. Мошенничество с использованием электронных средств платежа»;

б) в части первой:

абзац первый изложить в следующей редакции:

«1. Мошенничество с использованием электронных средств платежа, то есть хищение чужого имущества, совершенное с использованием поддельного или принадлежащего другому лицу электронного средства платежа, в том числе кредитной, расчетной или иной платежной карты, путем обмана уполномоченного работника кредитной, торговой или иной организации, -»;

в абзаце втором слова «арестом на срок до четырех месяцев» заменить словами «лишением свободы на срок до трех лет»;

4) абзац первый части второй статьи 159^6 изложить в следующей редакции:

«2. То же деяние, совершенное группой лиц по предварительному сговору или с банковского счета, а равно электронных денежных средств либо с причинением значительного ущерба гражданину, -»;

5) абзац первый части первой статьи 183 после слова «, путем» дополнить словом «обмана,».

Президент
Российской Федерации

Законопроект внесен в ГД
asozd2.duma.gov.ru/main.nsf/(Spravka)?OpenAgent&RN=186266-7

Предложения и инициативы Сбербанка направленные на повышение эффективности регулирования в уголовном и уголовно-процессуальном законодательстве РФ (с начала 2017)

Внести изменения в статью 273 УК РФ в части введения уголовной ответственности за хранение, предоставление, предложение предоставления и приобретение вредоносной компьютерной программы. Статью 273 УК РФ изложить в следующей редакции: «Создание, хранение, использование, распространение, предоставление, предложение предоставления и приобретение вредоносной компьютерной программы».

Инициировать перед Верховным Судом РФ издание нового **Постановления Пленума, закрепляющего принципы правоприменительной практики по делам о хищениях с применением ИТ и в сфере компьютерной информации,** а также по делам, связанным с неправомерным доступом к охраняемой законом компьютерной информации (вместо устаревшего Постановления Пленума ВС РФ № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате» от 27.12.2007).

Ввести в законодательство понятие киберпреступления, описать типовые схемы кибермошенничества, разработать, согласовать и утвердить методические указания проведения расследований киберпреступлений.

Текущее регулирование в законодательстве РФ в сфере обработки и защиты персональных данных

ФЗ-152 "О персональных данных"
Ст.3 Персональные данные (ПДн) - **<u>любая</u>** информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн)
Постановление Правительства №1119
«Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
Приказы ФСТЭК №49 и 21
«Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн»
Приказ ФСБ №378
«Об утверждении Состава и содержания орг-технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн с использованием СКЗИ»

ФЗ-126 "О связи"
Ст.53 Базы данных об абонентах операторов связи
К сведениям об абонентах относятся:
- **фамилия, имя, отчество** или псевдоним;
- наименование абонента ЮЛ;
- фамилия, имя, отчество руководителя и работников этого ЮЛ;
- **адрес абонента или адрес установки оконечного оборудования**;
- абонентские номера;
- **другие данные, позволяющие идентифицировать абонента или его оконечное оборудование**;
- **сведения БД систем расчета за оказанные услуги связи, в т.ч. о соединениях, трафике и платежах абонента**
Ст.63 Тайна связи
гарантируется тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи

Конституция
Ст.23
1. Каждый имеет право на неприкосновенность частной жизни, **личную и семейную тайну**, защиту своей чести и доброго имени.
2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.
Гражданский Кодекс РФ
Ст.857 Банковская тайна
Банк гарантирует тайну банковского счета и банковского вклада, операций по счету и **сведений о клиенте**

ФЗ-395 "О банках и банковской деятельности"
Ст.26 Банковская тайна
Кредитная организация гарантирует тайну об операциях, о счетах и вкладах **своих клиентов** и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону

Открытые вопросы регулирования в законодательстве РФ о персональных данных

Обширность определения ПДн, смешаны сведения и личного, и семейного характера, идентифицирующие личность признаки, включая биометрические данные, иные виды сведений, отнесенных к так называемым «специальным», а также второстепенные, технологические, атрибутивные сведения типа:

