

Информационное агентство
«WEB-мониторинг»
Свидетельство ИА № ФС7733219 от 19 сентября 2008 года
Научно-практический электронный журнал

ФИНАНСОВЫЕ ПРАВОНАРУШЕНИЯ И ПРЕСТУПЛЕНИЯ

№ 2 (113) 2016
(выходит с октября 2006 г.)



Полиция информирует: как не стать жертвами мошенников

Фото с сайта

http://static8.depositphotos.com/1005404/1049/i/950/depositphotos_10499957-Money-security.jpg

См. раздел

«Безопасное ведение бизнеса и домохозяйства»

**Издатель
ИП Фединский Ю.И.**

www.webmonitor.ucoz.ru
www.finprest.ucoz.ru
webmonitor@yandex.ru
тел. 8 985 333 87 59

Москва
2016

Подписку на издания ИА «WEB-мониторинг»
с любого календарного месяца
можно оформить

по электронному каталогу
ИД «Экономическая газета»

Финансовые правонарушения и преступления

Для тех, кому важно знать финансовые закон и формы их нарушения

Подписной индекс **80663э**

Информация здесь

Валюта: регулирование и контроль

Для тех, кто хочет быть в курсе валют: вчера, сегодня и завтра

Подписной индекс **42335э**

Информация здесь

Налоговые правонарушения и преступления

Для тех, кто стремится грамотно платить налоги

Подписной индекс **41587э**

Информация здесь

ИД "Экономическая газета"

<http://www.arpk.org>

тел. (499) 152 88 50

Подписка

на 2016 год

на электронный журнал

Финансовые правонарушения и преступления

Для тех, кому важно знать законы и формы их нарушения

Объединенный каталог «Пресса России»
подписной индекс **80663**

Оглавление

Криминальная хроника	16
Новости в заголовках	16
"Бывшего банкира осудили с помощью Интерпола"	22
Ликероводочная афера в Коми	23
Российская Газета: "СК РФ: потерпевшими по делу генерала МВД Сугробова признаны 30 человек"	24
Завершено следствие по делу бывшего главы петербургской турфирмы «Атлас»	25
Пока ЕСПЧ будет разбираться с жалобой националиста Поткина, в Москве начнется процесс по его делу	25
Чайка и Бастрыкин проверят главу ФСБ по заявлению Навального о махинациях с землей на Рублевке	26
От главы Минсельхоза требуют отчитаться об аграрном бизнесе своих родных	27
На сына губернатора Иркутской области завели третье уголовное дело	27
За хищение 500 млн руб. судят зампреда лишившегося лицензии "Витас Банка 28	
Экс-министр Сердюков выступит в защиту зятя по делу о "мертвых душах" на 13 млн руб.	28
В Москве направлено в суд дело экс-банкира, обвиняемого в хищении на 570 млн руб. .29	
Осужденный бизнесмен обратился в президиум ВС	29
Сообщник «авторитетного» депутата «Маги банкира» попал под суд из-под домашнего ареста	30
Очередное заседание Межведомственной рабочей группы по противодействию незаконным финансовым операциям	30
Задержан обвиняемый в хищении бывший глава новосибирского филиала ВТБ	31
Брат бывшего вице-премьера Дагестана Гаджи Махачева задержан в Москве	31
В Москве задержан экс-финдиректор банка по делу о миллиардном хищении	31
ОПРФ просит Генпрокуратуру проверить кредиты на косметику	32
Генеральная прокуратура Российской Федерации организовала проверку исполнения законодательства, обеспечивающего защиту прав предпринимателей в сфере инвестиционной деятельности	33
В Новосибирске органы прокуратуры приняли меры, направленные на пресечение роста платы граждан за жилищно-коммунальные услуги	33
Следствие по делу экс-главы «Башнефти» Рахимова не уложилось в срок	33
Центробанк разбирается с банками «Интеркоммерц» и «Межтрансбанк»	34
Заместитель Генерального прокурора Российской Федерации Сергей Зайцев взял на личный контроль ход проверки деятельности микрофинансовых организаций и коллекторских агентств в Ульяновской области	35
Свердловская полиция разыскивает супругов, обманувших 300 человек	35
Экс-председатель партии «Социал-демократы России» Алексей Бунацев задержан за «африканские» аферы	36
В Ростове осудили экс-министра труда и соцразвития области и ее заместителя	37
За рубежом	38
В мире	38
Спорт в болоте: коррупция, допинг, договорные матчи и жажда наживы	38
Азербайджан	40
Банковские ячейки вместо депозитного счета?	40

Беларусь	42
Хищение из банкоматов – наиболее распространенное киберпреступление в Беларуси	42
Болгария	43
Ограбление банка по-болгарски	43
Германия.....	43
В попытке ограбления немецких инкассаторов обвиняются террористы-пенсионеры из RAF	43
Казахстан	43
Работу почтовых отделений планируют автоматизировать на 100% до 2017 года из-за системных хищений денег сотрудниками "Казпочты"	43
В Казахстане существует проблема хищения денежных средств сотрудниками сельских почтовых отделений	44
Самые громкие экономические преступления в РК.....	45
Тюрьмы из инкубаторов террористов нужно превратить в инкубаторы предпринимателей.....	46
Почти треть страховых выплат получают жулики - эксперты	51
Мошенничество – способов много, а цель одна	52
Наказание за новые виды мошенничества может появиться в Уголовном кодексе	53
Кризис сделал страховое мошенничество бизнесом	55
Китай	56
Китайский центр исследований и мониторинга борьбы с отмыванием денег и Управление по борьбе с финансовыми преступлениями США подписали меморандум о сотрудничестве.....	56
Кыргызстан	56
Какое государство мы строим: применим ли сингапурский и китайский опыт борьбы с коррупцией в Кыргызстане?.....	56
Ипотека.kg: ловкость рук, и никакого мошенничества, -.....	62
Латвия	64
Взрыв в Болдерае: преступники хотели ограбить банкомат (видео)	64
Сербия.....	65
Масштабнейшее в истории страны расследование по борьбе с коррупцией.....	65
США.....	65
Расплата	65
ФБР: люди должны доверять своим чиновникам.....	67
В 2015 ритейлеры США чаще сталкивались с фродом.....	70
Украинца осудили в США на 15 лет за мошенничество с автостраховками	71
Таджикистан	71
Операция "птичка". Кто украл мешок денег у "Сохибкорбонк"?.....	71
Пришел, инвестировал - в тюрьму. Как китайского предпринимателя брали на взятке? ..	72
Украина	75
«Липовая» страховка. Как мошенники зарабатывают 200 миллионов в год на полисах «автогражданки»	75
Цель грабителей — домашняя техника с выходом в интернет	77
Киеве полицейские отпустили грабителя банка, который показал "корочки" МВД.....	79
Военно-финансовые махинации.....	80
Франция	82
Сын главы МИД Франции допрошен по делу об отмывании денег.....	82

Чехия	82
Все большую популярность в Чехии приобретает страховое мошенничество	82
Видео: вор не только банк ограбил, но и дверь выломал	83
Швейцария	83
СМИ узнали сумму выплат Credit Suisse и Barclays за финансовые махинации	83
Дайджест	84
Важнейшие правовые темы в прессе – обзор СМИ (январь 2016)	84
Аналитика	126
Нелегальный вывод капитала из России в 2004-2013 годах превысил \$1 трлн	126
КС хотел защитить вкладчиков, а открыл ящик Пандоры	126
В газете "Известия" опубликована авторская колонка официального представителя Ск России в. И. Маркина	127
С пластиковых карт россиян с января по сентябрь 2015 года в результате ошибочных и злонамеренных действий сотрудников банков списан уже 1 млрд рублей	129
ВЦИОМ: в услугах ЖКХ россиян больше всего не устраивают высокие тарифы	129
Интервью руководителя четвертого следственного управления Главного следственного управления Следственного комитета Российской Федерации Руслана Ибиева «Российской газете»	130
Алексей Навальный: "Швейцария - ключевой для высокопоставленных чиновников регион"	133
Интервью Генерального прокурора Российской Федерации Юрия Чайки «Российской газете»	133
Чайка связал резкий рост преступности в 2015 году с финансовым кризисом	137
Меньше денег — больше краж	138
В Москве зафиксирован рост преступлений, характерных для кризиса 1998 года	139
СКР и МВД сильно разошлись по статистике раскрываемости преступлений	139
Интервью председателя Следственного комитета Российской Федерации Александра Бастрыкина "Российской газете"	140
Коммерсантъ: "Инженерам Восточного подчитали взятки"	143
Незаконные финансовые потоки: кто обескровливает Россию и почему об этом молчат	144
Кризис толкает на преступления	147
На Дальнем Востоке прокуроры принимают активные меры в целях противодействия коррупции	148
Новый КоАП: учёные-правоведы раскритиковали проект кодекса	149
Коррупционная Россия	154
Юридический консалтинг под санкциями: как заработать юристам на экономических ограничениях	155
Генеральный прокурор Российской Федерации Юрий Чайка взял под личный контроль ситуацию, связанную с деятельностью коллекторов в стране	159
За год число экономических преступлений в Новочеркасске увеличилось на 45%	160
Законодательство и право	161
С 1 января 2016 года при расчете налоговых пеней ставку рефинансирования предлагают заменить ключевой	161
Граждан без официального трудоустройства, которые тратят при этом более 1 млн рублей в год, могут начать контролировать налоговые органы	161
СКР предлагает ввести конфискацию имущества, как меру наказания	162