1. Псевдоним пользователя в сети, и даже сессионные куки
2. Адрес установки оконечного оборудования связи
3. сведения БД систем расчета за оказанные услуги связи, в т.ч. о соединениях, трафике и платежах
4. Технологические данные о номере sim карты, IMSI, IMEI, MAC, IP-адрес пользовательского оборудования

Для сравнения, в международном стандарте PCI DSS v.3 четко разграничены виды чувствительных данных, как и область его применения:

		Элемент данных	Хранение разрешено	Хранение данных в … согласно тре…
Данные платежных карт (Account Data)	Данные держателя карты (Cardholder Data)	Основной номер держателя карты (PAN)	Да	Да
		Имя держателя карты	Да	Нет
		Сервисный код	Да	Нет
		Дата истечения срока действия карты	Да	Нет
	Критичные аутентификационные данные (Sensitive Authentication Data)[2]	Полные данные дорожки[3]	Нет	Нельзя хранить согла…
		CAV2/CVC2/CVV2/CID[4]	Нет	Нельзя хранить согла…
		PIN/PIN-блок[5]	Нет	Нельзя хранить согла…

Требования 3.3 и 3.4 стандарта PCI DSS применяются только к основному номеру держателя карты (PAN). Если PAN хранится вместе с другими данными, то в соответствии с требованием 3.4 хранить в нечитаемом виде необходимо только PAN.

Запрещается хранить критичные аутентификационные данные после авторизации, даже в зашифрованном виде. Данное требование действует, даже если PAN отсутствует в среде. Организации должны напрямую связаться со своими эквайерами или отделениями, отвечающими за отдельные торговые марки, чтобы узнать, разрешается ли хранить критичные аутентификационные данные до авторизации и в течение какого срока, а также получить информацию о других требованиях к использованию и защите данных.

Область применения стандарта PCI DSS

Данный стандарт применяется для всех организаций сферы обработки платежных карт: торговых точек, процессинговых центров, финансовых учреждений и поставщиков услуг, а также других организаций, которые хранят, обрабатывают или передают данные держателей карт и (или) критичные аутентификационные данные.

Данные держателей карт и критичные аутентификационные данные включают следующее.

Данные платежных карт (Account Data)	
Данные держателя карты:	**Критичные аутентификационные данные:**
▪ Основной номер держателя карты (PAN) ▪ Имя держателя карты ▪ Дата истечения срока действия карты ▪ Сервисный код	▪ Полные данные дорожки магнитной полосы или ее эквивалент на чипе ▪ CAV2/CVC2/CVV2/CID ▪ PIN/PIN-блоки