Центробанк должен лишать банки лицензии за нарушение антиотмывочного законодательства только через суд	163
Депутаты разрешили покупать ювелирные изделия без паспорта на сумму до 40 тыс. рублей	163
Обзор бухгалтерских событий за неделю: бизнесу повышают штрафы за ложную статистику	163
В Госдуму внесен законопроект о переходе на новые кассы, передающие данные в ФНС	164
Медведев пообещал масштабную либерализацию УК для бизнеса	165
"Ведомости": Путину предложили расширить полномочия прокуроров в интересах бизнеса	165
Путин передал Росалкогольрегулирование и ФТС в ведение Минфина	165
Правительство поддержало увеличение штрафов работодателям за задержку зарплаты	166
Инициатива введения суда присяжных для вынесения решений по экономическим преступлениям	166
В ГД вернулись к обсуждению законопроекта об ужесточении правил проведения торгов госкорпорациями	166
КС принял к рассмотрению жалобы на порядок сбора средств для капремонта	167
ГК поправят для защиты добросовестных приобретателей криминального жилья	167
В ГД раскритиковали новый КоАП, написанный "для ученых и адвокатов"	168
Путин предложил многократно повысить порог ущерба по экономическим статьям	169
Госдума вводит уголовную ответственность за фальсификацию доказательств по административным делам	169
Обсуждение КоАП: прокурорам – полномочия, мелким хищениям – особый порядок	169
Местные власти могут лишиться полномочий за нецелевое использование бюджета ...	171
Государственная дума одобрила увольнение мэров за нарушения бюджетного законодательства	172
Незаконная банковская деятельность	173
Как устроена финансовая «воронка» РФ	173
1,5 млрд рублей прокачали через однодневки	175
В Новгородской области вынесен приговор о незаконном обналичивании 290 млн рублей	175
Банкротство фиктивное и преднамеренное	177
В Пермском крае прокуратура направила в суд уголовное дело о хищении руководителем управляющих компаний более 330 млн рублей	177
Коммерсантъ: "ОПС специализировалось на банкротствах"	177
Предправления АКБ «Кодекс» будут судить за преднамеренное банкротство 5-летней давности	178
Управление ФНС России по Амурской области информирует об изменениях в законе «О банкротстве (несостоятельности)»	179
Безопасное ведение бизнеса и домохозяйства	180
Зачем интернет-банку мониторинг контрагентов	180
Материалы по защите прав потребителей финансовых услуг	181
Андрей Заикин: «Структурированные данные — основа информационной безопасности банка»	181
Осторожно, мошенники! Как уберечь себя от обмана	184
В МВД по Чувашской Республике прошла пресс-конференция по теме: «Киберпреступления и телефонные мошенничества»	185

МВД России по Тверской области советует, как уберечь себя от мошенничества в интернете.....	187
Никогда не сообщайте посторонним лицам номер своей банковской карты!.....	188
Надежно, как в Сбербанке: в Верхневолжье осудили специалиста по работе с клиентами	189
В Ульяновске полиция разыскивает женщину, похитившую в банке 5 млн рублей	189
Памятка для граждан: Подозрительно низкая цена товара в Интернете.....	190
Полиция информирует граждан о том, как не стать жертвами мошенников	190
Заражение телефона вирусом грозит потерей денежных средств с банковской карты ..	191
Финансовые правонарушения в сфере ЖКХ	192
В Сибири прокуроры потребовали от органов местного самоуправления исполнять законы в сфере жилищно-коммунального хозяйства	192
В Амурской области прокуратура принимает меры, направленные на защиту прав граждан в сфере жилищно-коммунального хозяйства	192
В Ханты-Мансийском автономном округе по итогам прокурорской проверки возбуждено уголовное дело о хищении более 14,5 млн руб. в сфере ЖКХ	193
В Петербурге директора консалтинговой фирмы подозревают в хищении миллиона	193
На Камчатке в суд направлено уголовное дело о махинациях с коммунальными платежами на сумму более 91,7 млн рублей.....	193
В Башкортостане по требованию прокуратуры управляющая компания произвела перерасчет незаконно начисленной гражданам платы за отопление на сумму свыше 19 млн рублей	194
В Алтайском крае направлено в суд уголовное дело о хищении денежных средств, перечисленных 253 жителями многоквартирных домов за услуги ЖКХ	194
Незаконный игорный бизнес.....	195
В Санкт-Петербурге полицией пресечена деятельность незаконного игорного заведения	195
В городе Тихвине полицейские пресекли деятельность незаконного игорного заведения	195
Подпольный покерный клуб ликвидировали столичные полицейские в Москве на Кутузовском проспекте	196
Полицией Екатеринбурга пресечена деятельность нелегального покерного зала.	196
По иску Одинцовской городской прокуратуры Московской области суд взыскал с осужденных за незаконные организацию азартных игр более 24 млн руб.	196
Полицией Екатеринбурга пресечена деятельность нелегального покерного зала	197
В Набережных Челнах полицейские пресекли деятельность незаконного игорного заведения	197
В Подмосковье вынесен приговор по уголовному делу в отношении организатора незаконного игорного бизнеса в Наро-Фоминском районе	197
В Архангельской области направлено в суд уголовное дело в отношении бывшего полицейского, обвиняемого в покровительстве игорному бизнесу.....	198
В Архангельской области направлено в суд уголовное дело в отношении десяти бывших сотрудников полиции, покровительствовавших игорному бизнесу.....	198
Почему Россия стоит на пороге легализации онлайн-покера	199
На западе Москвы полицейские ликвидировали подпольный покерный клуб и задержали его организатора.....	200
Исследования	201
Заемщик не платит по ипотечному кредиту. Популярны варианты развития ситуации	201

Банкоматное мошенничество	204
Киберпреступления	211
Хакеры сняли почти 100 млн рублей со счетов банка.....	211
Что делать после кибератаки?	211
Чувашские полицейские задержали кибермошенников, обманывавших пользователей социальной сети (видео)	212
Финансовый троян атакует устройства на базе Android.....	212
Генеральная прокуратура Российской Федерации направила в суд уголовное дело в отношении одного из руководителей преступного сообщества, обвиняемого в мошенничестве в сфере компьютерной информации	213
Судят взломщика электронной базы банков, похитившего со счетов их клиентов 25 млн руб.	213
Хищение денежных средств с банковских карт	214
Два года лишения свободы может получить бывший программист волгоградского предприятия за неправомерный доступ к корпоративной почте	215
Ущерб от кибератак в России составил 4 миллиарда долларов в 2015 году	215
Trend Micro: 2016 год будет знаковым в деле противостояния киберпреступности.....	216
Противодействие коррупции	217
Интервью официального представителя Следственного комитета России Владимира Маркина программе "Формула смысла" в эфире радио "Вести FM".....	217
Интервью официального представителя Следственного комитета России Владимира Маркина «Российской газете»	223
Интервью руководителя следственного управления Следственного комитета России по Хабаровскому краю Петра Решетникова информационному агентству «Интерфакс».....	225
Коммерсантъ: "Коррупцию подсчитали и обобщили"	228
По инициативе прокурора Чеченской Республики 20 служащих регионального министерства финансов привлечены к ответственности за нарушения антикоррупционного законодательства.....	229
В Калининграде по материалам прокуратуры возбуждено уголовное дело о незаконном получении административными сотрудниками больницы премий на сумму более 9 млн рублей.....	229
«Вашингтон серьезно подвел российский народ»	229
Глава управления Росимущества приговорен к 10 годам и 385-миллионному штрафу за взятку	235
Адвокат задержан с 6-миллионной взяткой для следователей	235
Задержан глава УЭБиПК, получивший 1 млн руб. "за покровительство"	235
В Костроме подмосковного юриста будут судить за крупнейшую взятку 0	236
Заседание Совета по противодействию коррупции.	236
Замдиректора ФГУП «РСУ» не смог обжаловать приговор за подкуп при строительстве Приморского океанариума	240
Яровая: Необходимо ввести новый критерий обоснованности закупки	240
Коррупция на уровне Западной Африки	241
В Омске осужден один из руководителей организации за незаконное получение в качестве коммерческого подкупа более 1 млн руб.	242
В Пермском крае по постановлению прокуроров две коммерческие организации привлечены к штрафам за коррупционные правонарушения	243
Кража, ограбление, разбой.....	244
Ограбление банков	244
Упавшие с небес. Зачем смотреть экшн "На гребне волны"	244

В канун Нового Года в Москве на 12 млн. рублей был ограблен банк	244
Хакеры сняли почти 100 миллионов рублей со счетов коммерческого банка	244
В Санкт-Петербурге перед судом предстанут члены преступного сообщества, похищавшие денежные средства через банкоматы	244
Рекордное ограбление банка расследует спецгруппа полиции Петербурга.....	245
Миллиардное ограбление "Промсвязьбанка": можно ли доказать ущерб?	245
Грабители "Промсвязьбанка" год изучали систему безопасности	247
По факту ограбления банка в Ярославле возбуждено уголовное дело	248
Ограбления по-ярославски. 8 удачных и не очень попыток злоумышленников поживиться за счет банков	248
Очевидица ограбления ярославского "Локо-Банка": "Преступником может быть покупатель соседнего магазина!"	249
В Ярославле ограбили банк: стала известна сумма ущерба.....	250
Ограбление банка в Нижнем Тагиле попало на видео.....	250
За голову грабителя "Промсвязьбанка" бизнесмены обещают 10 миллионов рублей	250
Хищение денег из банкоматов	251
Необычные способы хищения средств из банкоматов	251
В Волжском грабитель-неудачник похитил из банкомата только видеокамеру.....	251
Бывшего учителя осудили в Москве за подрыв и ограбление банкомата 0	251
В Москве задержали банду похитителей банкоматов	252
В Улан-Удэ грабители взорвали банкомат «БайкалБанка»	252
Сбербанк требует с охранников более шести миллионов рублей за ограбленный банкомат	253
Наладчик банкоматов, задержан за попытку ограбить один из них.....	253
В Подмосковье при ограблении банкомата мужчина подорвался на самодельной бомбе	253
В Краснотурьинске задержали взломщика банкомата	254
Стали известны подробности о взрыве банкомата "Сбербанка" в Москве на Ленинском проспекте в новогоднюю ночь	254
В Пензе ограблен второй банкомат за последние 4 дня.....	254
Комсомольчане взрывали банкомат в новогодних костюмах	255
В Уфе грабители пытались автомобилем вытащить банкомат из магазина	255
Банкомат с 1,5 млн рублей "вскрыли" на новогодних каникулах в Приморье.....	255
Челябинец разгромил банкомат в Переславле, чтобы купить водки.....	256
Полицейские предотвратили ограбление банкомата с 15,5 млн руб. в ЗАО	256
После ограбления банкомата в здании РГА, депутаты сменили охранную фирму.....	256
Дерзкое ограбление банкоматов в Красноярске на миллионы	257
Как потрошат банкоматы	257
900 тысяч рублей украли из банкомата	259
Полиция подмосковного города Люберцы сообщила о задержании жителей Курска, которые промышляли в столичном регионе ограблениями банкоматов посредством их подрыва.	260
Курские грабители взрывали банкоматы в Подмосковье	260
В Новгородской области осужден член преступной группы, пытавшейся похитить банкомат и более 1,5 млн рублей	260
Хакер опозорился и не смог вскрыть банкомат на Чкаловском проспекте	261
В Шахтах, при попытке ограбления банкомата, был застрелен охранник	261

Горе-взломщикам банкомата дали по четыре года условно	261
Королёвский житель будет отбывать срок в колонии за попытку ограбления банкомата	264
Гражданина Армении, подозреваемого в похищении терминала с деньгами, поймали в Твери	265
Нападение на инкассаторов	265
В распоряжение DonDay Шахты попало видео, ставшее первой зацепкой в деле ограбления валютчика	265
Почтовое отделение №128 Челябинска, у которого ограбили инкассаторов, закрыли на период следственных действий	266
Омске ищут вооруженных грабителей на серебристой «Десятке»	266
В Челябинске задержали подозреваемого в нападении на инкассаторов	266
На Урале начальницу почты убили за тысячу рублей	267
Незаконное получение и невозврат кредита и субсидий	268
В Серове вновь вскрыт факт кредитного мошенничества	268
В Тюмени направлено в суд уголовное дело о хищении бюджетной субсидии в размере более 1,4 млн руб., выделенной на приобретение жилья	268
В Петербурге кредитный мошенник с поддельным паспортом похитил несколько миллионов рублей	269
В Волгограде вынесен приговор по уголовному делу о незаконном получении банковского кредита в сумме 40 млн рублей	269
Ставропольский бизнесмен незаконно кредитовался на 25 млн рублей	269
Незаконное получение и использование материнского капитала	270
В Оренбургской области директор микрофинансовой организации предстанет перед судом за мошенничества с материнским капиталом	270
В Ханты-Мансийском автономном округе прокуратура защитила права многодетной матери, получившей отказ в распоряжении частью средств материнского капитала на образование своих детей	270
Мошенничество с материнским капиталом: в суд передано дело директора микрофинансовой организации	270
Финансовые мошенничества	272
Карты и мошенники: вернёт ли банк деньги, незаконно списанные со счёта	272
Генералу ФСИН вменили платную защиту бизнесмена	274
В Ленинградской области направлено в суд уголовное дело о мошенничестве с субсидиями для предпринимателей	274
Антология мошенничества	275
В Коми возбуждено уголовное дело по факту мошенничества с ценными бумагами	277
В Ставропольском крае вынесен приговор по уголовному делу о мошенничестве	277
В Нижегородской области завершено расследование уголовного дела по факту мошенничества в сфере эзотерических услуг	278
В Алтайском крае направлено в суд уголовное дело о мошенничестве при строительстве жилья	278
В Татарстане вынесен приговор бывшим адвокатам, признанным виновными в попытке хищения у клиента 6 млн рублей	278
В Пермском крае осужден телефонный мошенник, который представляясь должностным лицом похитил у престарелых граждан более 3 млн рублей	279
В Ульяновской области по материалам прокурорской проверки возбуждено уголовное дело о хищении средств, предназначенных для развития малого предпринимательства	279

В Башкортостане осуждены сообщницы, похитившие 95 млн рублей под видом заключения договоров о строительстве жилья.....	279
Прокуратура г. Волгограда направила в суд уголовное дело о мошенничестве, причинившем государству ущерб на сумму свыше 61 млн рублей	280
В Ленинградской области по инициативе прокуратуры возбуждено уголовное дело о мошенничестве с бюджетными средствами, выделенными на развитие здравоохранения.....	280
Внешпромбанк: мошенники или жертвы?	281
Краснодарский интернет-мошенник сядет в тюрьму на 2 года	282
Мошенники все чаще находят жертв среди самарцев, разместивших объявления на "Авито"	282
Самые популярные схемы мошенничества при приеме на работу	283
Омский мошенник, обманувший дольщиков на 60 миллионов, требует смягчения наказания по судуаркет	283
Банк России предупредил о новой схеме финансового мошенничества	284
В Воронеже возбуждено уголовное дело по факту мошенничества при получении выплат	284
Авторитетный финансист ответит за обещание спасти банк	285
В России появилась новая схема банковского мошенничества	285
В Республике Алтай вынесен приговор по уголовному делу о покушении на мошенничество на сумму более 12 млн руб.	286
В Москве задержали подозреваемых в мошенничестве со стройматериалами на 150 млн рублей	287
Барнаулец перевел интернет-мошенникам 100 тысяч рублей для покупки авто	287
Во Владивостоке вынесен приговор по уголовному делу о покушении на мошенничество в размере 1,5 млн долларов	288
В Тульской области направлено в суд уголовное дело в отношении муниципальной служащей, обвиняемой в совершении мошенничества	288
Мошенников в Хакасии стало больше	288
В Воронеже директор инновационной компании осужден за мошенничество на 5 млн. рублей	289
Навигатор	290
Банкротство физических лиц	290
Незаконные сделки с недвижимостью	292
Во Владимирской области направлено в суд уголовное дело в отношении «черных риелторов»	292
Башкортостане бывший землеустроитель осужден за махинации с муниципальными землями стоимостью около 5,8 млн рублей.....	292
В Краснодарском крае прокуратура направила в суд уголовное дело о хищении в Сочи земельного участка стоимостью более 9 млн рублей.....	292
Прокуратура Волгоградской области утвердила обвинительное заключение по уголовному делу в отношении членов организованной группы т.н. «черных риелторов»	293
Нецелевое использование бюджетных средств	294
В отношении министерства промышленности, транспорта и дорожного хозяйства Марий Эл возбуждено уголовное дело	294
В Крыму за нецелевое использование бюджетных средств оштрафованы три фонда...294	294
За нецелевое использование бюджетных средств оштрафуют на 200 тысяч рублей.....295	295
Финансовые пирамиды	296
В Чувашии будут судить бизнесмена за мошенничество на 93 миллиона рублей	296

В Самарской области перед судом предстанет создатель финансовой пирамиды, обещавший гражданам избавить их от кредитов.....	296
Мошенник похитил у граждан 52 млн рублей, обещая помощь в оформлении кредитов.....	296
Кооперативы проявили признаки пирамид.....	297
Организатора финансовой пирамиды КПК «ИД-Финанс», похитившего 48 млн руб., осудили в Ижевске.....	298
В Москве глава финансовой пирамиды обманул вкладчиков на 6 млн рублей.....	298
Финансовые пирамиды снова в моде.....	299
В Москве вынесен приговор по уголовному делу в отношении генерального директора «финансовой пирамиды», от деятельности которой пострадали 105 граждан.....	300
В Казани возобновлено рассмотрение дела о финансовых махинациях на 44 млн рублей.....	300
Российская полиция расследует 202 дела о финансовых пирамидах.....	301
Присвоение или растрата.....	302
В Тыве по материалам прокурорской проверки возбуждено уголовное дело о присвоении и растрате бюджетных средств.....	302
В Мурманской области перед судом предстанут сотрудники регионального ГУ МЧС России, обвиняемые в присвоении денежных средств в особо крупном размере.....	302
Коммерсантъ: "Генерал ФСИН получил к юбилею наручники".....	302
Бывшие руководители двух компаний подозреваются в присвоении акций одной из них.....	304
В Коми по материалам прокуратуры возбуждено уголовное дело о растрате 13 млн рублей при строительстве дома для переселения граждан из аварийного жилфонда.....	304
В Ставропольском крае вынесен приговор по факту присвоения свыше 6 миллионов рублей.....	304
В Москве направлено в суд уголовное дело в отношении президента ООО КБ «Огни Москвы», обвиняемой в растрате и мошенничестве.....	305
Финансовая разведка.....	306
Крот из финансовой разведки угрожает бизнесу.....	306
«Попадают подделки на уровне Гознака».....	307
В Росфинмониторинге состоялось совещание руководителей подразделений финансовых разведок стран СНГ.....	309
Расследования.....	311
Чайка разоблачил Навального.....	311
«Открытие» по выводу активов.....	313
Одни деньги можно украсть дважды.....	318
«Банк превратился в пирамиду и проедал сам себя».....	323
«Огни Москвы» осветят в особом порядке.....	328
Дело ЮКОСа: кто-то за это должен заплатить.....	329
«Был чемпионат мира по футболу, и диалог не получался».....	330
Теневой губернатор Свердловской области: часть 3 — бизнес-империя.....	331
Экс-главу фонда поддержки Воронежской академии искусств Светлану Шове подозревают в хищении 1,7 млн. рублей.....	335
Расхитителей кредитов в банке «Соотечественники» никто не ищет.....	336
Страховое мошенничество.....	338
Депутата обвинили в хищении субсидий по агрострахованию.....	338

Мошенники подменили документы о ДТП, получив страховую выплату на 163 тысячи рублей	338
Число мошеннических действий на рынке ОСАГО со стороны клиентов в 2015 г. выросло на 20% - РСА	338
«Страховая Компания Опора» предотвратила страховое мошенничество	339
Суд отказал родственникам погибших на борту лайнера А321 в получении полной компенсации	339
В 2015 году число страховых мошенников-клиентов на рынке ОСАГО выросло на 20%	341
Служба безопасности СК «Согласие» разоблачила деятельность аферистки, которая продавала фальшивые полисы КАСКО	341
"Агромошенника осудили на 5 лет и постановили вернуть страховщику 22,6 млн. руб.", "НСА"	342
Служба безопасности АО «Страховая Компания Опора» пресекла попытку страхового мошенничества в Ульяновске	342
ВСК предотвратила мошенничество на 68 млн руб.	342
Бывший следователь обвинен в страховом мошенничестве	343
25 миллиардов из карманов автолюбителей	343
Челябинец, обманувший страховые компании, прятался в Новосибирске	345
В Самаре раскрыта деятельность ОПГ, специализирующейся на страховом мошенничестве ¹	345
За попытку хищения у страховщиков 14 млн под суд пойдет участник ОПГ	346
Страховщики рассказали о мошенничестве в страховании	346
«ГУТА-Страхование» предотвратило мошенничество по автокаско	347
Как страховщики обманывают калининградцев, а водители — страховщиков	347
Нижегородцев предупреждают о мошенничестве с полисами ОСАГО	348
СК "Альянс" отбила 40 исков агромошенников на 1 млрд руб., новым атакам подвергся фонд гарантий НСА	349
На новый вид мошенничества попался житель Омутнинска	351
В Иркутске разыскивают мошенниц, выдающих себя за страховых агентов ¹	352
«Согласие» предотвратило мошенничество на 5 млн руб.	352
Судебная практика	353
Верховный суд разрешил арестовывать единственное жилье должников	353
В Тверской суд Москвы поступили материалы уголовного дела в отношении банкира и бывшего гендиректора хоккейного клуба "Спартак" Петра Чувиллина и экс-сотрудника УФСБ по Москве и Московской области Юрия Ярославцева	354
У жены ульяновского чиновника отобрали две дорогие квартиры	355
Тверской суд Москвы во вторник заключил под стражу президента Внешпромбанка Ларису Маркус по делу о мошенничестве	355
В Мещанском суде столицы 25 декабря продолжится слушание по одному из серии уголовных дел о хищениях в муниципальном Банке Москвы	355
Предпринимательница взыскивает со Сбербанка похищенные из хранилища €20 млн для руководства Украины	357
Столичный арбитраж рассмотрел иск вкладчика обанкротившегося банка "Российский кредит" против ЦБ	358
АСВ предложило ввести досудебные ограничения для владельцев проблемных банков	358
Юристы РФ разъяснили суду США свою позицию по взысканию \$50 млрд в счет экс-акционеров ЮКОСа	359
Кехман оспорил акт суда о реструктуризации долгов по иску Сбербанка	359