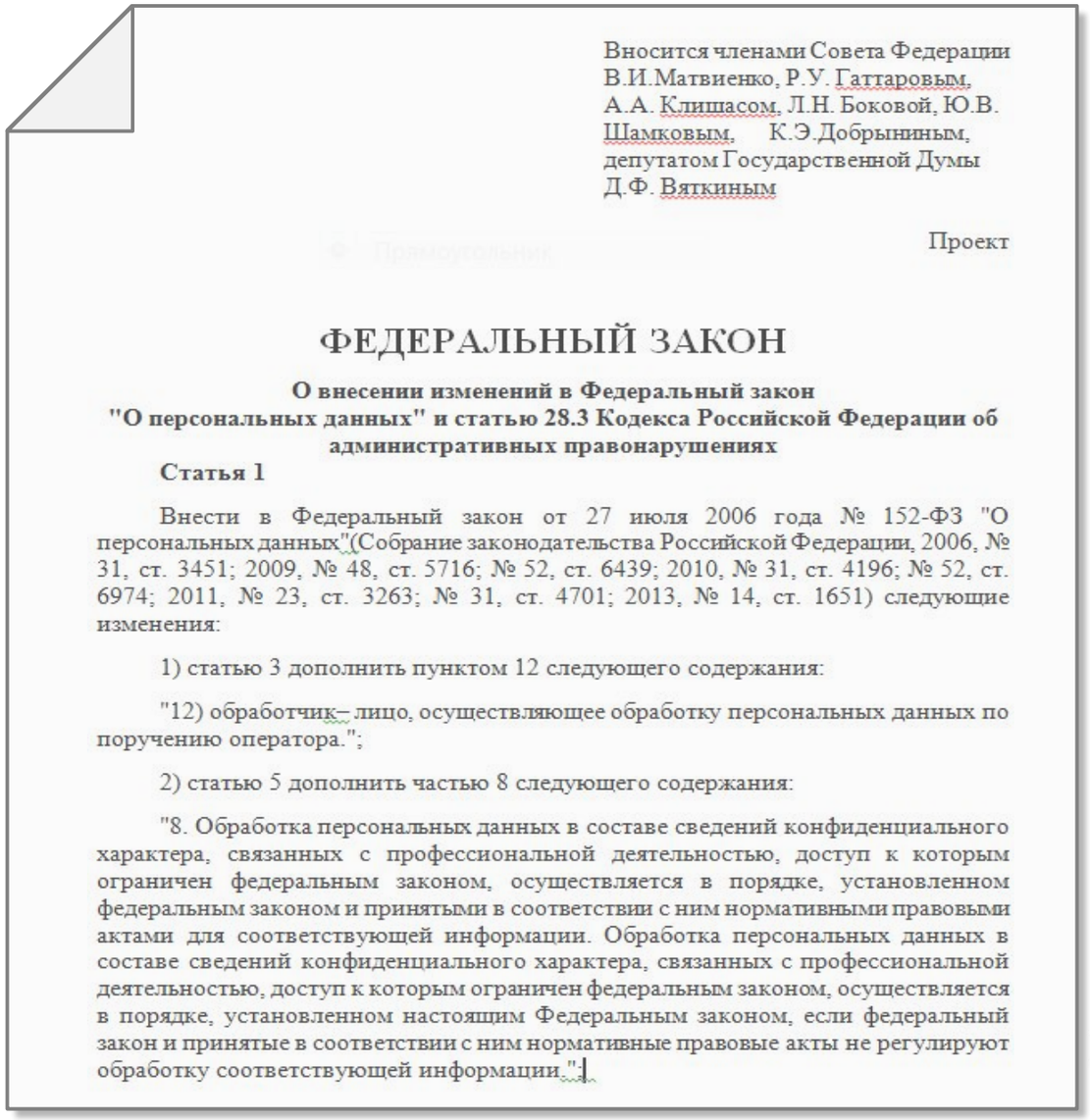
Основной номер держателя карты является определяющим фактором для данных держателя карты. Если имя держателя карты, сервисный код и (или) срок действия хранятся, обрабатываются или передаются вместе с основным номером держателя карты или другим образом присутствуют в информационной среде держателей карт, то они должны быть защищены согласно применимым требованиям PCI DSS.

Предложения Сбербанка направленные на повышение эффективности регулирования в законодательстве РФ о персональных данных

- **Конкретизировать, что обработка ПДн** в составе сведений конфиденциального характера, связанных с профессиональной деятельностью, доступ к которым ограничен федеральным законом, **осуществляется в порядке, установленном федеральным законом и принятыми в соответствии с ним нормативными правовыми актами** для соответствующего вида конфиденциальных сведений

- **Уточнить, что к биометрическим персональным данным относятся сведения, которые характеризуют физиологические и биологические особенности человека**, на основании которых можно установить его личность и которые используются оператором для автоматической идентификации субъекта ПДн