Дело "Яндекса" грозит Google потерей 7% выручки от оборота его магазина приложений и игр.....	360
Экс-руководитель филиала ВТБ объявлен в розыск по делу о хищении 1,1 млрд руб. ...	360
ВС встал на сторону ФНС по делу о трансграничных операциях "Орифлейм" на 600 млн руб.	361
Самарский арбитраж арестовал акции оператора "СМАРТС" по спору с МТС на \$35 млн	362
Советник правового отдела Минобороны осужден за присвоение столичных квартир на 260 млн руб.....	362
ВС оставил условно осужденных без загранпаспортов	363
Экс-сотрудник Минобороны РФ осужден за хищение свыше 40 квартир на 260 млн рублей	363
КС по запросу арбитражей вернул смягчающие обстоятельства для неплательщиков страховых взносов	364
"ЮТэйр" по решению суда выплатит \$3,2 млн дочерней структуре "ВТБ Лизинга"	364
Суд наказал компанию за конверт с деньгами от ее шефа в бумагах помощника прокурора ЮЗАО Москвы.....	365
Верховный суд Калмыкии заменил шурину Лужкова заключение на штраф	365
Верховный суд ограничил ответственность оценщиков за недостоверный отчет	366
Почему Верховный суд отменил санкцию для банка, который нарушил инструкции	367
Пять крупнейших арбитражных международных споров 2016 года.....	368
Экономколлегия ВС: Что ждет экс-гендиректора за отказ вернуть документы компании.....	370
Бизнесмен получил 5 лет условно за хищение имущества "БТА Банка"	371
Экономколлегия ВС: Исполнительное производство никак не влияет на конкуренцию ..	372
Незаконное получение и разглашение банковской и коммерческой тайны	374
Кому предоставляются сведения, составляющие банковскую тайну	374
Хищение денежных средств	376
"В деле о хищениях в судебной системе появился новый фигурант"	376
Дело инженера Минобороны, укравшего 14 млн с Восточного, ушло в суд.....	376
Задержан врио замдиректора ФСИН генерал-лейтенант Александр Протопопов.....	377
РКС выявила факт хищения 1,5 млрд рублей в Роскосмосе.....	377
В Хабаровском крае по материалам прокурорской проверки возбуждено уголовное дело по факту хищения более 7,2 млн рублей бюджетных средств при строительстве водозабора ..	378
В Омске по представлению прокуратуры заведующему отделением больницы за хищение путем мошенничества денежных средств у пациентов назначено более строгое наказание.....	378
В Брянске вынесен приговор по уголовному делу о хищении бюджетных средств на общую сумму около 23 млн руб.....	378
В Омске по материалам прокурорской проверки возбуждено уголовное дело по факту хищения из муниципального бюджета более 900 тысяч рублей	379
В Ульяновске перед судом предстанет главный бухгалтер двух муниципальных дошкольных образовательных учреждений, обвиняемый в хищении бюджетных средств	379
В Мурманской области направлено в суд уголовное дело по факту хищения свыше 45 млн рублей при строительстве жилого дома для молодых ученых.....	380
Задержан экс-руководитель филиала ВТБ, сбежавший от суда по делу о хищении 1 млрд руб.	380
В Красноярском крае полицейские доказали вину директора туристической фирмы в обмане клиентов	380

В Карелии бывший главный бухгалтер школы-интерната осуждена за хищение 3 млн рублей	381
В Москве задержали предпринимателя по подозрению в хищении 29 млн руб. бюджетных средств	381
В Алтайском крае направлено в суд уголовное дело о хищении на предприятии денежных средств под видом выплаченной заработной платы	381
В Свердловской области вынесен приговор мошеннику, похитившему 89 млн рублей у металлургического завода	382
В России появилась новая схема банковского мошенничества	382
Экс-банкир, обвиняемый в мошенничестве на миллиард, пойман в Москве	383
В Новгородской области вынесен приговор по уголовному делу о хищении из ювелирного магазина драгоценностей на сумму около 3 млн рублей	383
В Саратове осуждена уборщица коммерческой организации, которая обманным путем похитила у граждан почти 9 млн рублей	384
В Санкт-Петербурге перед судом предстанет бывший руководитель турагентства, обвиняемая в хищении денежных средств клиентов	384
ОПГ из Усть-Вымского района похитила более 200 тысяч рублей у жителей России	384
В Ульяновской области перед судом предстанет группа руководителей предприятия лесопромышленного комплекса, обвиняемых в хищениях на сумму более 24 млн рублей	385
В Татарстане бывший руководитель коммунального предприятия предстанет перед судом по обвинению в хищении бюджетных средств на сумму более 16 млн рублей	385
В Свердловской области по материалам прокурорской проверки возбуждено уголовное дело о хищении пенсионных накоплений с банковских карт пожилых людей и инвалидов, проживающих в доме-интернате	386
В Башкортостане директор строительной фирмы осужден за хищение 74 млн рублей под видом инвестирования в жилищное строительство	386
В Брянской области направлено в суд уголовное дело о хищении из федерального бюджета более 1,3 млн руб.	387
В Хабаровске осужден сотрудник авиакомпании, похищавший денежные средства за продажу билетов	387
Документы	388
Сведения о деятельности Следственного комитета Российской Федерации	388

Вниманию читателей!

Строки, выделенные цветом и подчеркнутые, являются активными гиперссылками.

Пользуйтесь ими для получения в Интернете оригиналов публикаций.

Безопасное ведение бизнеса и домохозяйства

21.12.2015

Зачем интернет-банку мониторинг контрагентов

Ольга Стаднийчук менеджер по развитию направления компании СКБ Контур

В 2015 году Альфа-Банк внедрил в свой интернет-банк «Альфа-Бизнес Онлайн» сервис проверки контрагентов. Перед отправкой платежа клиенты банка видят необходимую информацию о своих деловых партнерах и могут сберечь свои средства в случае потенциальной угрозы.

Задача: сделать интернет-банк единым функциональным окном

В 2014–2015 годах в банковских кругах витала идея «единого окна», когда в интернет-банке клиенту должны быть доступны все инструменты для ведения бизнеса: бухгалтерские программы, сервисы отправки отчетности и т. д. В результате на сайтах банков появились спецпредложения партнеров на базе агентских договоров. Клиенты не получили каких-то новых полезных возможностей, а партнеры не расширили объемы сбыта.

Следующим шагом стала интеграция ДБО и веб-бухгалтерий. Но несмотря на простоту идеи, реализация выливалась в пул громоздких мероприятий: диалог с вендорами платформ, бюджетирование разработки, согласование безопасности. Одно из самых главных препятствий состояло в том, что на старте было трудно спрогнозировать монетизацию.

Наибольший успех в этой области мог иметь проект, который бы обеспечивал максимальный синергетический эффект с точки зрения нужной пользователю функциональности и приносил бы банку дополнительный доход. Таким проектом стало внедрение в 2015 году в интернет-банк «Альфа-Бизнес Онлайн» сервиса проверки контрагентов от СКБ Контур.

Принципы работы

По данным экспертов, в последний год участились случаи, когда компании получали ущерб от фирм-однодневок и «плохой» дебиторской задолженности. Например, поставщику отправляют аванс, а он уже не может выполнить свои обязательства и не возвращает деньги. Причина потерь в том, что бизнес не владеет актуальной информацией о своих контрагентах. Чтобы компании могли регулярно и быстро проверять юрлица и ИП, с которыми работают, СКБ Контур разработал сервис для интернет-банков «Светофор». Он базируется на профессиональном веб-сервисе проверки контрагентов Контур.Фокус.

При загрузке платежных поручений в «Альфа-Бизнес Онлайн» сервис узнает ИНН контрагента и через API-шлюз обращается за данными о контрагенте в Контур.Фокус. В результате перед отправкой платежа клиент видит последние сведения о банкротствах, арбитражных делах, исполнительных производствах и другие важные факты о контрагентах. Сервис имеет понятную визуализацию в виде сигналов светофора, окрашенных в зависимости от важности обнаруженных данных. Кликнув по сигналу, клиент узнает информацию, которая может повлиять на его решение о платеже. Например, данные об арбитражах и сами арбитражные дела.

Также сервис анализирует директора и учредителей контрагентов на предмет «номинальности» и может порекомендовать установить надежный контакт с руководством компании. Так, сервис помогает избежать «плохой дебиторки», проблем с возвратом НДС и повысить информированность о контрагентах.

Результаты внедрения и эффективность

В Альфа-Банке отмечают, что сервис востребован среди клиентов — пользователей интернет-банка «Альфа-Бизнес Онлайн». Полезную опцию уже попробовали несколько тысяч юридических лиц.

Многие из них высоко оценили удобство «Светофора» и реальную пользу их бизнесу. Например, один из предпринимателей планировал перевести своему давнему контрагенту 1,5 млн рублей. Перед отправкой он увидел предупреждающий сигнал и решил не переводить деньги. Оказалось, что предприятие уже не может выполнить свои обязательства.

— Благодаря сервису экспресс-проверки контрагентов, который мы полгода назад внедрили в «Альфа-Бизнес Онлайн», десятки тысяч клиентов Альфа-Банка в онлайн-режиме узнают о последних важных фактах из жизни своих партнеров. Некоторым предпринимателям сервис уже помог предотвратить потерю средств. Вместе с СКБ Контур мы сделали классную и полезную фишу для бизнеса и очень этим довольны, — комментирует Петр Диденко, начальник управления развития электронных продуктов для корпоративных клиентов блока «Электронный бизнес» Альфа-Банка.

В ближайшие полгода СКБ Контур планирует внедрить сервис в нескольких федеральных и региональных банках, а в декабре 2015 г. стартуют первые решения вендоров банковских платформ: BSS (Юниаструмбанк) и iSimpleLab (Крайинвестбанк). Ожидается, в 2016 г. «Светофор» станет всеобщим гигиеническим инструментом при отправке платежей в интернет-банке.

// bankir.ru, 21 декабря 2015 № 1589320

[Финансы, банки №1589320](#)

Навигатор

Материалы по защите прав потребителей финансовых услуг



Информационные материалы по защите прав потребителей финансовых услуг были созданы одним из партнеров Проекта по повышению уровня финансовой грамотности жителей, компанией ПАКК, в 2015 году.

Материалы разработаны с учетом специфики восприятия целевых групп Проекта и прошли апробацию.