- **Дополнить определение ПДн уточнением**, что к ПДн не относятся данные, которые сервисы сами собирают и обрабатывают на своих вычислительных мощностях, а именно: псевдоним пользователя в сети, сессионные куки, ip-адрес устройства пользователя, посредством которого пользователь зашел на сайт Оператора, историю запросов пользователя, посещаемые интернет-ресурсы и т.п., а также иную технологическую информацию: данные о номере sim карты, IMSI, IMEI, MAC-адрес пользовательского оборудования



Вносится членами Совета Федерации В.И.Матвиенко, Р.У. Гаттаровым, А.А. Клишасом, Л.Н. Боковой, Ю.В. Шамковым, К.Э.Добрыниным, депутатом Государственной Думы Д.Ф. Вяткиным

Проект

ФЕДЕРАЛЬНЫЙ ЗАКОН

О внесении изменений в Федеральный закон "О персональных данных" и статью 28.3 Кодекса Российской Федерации об административных правонарушениях

Статья 1

Внести в Федеральный закон от 27 июля 2006 года № 152-ФЗ "О персональных данных"(Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2009, № 48, ст. 5716; № 52, ст. 6439; 2010, № 31, ст. 4196; № 52, ст. 6974; 2011, № 23, ст. 3263; № 31, ст. 4701; 2013, № 14, ст. 1651) следующие изменения:

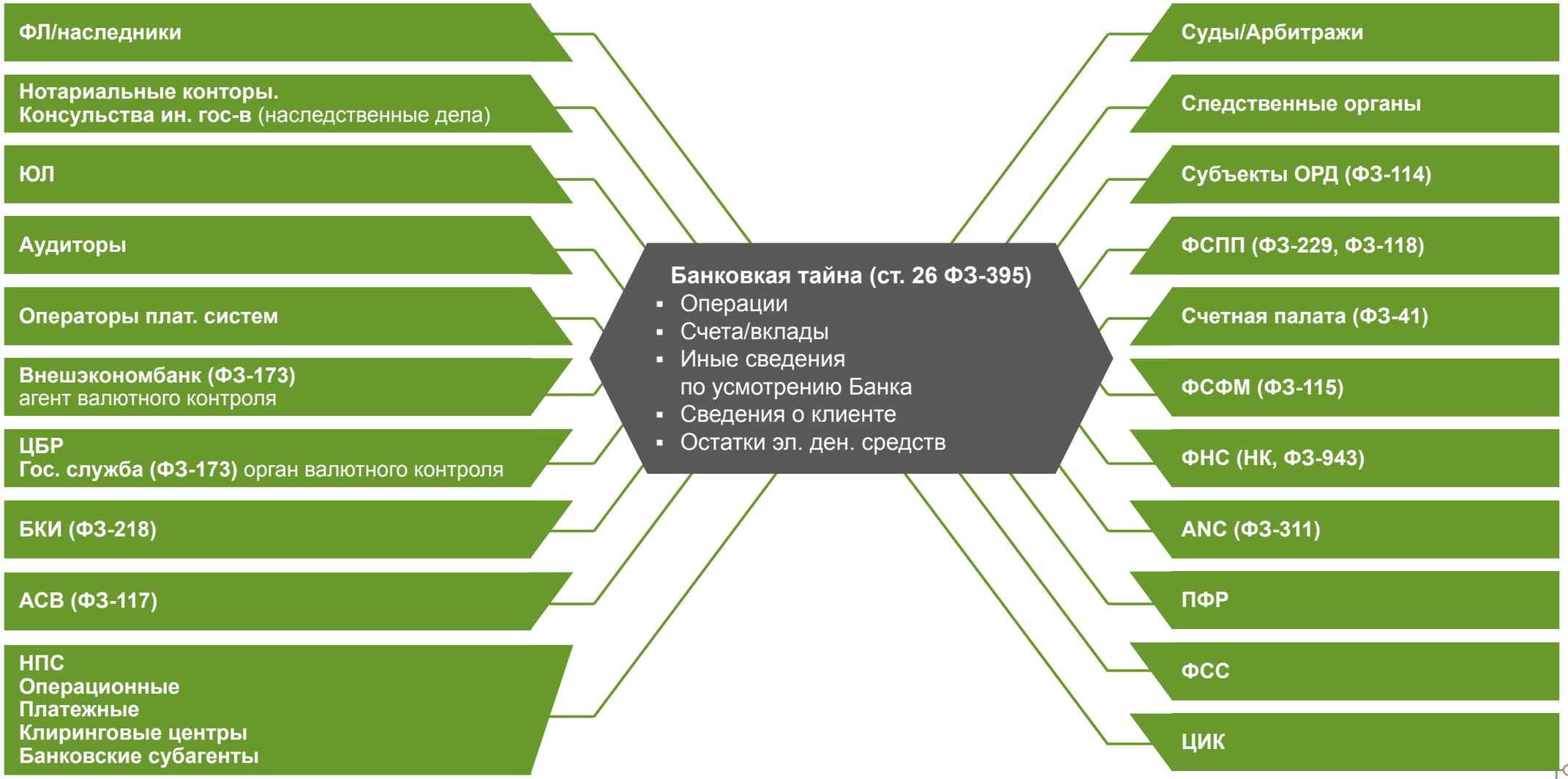
1) статью 3 дополнить пунктом 12 следующего содержания:

"12) обработчик– лицо, осуществляющее обработку персональных данных по поручению оператора.";

2) статью 5 дополнить частью 8 следующего содержания:

"8. Обработка персональных данных в составе сведений конфиденциального характера, связанных с профессиональной деятельностью, доступ к которым ограничен федеральным законом, осуществляется в порядке, установленном федеральным законом и принятыми в соответствии с ним нормативными правовыми актами для соответствующей информации. Обработка персональных данных в составе сведений конфиденциального характера, связанных с профессиональной деятельностью, доступ к которым ограничен федеральным законом, осуществляется в порядке, установленном настоящим Федеральным законом, если федеральный закон и принятые в соответствии с ним нормативные правовые акты не регулируют обработку соответствующей информации."

Текущее регулирование в законодательстве РФ в сфере обработки сведений, составляющих банковскую тайну



Предложения по внесению изменений в законодательство РФ в части касающейся обмена банковской тайной и ПДн клиентов

1

Внести изменения в **ФЗ-152 «О персональных данных» и ФЗ-126 «О связи», отделив сведения личного и семейного характера от технологических данных**, связанных с гражданином-ФЛ, как пользователем услуг связи, которые, одновременно, не позволили бы провести его идентификацию как субъекта ПДн. К технологическим данным считаем возможным отнести:

- IMEI код телефонного устройства
- ICCID идентификатор SIM карты
- IMSI идентификатор абонента в сети сотовой связи любого оператора РФ
- MAC и IP адреса пользовательских устройств, подключаемых к сети интернет
- а также данные о фактах изменения статусов обслуживания абонентов, например, замены SIM

2

Закрепить в ФЗ-161 «О Национальной платежной системе» и ФЗ-126 «О связи» за банками право формирования запросов о технологических данных своих клиентов, являющихся абонентами соответствующего оператора связи или интернет-провайдера, иных операторов ПДн, без получения письменного согласия граждан – субъектов ПДн.

3

Внести изменения в ФЗ-395 «О банках и банковской деятельности», уголовное и уголовно-процессуальное законодательство положения, предусматривающие возможность для банков инициативно сообщать в правоохранительные органы и субъектам ОРД сведения, составляющие банковскую тайну в отношении лиц, подозреваемых в совершении киберпреступлений.