Брошюры, буклеты и плакаты распространяются с сентября 2015 года. В Калининградской области информационные материалы распространяются региональным управлением Роспотребнадзора, а также в образовательных и других социальных учреждениях. Плакаты добавлены в фотогалерею - в самом подвале страницы. Список макетов брошюр и буклетов в PDF-формате:

Файлы

- [Avtokredit_broschura.pdf](#)
- [Debetovaya karta_broschura..pdf](#)
- [Dobrovolnye pensionnye nakoplenya_broschura.pdf](#)
- [Ipotechniy kredit_broschura.pdf](#)
- [Kreditnaya karta_broschura.pdf](#)
- [Materialy dlya shkolnikov_broschura.pdf](#)
- [MFO_broschura.pdf](#)
- [OSAGO DSAGO avtokasko_broschura.pdf](#)
- [Plategnye uslugi_broschura.pdf](#)
- [Potrebitelskiy kredit_broschura.pdf](#)
- [Vklad i schet_broschura.pdf](#)
- [Avtokasko_buklet.pdf](#)
- [Avtokredit_buklet.pdf](#)
- [Banki vklady i kredity_buklet shkolniki.pdf](#)
- [Bankovskaya karta_buklet shkolniki.pdf](#)
- [Debetovaya karta_buklet.pdf](#)
- [Dobrovolnye pensionnye nakoplenya_buklet.pdf](#)
- [Ipotechniy kredit_buklet.pdf](#)
- [Kreditnaya karta_buklet.pdf](#)
- [MFO_buklet.pdf](#)
- [OSAGO DSAGO_buklet.pdf](#)
- [Pamyatka_zaemshchika_buklet.pdf](#)
- [Plategnye uslugi_buklet.pdf](#)
- [Potrebitelskiy kredit_buklet.pdf](#)
- [Strahovanie_buklet shkolniki.pdf](#)
- [Vklad i schet_buklet.pdf](#)

Источник: <http://fingram39.ru/projects/371-materialy-po-zashchite-prav-potrebiteley-finansovykh-uslug.html>

22.12.2015

Андрей Заикин: «Структурированные данные — основа информационной безопасности банка»

Андрей Заикин, руководитель направления информационной безопасности компании КРОК
Беседовал: Сергей Вильянов, редактор

Из опубликованного недавно отчета компании Veritas Technologies, получившего название Databerg Report 2015, следует, что IT-специалисты в российских организациях не имеют сведений о 53% данных, хранящихся на внутренних ресурсах, а 30,5% этих данных бесполезны для бизнеса. Это значит, что значительные ресурсы заняты, фактически, хранением цифрового мусора, среди которого могут обнаружиться разнообразные злоумышленники.

Что еще неприятнее, столь высокая доля неконтролируемого пространства корпоративной сети, которое может содержать конфиденциальные данные, часто становится свидетельством неэффективной работы IT-подразделения. О способах противодействия накоплению цифрового мусора и повышению безопасности данных в корпоративной сети мы говорили с Андреем Заикиным, руководителем направления информационной безопасности компании КРОК.

— На текущий момент IT-инфраструктуры компаний, особенно работающих долгие годы, очень разрослись. И в ходе этого роста в хранилищах накопились данные, историю появления которых уже никто не помнит. И что в них, собственно, содержится, тоже не всегда очевидно. Даже на уровне личных архивов отдельного сотрудника не всегда наблюдается упорядоченность, и этот сотрудник сам не может объяснить, что, собственно, хранится в файлах, созданных несколько лет назад. И актуальность хранимого под большим вопросом.

На уровне компании эта проблема встает в полный рост. Во-первых, ее хранилище используется неэффективно. В неструктурированных файловых «свалках» лежит очень странный набор информации, включающий музыку, фильмы, какие-то запускаемые файлы с торрентов и т. д. Среди этого может прятаться что-то действительно опасное. Или его там можно надежно спрятать до поры до времени.

Во-вторых, среди этих массивов данных может храниться (и утекать) конфиденциальная информация. Как известно, некоторые вещи с годами могут становиться лишь привлекательнее для третьих лиц.

— *Современные Авгиевы конюшни, в общем. С одной стороны, цена гигабайта сейчас такова, что мусор лежит почти бесплатно. С другой — иметь под боком неконтролируемую terra incognita не очень приятно. И как покорить эту целину?*

— Необходимо переводить информацию из неструктурированного вида в структурированный. Первый вариант — внедрять системы документооборота, благодаря которым появятся дополнительные метаданные — версионность, владелец, стадия согласования и т. д. Этот процесс движется параллельно развитию информационной индустрии и радикальных перемен не вносит.

Второй вариант — использовать специализированные системы, которые позволяют обеспечить комплексный подход к работе с неструктурированными данными. Такие системы разрабатывают несколько вендоров, например Varonis и Symantec. Класс таких систем называется Data Governance.

Здесь стоит оговориться, что есть системы управления правами доступа — Identity Access Management, Identity Access Governance — они регулируют доступ к корпоративным системам и ресурсам. Data Governance работает именно с неструктурированными данными и обладает особой функциональностью для эффективной работы с ними.

Прежде всего надо классифицировать данные по содержанию. Выяснить, есть в них что-то конфиденциальное или нет. Здесь помогает поиск по ключевым словам, например по номеру заведомо конфиденциального договора, по названиям компаний-партнеров, по автору документа. Также анализируется список пользователей, имеющих доступ к файловым ресурсам. Например, если папка закреплена за топ-менеджером, то в ней с большой вероятностью может храниться что-то важное, даже если к данным давно не обращались.

Исходя из таких эвристик, мы понимаем, что одни данные важны, другие — менее важны, но подлежат хранению (например, бухгалтерская отчетность за прошлые годы), а третьи — важности не имеют вовсе.

Отбор «неважных» данных — довольно кропотливое дело, потому, используя вроде бы очевидные признаки, можно легко ошибиться. Например, что делают видеофайлы большого объема в корпоративной сети? Можно ли их удалять? В большинстве случаев можно, но если видеоматериалы обнаруживаются, к примеру, в общей папке отдела маркетинга, то это нормальная ситуация. Скорее всего, они предназначены для решения рабочих задач. Но если в открытой папке лежат терабайты фильмов, церемониться не стоит.

Анализируется статистика доступа к файлам. Собираются все логи, по которым видно, какой пользователь и когда записал файлы, когда прочитал, в каких группах он находится, какие у него права. Исходя из этого, можно делать определенные выводы. Если человек записал некие данные и больше ни он сам, ни другие к ним не обращались, то, вероятнее всего, они неважны, особенно если прошло несколько лет. Можно обратиться к сотруднику и уточнить, что это. Или просто удалить сразу, если речь идет об avi-файле на 4 гигабайта.

— *И как это делать, вручную?*

— Такие системы есть в автоматизированном варианте, например Varonis Data Transport Engine, позволяющий переносить данные по определенным признакам на внешние накопители или просто удалять. Или можно делать это вручную, что, конечно, надежнее, но дольше.

Данные, которые вроде бы нужны, но крайне редко используются, лучше архивировать. Например, если к неким папкам больше года никто не обращался, их можно упаковать в архив. Всех сотрудников, имеющих к ним доступ, заранее предупреждают: если данные все же нужны, переместите их в актуальные папки или в личный архив.

Наконец, самые необходимые и востребованные данные необходимо тщательно структурировать и защищать. Мы особенно тщательно отслеживаем, кто к ним обращается и из каких отделов. Например, когда бухгалтерия имеет доступ к своей папке, это нормально. Но если права доступа к ней есть у рядового сотрудника IT-отдела, здесь уже нужно разбираться. Чтобы

расследовать этот потенциальный инцидент, мы смотрим статистику доступа: когда он последний раз обращался и что делал. Если он обращается каждый день напрямую в NTFS и читает все появляющиеся файлы, подозрения усиливаются. Если же обращение было единоразовым и случилось год назад, то, возможно, речь идет о случае техподдержки или восстановления данных из бэкапа. И права доступа уже не нужны.

Есть возможность автоматически отбирать потенциально лишние привилегии. Это может происходить как по причине долгого отсутствия обращений, так и из-за «непохожести» конкретного пользователя на тех, кто обычно имеет доступ к папке. Также можно установить системы, предоставляющие доступ к данным. И вместо того чтобы каждый раз писать заявку в IT-отдел, у нас будет один бизнес-пользователь, который понимает, какие данные хранятся и кому нужен к ним доступ. И он сам будет через специальный портал эти данные предоставлять. Конкретным людям и на заранее определенный срок. Это радикально снижает нагрузку IT-отдела. Но чтобы добиться этого, необходимо провести структурирование данных, о котором мы говорили в самом начале.

— *А какую банковскую специфику стоит отметить?*

— В банках доля ценных данных особенно высока. Их структуризация позволяет распределить информацию по накопителям различной скорости, самое важное — на самые быстрые и защищенные, остальные — на более объемные и дешевые. Также появляется возможность разместить определенные массивы данных ближе к их непосредственным потребителям, что особенно актуально при разветвленной филиальной сети. В частности, сейчас как раз ведем похожий проект для территориально распределенного банка, который пожелал навести порядок и усилить информационный контроль за региональными филиалами.

— *Хорошо, допустим, мы структурировали информацию, как нам теперь контролировать ее перемещение? Расскажите, пожалуйста, о подходах DLP и IRM. Какой из них более эффективен на практике?*

— Не секрет, что есть два подхода к борьбе с утечками. Первый — это решения класса Data Loss Prevention (DLP), и второй — Information Rights Management (IRM).

DLP изначально нацелено на защиту от непреднамеренных угроз, когда пользователь хочет отправить информацию наружу без злого умысла. Однако подкованный злоумышленник может, как правило, обойти такую систему.

IRM-система заточена против преднамеренных утечек. Информация, считающаяся конфиденциальной, упаковывается в контейнер, и доступ к ней есть только у проверенных пользователей, обладающих всеми правами. Но права доступа в IRM-системах, как правило, не регулируются, потому что их определяет владелец данных. И чем больше масштабы организации, тем больше времени требуется на настройку IRM. Поэтому есть смысл использовать DLP-системы для защиты всего массива данных от непреднамеренных утечек и IRM — только для конфиденциальной информации.

Но, еще раз повторяюсь, внедрение различных систем информационной безопасности практически невозможно, пока данные не структурированы. Нельзя просто купить некое решение, и оно все само как-то заработает. Нет, начинать надо именно со структурирования. Когда данные упорядочены, мы вольны выбирать между различными системами защиты.