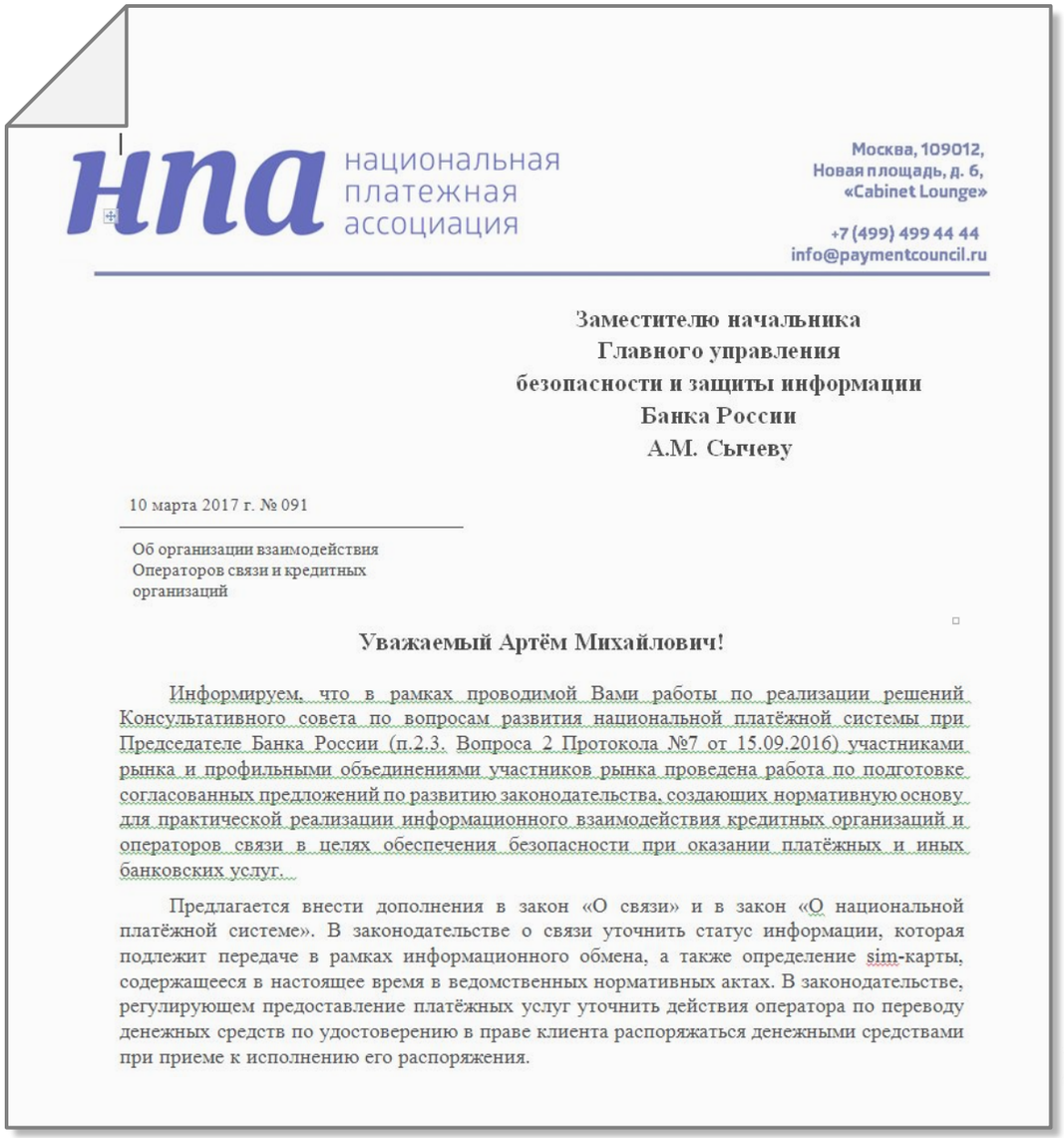
SCST

Инициативы Сбербанка направленные на повышение эффективности противодействия киберпреступлениям путем изменений в законодательстве РФ о связи и НПС