— *В наступающем году у значительной части банков стоит задача не потратить деньги на что-то новое, а, скорее, сократить затраты. Как в это вписывается тема нашей беседы?*

— Много лет подряд банки могли себе позволить быстрое и дорогостоящее развитие систем. Теперь возможностей для этого поменьше. Но когда быстро растешь, не всегда есть время и средства уделять внимание мелким деталям. Сейчас мы видим, что клиенты из банковской сферы стали делать акцент не столько на покупку новых систем, сколько на систематизацию данных и выстраивание внутренних процессов. Да и уже купленные продукты можно настроить более вдумчиво.

Выгода от погружения в оптимизацию зависит от каждого конкретного случая. Но то, что хорошо отлаженные процессы и эффективно работающая система безопасности берегут деньги и снижают риски, это очевидно.

Мы предлагаем услуги по аудиту и описанию бизнес-процессов, связанных с управлением доступом к данным, даем рекомендации по изменениям и готовим соответствующие методики.

Также мы помогаем банкам внедрять соответствующие инструменты для работы с неструктурированными данными, с правами доступа, DLP и IRM-системы.

2016 год будет годом оптимизации затрат в сфере ИБ и IT. Навести порядок в данных необходимо. Это не только расчистит хранилище, но и снизит риски...

// bankir.ru, 22 декабря 2015 № 1592388

[Финансы, банки №1592388](#)

04.01.2016

Осторожно, мошенники! Как уберечь себя от обмана

Практически ежедневно граждане обращаются с заявлениями о мошенничестве. Особенность данного вида преступлений в том, что люди сами добровольно передают преступникам денежные средства, ценности, сообщают в полицию.

Мошенники, как правило, отличаются способностями психологического воздействия на жертву, красноречивостью, умением убедить в выгодности своих предложений. Часто им на руку оказывается жадность людей, желание без особого труда получить материальную выгоду (приобрести товар по выгодной цене, вложить средства под высокие проценты), либо наивность, малограмотность, отсутствие бдительности, осторожности и мягкосердечность. Во многих случаях в сети мошенников попадают пожилые люди.

Наиболее распространенными видами таких преступлений являются телефонные звонки с информацией о том, что родственник совершил ДТП, совершил преступление по неосторожности и во избежание привлечения его к уголовной ответственности необходима большая сумма денег, якобы для передачи сотрудникам полиции, прокуратуры, пострадавшему или его родственникам. При таких обращениях преступник стремится действовать быстро, напористо, не давая опомниться своей жертве, объясняя это нехваткой времени и тем, что спасти родственника через считанные минуты будет уже невозможно.

Рекомендуемые действия:

Ни в коем случае не сообщать о наличии наличных денег и никому не передавать их. Объяснить преступнику, что необходимо время для сбора, снятия с карты (счета) требуемой суммы. Можно пообещать перезвонить на его номер через несколько минут. Отключившись, немедленно сообщить о звонке в полицию. Для собственного успокоения сделать звонок своим родственникам, которые якобы попали в сложную ситуацию. При этом необходимо помнить, что если телефон родственника недоступен или не отвечает, то это не подтверждает правдивость и достоверность поступившего звонка. Дальнейшие действия согласовывать с полицией.

Часто граждане обращаются с заявлениями о том, что внесли крупные суммы в кредитно-потребительские кооперативы, где обещали высокую доходность, а на деле не возвращают даже внесенные средства. Об этом уже много говорили и писали, было множество примеров, но граждане продолжают верить в чудо и доверяют свои сбережения сомнительным предпринимателям. Чей-то пример о получении прибыли в этой организации не дает никакой гарантии выполнения обязательств перед вами. Сам принцип финансовых пирамид заключается в привлечении максимальных средств от вкладчиков, благодаря рекламе определенного круга лиц, которые реально получили доход. Это сродни игровому бизнесу, и каждый должен понимать, что жертвуя своими деньгами, он не получает никаких гарантий дохода, а шанс стать счастливым очень призрачный. Это доказали тысячи обращений в полицию пострадавших от мошенников, но и по сей день люди ждут чуда и сами ищут кому доверить свои сбережения, чтоб быстро разбогатеть. Остается напомнить, что чудеса бывают только в сказке, а в реалии от граждан продолжают поступать десятки заявлений о потерянных деньгах и несбывшихся мечтах.

В последнее время жулики активно используют интернет-ресурсы. Один из способов получения легких денег – введение в заблуждение пользователей одного из распространенных сайтов бесплатных объявлений. Очень удобный ресурс для тех, кто хочет что-то продать или купить, но и тут нельзя терять бдительность. Для примера один из распространенных способов, которыми пользуются мошенники. Совершают телефонный звонок гражданину о том, что планируют купить вещь, представленную в объявлении на сайте. Для гарантии серьезности своих намерений предлагают внести на банковскую карту продавца предоплату, для чего просят продиктовать номер и другие данные карты. Продавец в соблазне быстрой продажи и получения денег с удовольствием предоставляет требуемые данные. В последующем, пользуясь этими данными, мошенники снимают с карты все денежные средства, либо оплачивают товары или услуги с карты потерпевшего. Такие преступления заявляются практически ежедневно.

Так, 1 ноября текущего года в дежурную часть отдела поступило заявление гражданки, 1987 г.р., которую заинтересовало объявление о продаже автомобиля. Цена казалась заманчивой и авто подходящим. Созвонившись с продавцом, она согласилась сделать предоплату в сумме 10 тысяч рублей на указанный номер карты, чтоб забронировать покупку. Продавец обещал в ближайшее время пригнать машину и оформить сделку. Но после перечисления задатка номер телефона оказался заблокирован, а несостоявшаяся покупательница осталась один на один с нажитой проблемой.

2 ноября лишилась денежных средств в сумме 450 тысяч рублей еще одна гражданка, которая сообщила «покупателю» данные своей карты, по ранее поданному ею объявлению на Интернет-сайте о продаже козы. Коза вместо дохода принесла большой убыток, а деньги, как было установлено, «ушли» в Ульяновскую область.

Вывод: никогда никому не передавайте данные своей банковской карты, так как они могут быть использованы преступниками. Даже если вы пользуетесь услугами известных интернет магазинов с использованием банковской карты, то целесообразно иметь запасную карту, на которой размещен минимум средств, для проведения покупки.

Не обошли стороной наших горожан и мошенники, действующие через социальные сети. Взломав страничку пользователя и обнаружив там множество его друзей, всем им были разосланы письма с просьбой, в связи с возникшими проблемами, перечислить займы денежные суммы на указанный номер телефона либо интернет-кошелек. Естественно, нашлись друзья, готовые помочь материально в трудную минуту, и направившие свои кровные мошенникам. В последнее время участились случаи, когда потерпевшие, желая трудоустроиться, перечисляют денежные средства по объявлению с предложением работы. Практически все такие случаи заканчиваются визитом в полицию и утраченными крупными денежными суммами. Мнимый работодатель красочно описывает возможность трудоустройства в госучреждение (варианты - объект энергетики, предприятие на Севере), обещая высокую зарплату, полный соцпакет и т.д. Для осуществления мечты нужно всего лишь взять коньячка, колбаски и придти в учреждение, где его встретит работодатель. Название учреждения выбирается таким образом, что оно есть в любом городе или райцентре. Через пару минут следует звонок, что для решения вопроса надо срочно «забросить» денег на интернет (сотовый телефон), которые потом вернут. Иногда следует предложение через час перечислить затраченную сумму на карточку, для чего нужны реквизиты карты. В результате соискатель работы обнаруживает, что его в учреждении никто не ждет, номер «работодателя» не доступен, деньги пропали. Потерпевшему ничего не остается как обратиться в полицию и снять полученный стресс не востребованным коньячком с закуской. Как правило, оказывается, что звонки с предложением работы были сделаны из другого, отдаленного региона.

Часто обращаются граждане внесшие предоплату за поставку товаров и услуг (поставка сруба, стройматериалов, проведение монтажных и ремонтных работ и т.д.). В последующем товар не поставляется, услуги не оказываются и после месяцев ожидания и попыток самостоятельно вернуть перечисленные средства, неизбежно обращение за помощью в полицию. Вернуть деньги бывает сложно и не всегда возможно, тем более что часто заявитель передает деньги без оформления каких-либо расписок, лишь по устной договоренности. Вывод: не передавайте и не перечисляйте деньги за не оказанные услуги. Планируемые сделки оформляйте документально.

Достаточно часто значительные денежные суммы с банковских карт похищаются с использованием современных технологий, посредством распространения вирусных программ, которые позволяют мошенникам снимать средства со счетов абонентов, пользующихся мобильным банком. При этом по факту перечисления сумм с карты извещение мобильного банка об операции блокируется и не производится. Более уязвимы для таких вирусов устройства с операционными системами, которые установлены на большинстве сотовых телефонов. Имеющееся антивирусное обеспечение для средств мобильной связи далеко не всегда способно предотвратить такое вмешательство. Самый надежный выход – не пользоваться приложением «Мобильный банк», так как шансы возврата утраченных сумм практически близки к нулю.

Остается добавить, что большинство денежных средств, утраченных по халатности потерпевших, так и не удается вернуть. Преступные схемы связанные с интернетом, телефонными звонками, банковскими картами, как правило, реализуются из других регионов России. Для получения средств используются утраченные паспорта граждан и телефонные номера, а порой и банковские карты оформленные с их помощью. Это, к слову, должно стать предостережением от утери своих документов и бережное к ним отношение.

Наивно было бы полагать, что при выборе жертвы преступники пожалеют одинокую пожилую больную женщину или побоятся обокрасть состоятельного чиновника с большими полномочиями. Потерпевшим может стать каждый из вас или ваших родственников. Наш город – наш дом. Мы хотим, чтоб жить в нем было спокойно, удобно и комфортно, а значит и безопасно. Мы призываем всех граждан содействовать нам в этом, проявляя бдительность, разъясняя своим родственникам, знакомым, соседям какие угрозы существуют, как от них защититься, противостоять. Не оставайтесь безучастными в вопросах профилактики правонарушений и преступлений. Любую информацию о совершенных или готовящихся преступлениях незамедлительно предоставляйте в дежурную часть территориального отдела внутренних дел.