При взаимодействии с представителями телеком-муникационной сферы: Минкомсвязи, Роскомнадзор, ключевые операторы сотовой связи, Национальной платежной ассоциации, на базе ГУБЗИ ЦБР, были выработаны **предложения о внесении изменений в ФЗ-126 «О связи» и ФЗ-161 «О национальной платежной системе»**, а именно:

1. Статью 53 (ФЗ-126 "О связи") пункт 1 дополнить частью 7 следующего содержания: «Оператор связи вправе на основании соглашения с кредитной организацией и по ее запросу, в соответствии с пунктом 4 Статьи 8 ФЗ-161 «О Национальной платежной системе», передавать информацию о факте замены идентификационного модуля, о приостановлении оказания услуг связи, о переоформлении абонентского номера или прекращении абонентского договора. Согласие абонента, пользователя услугами связи на передачу указанной информации не требуется».

2. Дополнить статью 8 (ФЗ-161 «О национальной платежной системе») пункт 4 частью 2 следующего содержания: «Оператор по переводу денежных средств с целью удостовериться в праве клиента распоряжаться денежными средствами вправе на основании соглашения с оператором связи получать от него информацию в соответствии с п.1 Статьи 53 ФЗ-126 «О связи»».



нпа национальная платежная ассоциация

Москва, 109012,
Новая площадь, д. 6,
«Cabinet Lounge»

+7 (499) 499 44 44
info@paymentcouncil.ru

Заместителю начальника
Главного управления
безопасности и защиты информации
Банка России
А.М. Сычеву

10 марта 2017 г. № 091

Об организации взаимодействия Операторов связи и кредитных организаций

Уважаемый Артём Михайлович!

Информируем, что в рамках проводимой Вами работы по реализации решений Консультативного совета по вопросам развития национальной платёжной системы при Председателе Банка России (п.2.3. Вопроса 2 Протокола №7 от 15.09.2016) участниками рынка и профильными объединениями участников рынка проведена работа по подготовке согласованных предложений по развитию законодательства, создающих нормативную основу для практической реализации информационного взаимодействия кредитных организаций и операторов связи в целях обеспечения безопасности при оказании платёжных и иных банковских услуг.

Предлагается внести дополнения в закон «О связи» и в закон «О национальной платёжной системе». В законодательстве о связи уточнить статус информации, которая подлежит передаче в рамках информационного обмена, а также определение sim-карты, содержащееся в настоящее время в ведомственных нормативных актах. В законодательстве, регулирующем предоставление платёжных услуг уточнить действия оператора по переводу денежных средств по удостоверению в праве клиента распоряжаться денежными средствами при приеме к исполнению его распоряжения.

Открытые вопросы в направлении сближения требований международного и национального регулирования в сфере информационной безопасности

Законодательство о кибербезопасности	Принятие решения о ратификации Конвенции Совета Европы о кибербезопасности (Budapest Convention on Cybercrime 2001г)
Законодательство в сфере международного сотрудничества и обмена информацией об инцидентах ИБ и фактах совершенных киберпреступлений	Создание условий (в т.ч. правовых) для организации обмена информацией о киберпреступлениях и инцидентах ИБ Координация действий между международными (European Cybercrime Centre*) и национальными (FinCERT), государственными и коммерческими центрами противодействия киберпреступлениям
Стандартизация и гармонизация международного и национального законодательства о ПДн	Гармонизация положений Регламента ЕС о защите персональных данных 2016/679 (GDPR) и ФЗ-152 «О персональных данных»

(*) Еврокомиссия создала в 2012г European Cybercrime Centre (EC3) в составе Европола с ШК в Гааге, а в 2013г была утверждена Европарламентом «Directive on Attacks against InfoSystems 2013/40/EU», заменившая рамочное решение 2005/222/JHA

СПАСИБО ЗА ВНИМАНИЕ!

ВОПРОСЫ?