<http://www.magcity74.ru/news/28958-ostrozhno-moshenniki-kak-uberech-sebja-ot-obmana.html>

28.01.2016

В МВД по Чувашской Республике прошла пресс-конференция по теме: «Киберпреступления и телефонные мошенничества»

28 января в МВД по Чувашской Республике прошла пресс-конференция по теме: «Киберпреступления и телефонные мошенничества». С представителями республиканских и районных СМИ встретились руководители управления уголовного розыска, отдела «К» и

Чувашского отделения ПАО «Сбербанк». Заместитель начальника отдела управления уголовного розыска МВД по Чувашской Республике подполковник полиции Евгений Андреев рассказал о мошенничествах, совершаемых на территории республики. «В 2015 году на территории Чувашии совершено 1058 фактов мошенничеств, из них 102 факта в сельской местности. Чаще всего жертвами обмана становились жители Чебоксар, Новочебоксарска, Канаша, Алатырского и Чебоксарского районов», - рассказал Евгений Анатольевич. Об основных видах совершаемых мошенничеств рассказал начальник отделения по раскрытию мошенничеств общеуголовной направленности УУР МВД по Чувашской Республике старший лейтенант полиции Андрей Яблоков. По его словам, чаще всего жители республики становятся жертвами так называемых «социальных» мошенничеств (совершаются под видом социальных работников, снятия порчи, продажи меда) и хищений с использованием средств сотовой связи и сети Интернет. О преступлениях, связанных с хищением денежных средств с банковских карт, рассказал начальник отдела «К» МВД по Чувашской Республике подполковник полиции Александр Смирнов. «С начала года зарегистрировано 49 фактов списаний денежных средств с банковских карт граждан, из них 7 случаев с использованием вредоносного программного обеспечения, скачанного при открытии смс-сообщений с незнакомых номеров», - уточнил Александр Владимирович. Об основах безопасного пользования банковскими картами и мерах по противодействию мошенничеству рассказал начальник управления прямых продаж Чувашского отделения ПАО «Сбербанк» Евгений Слепенко. В завершении мероприятия выступающие ответили на вопросы журналистов.

Пресс-служба МВД по Чувашской Республике

Несколько правил работы с банковскими платежными картами:

Нельзя никому и никогда сообщать пин-код карты и реквизиты карты (номер карты, секретный код, срок действия карты и на кого она зарегистрирована);

Необходимо выучить пин-код либо хранить его отдельно от карты;

Нельзя передавать карту другим лицам – все операции с картой должны проводиться на Ваших глазах или вами лично;

Не разрешайте операторам принимающим платежи или кассирам в магазинах разглядывать вашу карту и после ее возвращения уберите ее немедленно с глаз;

При снятии денежных средств нужно стараться использовать только те банкоматы, которые расположены в безопасных местах и оборудованы системой видеонаблюдения и охраной. Такие банкоматы устанавливаются в государственных учреждениях, банках, крупных торговых центрах и т.д. в которых затруднен доступ к банкоматам (пропускная система) или находятся под круглосуточным наблюдением охраны;

Не выкидывайте чеки от банкомата у самого банкомата, по возможности старайтесь уничтожить чек;

Совершая операции с пластиковой картой в банкомате следите, чтобы рядом не было посторонних людей, обращайте внимание на картоприемник, клавиатуру и сам банкомат. Если они оборудованы какими-либо дополнительными устройствами и на них приклеены коробочки с рекламой, то от использования данного банкомата лучше воздержаться и сообщить о своих подозрениях по указанному на банкомате телефону;

При осуществлении покупок в сети Интернет не вводите дважды информацию с карты. В случае сбоя, после ввода первого раза обязательно проверяйте адрес сайта в строке браузера. В случае неуверенности правомочности сайта немедленно заблокируйте карту;

При осуществлении оплаты услуг через сеть Интернет обращайтесь внимание на начало адреса в адресной строке браузера в которой должен быть указан нарисованный замочек и символы <https://> обозначающий зашифрованный протокол обмена данными;

10. При поступлении звонков на телефон от имени сотрудников банка, которые просят вас сообщить им сведения о вас и реквизиты банковской карты не разговаривайте с ними и по возможности сообщите в правоохранительные органы о номере телефона с которого поступил звонок;

11. Если у Вас возникли вопросы по работе с картой, советуйтесь только с сотрудниками банка, никогда не прибегайте к помощи или советам третьих лиц при проведении операций с банковской картой;

12. В случае смены номера телефона, на который приходят уведомления о совершаемых банковских операциях, замените и номер уведомления в отделении банка;

13. Банковскую платежную карту, являющуюся «зарплатной» и имеющей овердрафт (кредитный лимит) старайтесь не использовать при покупках в магазинах и в сети Интернет, так как в случае кражи с нее денежных средств снимут всю сумму хранимых денег и весь лимит кредита;

14. В случае обладания банковской платежной картой и имея привязанный номер сотового телефона, исключите возможность использования сотового телефона для работы в сети Интернет и посещения различных сайтов, так как велика возможность получения на сотовый телефон

вредоносных программ, осуществляющих кражи денежных средств с банковских карт, по возможности пользуйтесь не бесплатными антивирусными программами;

15. Храните пароли для работы с услугой «Интернет-банкинг» в недоступном месте для посторонних лиц, в случае их утери немедленно сообщите в банк о блокировке доступа к личному кабинету услуги «Интернет-банкинг» и примите меры к смене всех ранее выданных или полученных паролей.

Памятка владельцам банковских карт

Банковская карта – это очень удобный способ хранения денежных средств и безналичной оплаты покупок в магазинах, кафе и в сети Интернет. Эти карты были придуманы и созданы для удобства населения в обращении с деньгами и для исключения использования наличных средств. И вместе с тем, владельцы банковских карт из-за своей невнимательности или незнания элементарных правил безопасности подвергают себя опасности и могут лишиться своих денежных средств. В последнее время увеличилось количество преступных посягательств на «содержимое кошельков» граждан, хранимое на банковских счетах и обслуживаемых посредством банковской платежной карты (карточный счет). В силу того, что банковская карта для банковского счета является неким ключом, позволяющим совершать практически все банковские операции со счетом (с денежными средствами), при этом, требуется только наличие самой карты и знание ее ПИН-кода, то это обстоятельство явилось причиной резкого возросшего внимания со стороны преступных элементов в отношении лиц, владеющих такими платежными картами и средств, хранимых на счетах, обслуживаемых с помощью них.

По информации отдела «К» МВД по Чувашской Республике

<https://21.mvd.ru/news/item/7137684/>

28.01.2016

МВД России по Тверской области советует, как уберечь себя от мошенничества в интернете

tverlife_news_

В настоящее время все более распространенным способом хищений денежных средств граждан становятся хищения с банковских пластиковых карт при помощи услуги «Мобильный банк».

Данному виду преступлений в основном подвергнуты клиенты крупных банков. При открытии счета гражданам предлагается услуга «Мобильный банк», а для ее отключения необходимо написать заявление, о чем не всегда предупреждают клиентов.

В настоящее время можно выделить три основных способа, при помощи, которых совершаются хищения денежных средств.

1. Способ «Классический». Данный способ можно назвать самым распространенным.

Потерпевшим при заключении договора указывается абонентский номер, который и подключается к «Мобильному банку». По различным причинам, многие владельцы пластиковых карт банков перестают в дальнейшем пользоваться абонентскими номерами (потерял, переехал, сменил оператора и т.д.), в связи, с чем оператор сотовой связи через шесть месяцев перевыпускает СИМ-карту с данным абонентским номером и выставляет ее на продажу.

После приобретения данной СИМ-карты новому абоненту продолжают поступать СМС-сообщения о движении денежных средств по карте предыдущего владельца СИМ-карты и, соответственно, остается возможность управлять данной картой через «Мобильный банк».

Возможностью перевести денежные средства на свой новый абонентский номер могут как лица, которые приобрели СИМ-карту для себя, предоставив для этого необходимый пакет документов, так и лица, которые скупают оптом СИМ-карты у недобросовестных представителей операторов сотовой связи, не оформляя их надлежащим образом, в том числе в различных регионах России.

2. Способ «Вредоносные программы»

2.1. Используется вредоносная программа, которая самостоятельно рассылает СМС - сообщения с телефона потерпевшего.

Данная программа устанавливается (попадает) на телефон при получении СМС или ММС сообщений, а так же при посещении различных Интернет сайтов.

Одним из признаков наличия вредоносной программы на мобильном телефоне может являться направление «пустых» СМС или ММС сообщений на номера телефонов, имеющих в разделе «Контакты» мобильного телефона. При открытии такого СМС или ММС происходит заражение телефона, который получил данное сообщение. Возможно получение потерпевшим СМС с номера «900» с различной информацией, которую он не запрашивал.

Выявить, что на телефоне установлена вредоносная программа, так же можно при помощи получения детализации телефонных звонков и СМС. В данном случае, при наличии вредоносной

программы в распечатке звонков, в разделе «Исходящие СМС» будут сообщения на номер «900», которые владелец телефона не направлял.

2.2. Используется платный сайт или платная программа в интернете

При помощи данной программы злоумышленником отправляется СМС с подменой (клонированием) номера на сервисный номер «900», т.е. при направлении сообщения указывается номер потерпевшего, и как в вышеуказанном способе, денежные средства переводятся на абонентский номер или на расчетный счет.

Отличие от вышеперечисленного способа в п.2.1. является отсутствие в распечатке детализации телефонных звонков и СМС, т.е. в разделе «исходящие СМС» с абонентского номера потерпевшего не будет сообщений на номер «900», а будут только ответные (входящие) СМС с данного номера.

3. Способ «Фишинговый сайт»

Данный способ возможен, когда потерпевший пользуется «Личным кабинетом» на интернет-сайте банка. Злоумышленниками создается (используется) сайт, адрес, которого и внешнее оформление идентичны официальному сайту банка. Если потерпевший при входе на сайт банка не использует сохраненную ссылку, а просто набирает название банка в поисковике, то ему обычно предлагается несколько вариантов. Если потерпевшим будет осуществлен вход на такой фишинговый сайт, и будут использованы свои данные для входа в личный кабинет банка (логин и пароль), то данной информацией и могут воспользоваться злоумышленники для входа в «Личный кабинет» на настоящем сайте банка от имени потерпевшего. Далее возможен перевод денег из «Личного кабинета» или подключение карты потерпевшего к услуге «Мобильный банк» на любой абонентский номер.

Основным признаком, что клиент зашел на фишинговый сайт является то, что после ввода логина и пароля на странице появляется надпись о техническом обслуживании сайта или любая иная информация, в которой будет указано о том, что обратиться на сайт можно позднее.

В настоящее время мошенники активно применяют способ, связанный с получением от потерпевшего информации о реквизитах карты, таких как номер, срок действия, CVC/CVV-код (трехзначный код на обратной стороне карты), а так же кодов для осуществления операции по получению логина и пароля системы Интернет-банкинга (например, «Сбербанк Онлайн», «Телебанк» и др.) под предлогом осуществления перевода денежных средств на счет потерпевшего в качестве предоплаты за приобретение продаваемого им товара, недвижимости, автотранспорта, услуг и т.д.

Получив данную информацию, злоумышленник получает доступ к системе интернет-банкинга, в которой, как правило, отражены все имеющиеся пластиковые карты и счета потерпевшего, далее через неё дополнительно подключает услугу мобильного банкинга на свой абонентский номер, а затем беспрепятственно осуществляет перевод денежных средств со всех данных счетов.

Чтобы не стать жертвой мошенников соблюдайте простые правила безопасности:

- не осуществляйте операций по переводу денежных средств на счета и телефонные номера неизвестных Вам лиц;
- не сообщайте незнакомым людям банковские реквизиты принадлежащих Вам пластиковых карт и счетов, свои паспортные данные, любые пароли, пин-коды и иную конфиденциальную информацию;
- перед подключением и использованием услуг интернет-банкинга и мобильного банкинга внимательно ознакомьтесь с условиями, правилами и особенностями предоставления данных услуг, а так же механизмом их действия.
- при блокировке своего абонентского номера у сотового оператора, в случае наличия подключенной услуги мобильного банкинга, обязательно отключите её через оператора горячей линии банка.
- не распространяйте в сети Интернет личную информацию о себе и своих близких.
- используйте для совершения покупок в сети Интернет только проверенные магазины и ресурсы.

<http://www.tverlife.ru/short-news/105247.html>

29.01.2016

Никогда не сообщайте посторонним лицам номер своей банковской карты!

В 2015 году в ОМВД России по г. Ельцу по-прежнему было зарегистрировано большое количество сообщений о преступлениях так называемых « в сфере телефонного мошенничества и компьютерной связи». В настоящее время мошенники прибегают к новым способам завладения денежными средствами, а именно совершения телефонных звонков по объявлениям размещенных на сайтах «Авито.ру, Авто.ру». Так, в ходе телефонного разговора мошенники сообщают, что готовы приобрести ту или иную вещь, которая соответственно размещена на сайте продаж. В ходе диалога недобросовестный покупатель просит прислать продавца номер

банковской карты на которую он желает перевести задаток в качестве оплаты товара, чтобы последний не передумал продать товар другому лицу. После этого лицо введенное в заблуждение с радостью сообщает мошенникам данные своей банковской карты и денежные средства уже через считанные минуты поступают в пользование мошенникам. Такие лица могут позвонить даже по самым невостребованным товарам только с одним умыслом — это хищение денежных средств. Не становится меньше сообщений о преступлениях, когда мошенники наоборот сами размещают товар и просят добросовестных покупателей перевести на их банковский счет или абонентский номер денежные средства. Поэтому просим жителей г. Ельца быть более бдительными в разговорах при продаже и покупке товаров через Интернет, сообщает прокуратура Ельца.

<http://trkelets.ru/news-51128.html>

29.01.2016

Надежно, как в Сбербанке: в Верхневолжье осудили специалиста по работе с клиентами

Ржевский городской суд вынес приговор сотруднице Сбербанка.

За хищение чужого имущества в крупном размере она получила наказание в виде лишения свободы на срок два года без штрафа и без ограничения свободы, условно с испытательным сроком в три года

В ходе рассмотрения уголовного дела установлено, что не позднее 25 сентября 2014 года у специалиста по обслуживанию частных лиц дополнительного офиса 8607/0202 Тверского отделения №8607 ОАО «Сбербанк России» возник и сформировался корыстный умысел, направленный на незаконное личное обогащение посредством систематического хищения вверенных ей денежных средств ОАО «Сбербанк России» путем их присвоения.

- С 25.09.2014 года до 09.12.2014 года гражданка Г., исполняя свои функциональные обязанности специалиста по обслуживанию частных лиц на своем рабочем месте в дополнительном офисе 8607/0202 Ржевского отделения Тверского отделения №8607 ОАО «Сбербанк России» в Ржеве, имея умысел на хищение вверенного ей имущества, руководствуясь корыстными побуждениями, незаконно систематически совершала хищение денежных средств ОАО «Сбербанк России», которые безвозмездно против воли собственника обращала в свою пользу, — сообщили в пресс-службе Ржевского городского суда.

За этот период сотрудница Сбербанка присвоила и потратила по своему усмотрению 303 826,43 руб., принадлежащие ОАО «Сбербанк России». Отказавшись от дачи показаний против себя в силу ст. 51 Конституции РФ, в судебном заседании вину она все же признала.

ОАО «Сбербанк России» по уголовному делу заявлен гражданский иск на сумму 303 826 рублей 43 копейки, подсудимая Г. согласилась с указанным гражданским иском. Иск был удовлетворен в полном объеме.

<http://www glavny.tv/news/12657>

30.01.2016

В Ульяновске полиция разыскивает женщину, похитившую в банке 5 млн рублей



В Ульяновске неизвестная женщина подозревается в хищении денежных средств, общая сумма которых составила пять миллионов рублей. Информацию об этом предоставили сотрудники управления МВД Российской Федерации по Ульяновской области.

Как известно из сообщений УМВД по Ульяновской области, данный инцидент произошел еще в середине октября прошлого 2015 года. В отделении "Сбербанка" на улице Хрустальной женщина, которой на вид не более 50 лет, предоставила сотрудникам финансового института подложные документы, в том числе и удостоверение личности. После этого неизвестная сняла со счета 57-летней женщины, не проживающей в настоящее время на территории Ульяновска, денежную сумму в размере пять миллионов рублей.

Затем нарушительница скрылась, но ее лицо успело попасть на камеры видеонаблюдения, установленные в банке.

Подозреваемая имеет худощавое телосложение, светлые волосы и выглядит не старше 40-50 лет. На момент совершения преступления женщина была одета в яркий шарф, покрывающий голову, темную дубленку, имела очки в черной оправе. Всех, кто осведомлен о местонахождении нарушительницы, просят сообщать в соответствующие структуры.

Лица Морская

31.01.2016

Памятка для граждан: Подозрительно низкая цена товара в Интернете

Один из популярных способов мошенничеств, основанных на доверии, связан с размещением объявлений о продаже товаров на электронных досках объявлений и интернет-аукционах. Как правило, мошенники привлекают своих жертв заниженными ценами, выгодными предложениями и требуют перечисления предоплаты путем перевода денежных средств на электронный кошелек.

Внимательно изучите объявление, посмотрите информацию о лице, разместившем его. Если торговая площадка имеет систему рейтингов продавцов, изучите отзывы, оставленные другими покупателями, не забывая о том, что преступники могут оставлять положительные отзывы о себе, используя дополнительные учетные записи.

Воспользуйтесь Интернет-поиском. Иногда достаточно ввести в форму поиска телефонный номер или сетевой псевдоним продавца для того, чтобы обнаружить, что эти данные уже использовались в целях хищения денежных средств и обмана покупателей.

Посмотрите среднюю стоимость аналогичных товаров. Слишком низкая стоимость должна вызвать у вас подозрение.

Если продавец требует перечислить ему на электронный счет полную или частичную предоплату за приобретаемый товар, подумайте, насколько вы готовы доверять незнакомому человеку.

Помните, что, перечисляя деньги незнакомым лицам посредством анонимных платежных систем, вы не имеете гарантий их возврата в случае, если сделка не состоится.

Пресс-служба МВД по Республике Тыва

<https://17.mvd.ru/news/item/7147941/>

31.01.2016

Полиция информирует граждан о том, как не стать жертвами мошенников

Нередко в полицию поступают сообщения от пожилых граждан о том, что путем обмана и злоупотребления доверием их деньгами завладели неизвестные преступники. Как правило, мошеннические схемы всегда одинаковы: это звонок по телефону с сообщением о происшествии с родственником, которого необходимо «откупить» от уголовной ответственности, или же преступники под видом работников социальных служб проникают в дом к пенсионерам и похищают денежные средства. Мошенники в корыстных целях пользуются доверчивостью пожилых граждан, обещая пенсионерам, ветеранам войны и труда произвести социальные выплаты, получить подарки, предлагают провести в их домах и квартирах льготный ремонт. Это один из наиболее распространенных способов обмана, конечной целью которого является хищение или получение денежных средств от потерпевших.

Полицейские в очередной раз напоминают жителям Ростовской области о бдительности и осторожности. Если незнакомцы представляются сотрудниками горгаза, ЖКХ, Министерства здравоохранения – попросите их предъявить документы, лучше всего – удостоверение. Прежде, чем запустить кого-то в дом, сделайте звонок в организацию, представителями которой назвались пришедшие, и уточните, отправляли ли к вам сотрудников.

Не оставляйте незнакомцев без присмотра, ни в коем случае не уходите в другую комнату. Не рассказывайте гостям о своих сбережениях, тем более не демонстрируйте их перед пришедшими. И обязательно закрывайте за нежданными посетителями дверь.

Если Вам звонят с сообщением, что ваш родственник или знакомый попал в аварию, в полицию, в больницу, и теперь за него нужно внести залог, штраф, взятку – одним словом, откупиться, это мошенники! Обязательно свяжитесь с родственниками или знакомыми! Не принимайте поспешных решений. О данных мерах предосторожности также необходимо регулярно напоминать своим пожилым родственникам во время семейных бесед.

Если вас или вашего пожилого родственника все же обманули – сразу же звоните по телефону дежурной части «02» или в отдел полиции вашего района. Чем быстрее вы это сделаете, тем выше возможность задержать злоумышленников и раскрыть преступление по «горячим следам».

Пресс-служба ГУ МВД России по Ростовской области

<https://61.mvd.ru/news/item/7148791/>

31.01.2016

Заражение телефона вирусом грозит потерей денежных средств с банковской карты

Вирусная программа попадает в смартфон через спам-рассылку смс-сообщений, содержащих различные ссылки. Если пользователь кликает на нее, то скачивается вредоносная программа, которая способна без участия абонента совершать операции с банковской картой. Пользователь даже не догадывается о том, что его телефон заражен, и с его счета списываются средства, так как вирусная программа полностью удаляет входящие SMS-уведомления от банка. В итоге деньги переходят на электронные кошельки злоумышленников.

Сотрудники полиции рекомендуют владельцам телефонов избирательно относиться к получаемой информации и не открывать незнакомые ссылки во входящих смс-сообщениях, будь то даже известные приложения. Также не следует скачивать приложения из непроверенных источников.

В целях профилактики заражения смартфонов необходимо регулярно обновлять антивирусы на своих телефонах. В противном случае вы рискуете занести в свой аппарат вирус и лишиться денежных средств с банковской карты.

В случае обнаружения факта хищения денежных средств необходимо обратиться в кредитную организацию для получения подробной выписки о движении ваших средств (с указанием адресата получения переводов) и заблокировать карту. У сотового оператора нужно получить детализацию соединений по номеру, на который подключена услуга «Мобильный банк», и с этими документами обращаться в полицию.

Пресс-служба МВД по Чувашской Республике

<https://21.mvd.ru/news/item/7148895/>

Номер подписан в свет 08.02.2016