**Тема: Информационная безопасность (ИБ).**

Любые данные находятся в памяти выч. системы, любое сообщение пересылаемая по сети и любой файл хранящиеся на каком либо носители.

По степени доступа различают информацию открытую и ограниченного доступа.

**К информации ограниченного доступа относятся:**

Конфиденциальная информация (государственная тайна, коммерческая тайна, служебная тайна, персональные данные и т д .).

Владелец, пользователь, собственник.

**В вопросах защиты информации применяются 2 термина:**

Информационная безопасность (ИБ) и защита информации (ЗИ), (оба произошли от Английского выражения Information Security.

**Под ИБ понимается теоретические вопросы и разработка, а под ЗИ - описание практических мероприятий.**

**ЗИ** - это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на него.

**Утечка** - это неконтролируемое распространение защищаемой информации путём её разложения или несанкционированного доступа к ней.

**Несанкционированный доступ** - это доступ (воздействие) с нарушением правил доступа, например взлом администраторской БД, внедрение вируса или подмена электронного документа.

**Непреднамеренное воздействие** - это воздействия на защищаемую информацию из за ошибок пользования, сбоя технических или программных средств, или иных нецеленаправленных действий.

 **Целью защиты информации является:**

предотвращение ущерба собственнику, владельцу и пользователю информации.

 **Политика безопасности -** это набор документальных норм, правил и практических приёмов, регулирующих управления, защиту и распределение информации ограниченного доступа.

**Характеристики информации применительно к задачам защиты.**

**К ним можно отнести:**

- статичность;

- размер и тип доступа;

- время жизни;

- стоимость создания;

- стоимость потери конфиденциальности;

- стоимость скрытого нарушения целостности;

- стоимость утраты.

**1) Статичность** - определяет может ли защищаемая информация меняться в процессе использования.

**2) Размер защищаемой информации** - может накладывать ограничения на средства защиты.

**3) Время жизни информации** - это тот период на протяжении которой она актуальна.

**4) Стоимость создания является** - денежным выражением совокупности всех затраченных ресурсов (временных, финансовых, человеческих).

**5) Стоимость потери конфиденциальности** - выражает убытки которые понесёт владелец информации, если к ней получат не авторизуемый доступ сторонние лица.

**6) Стоимость скрытого нарушения целостности** - выражает убытки, которые могут возникнуть в случае внесении изменения информации, если факт модификации не будет обнаружен.

**7) Стоимость утраты** - описывает ущерб от полного или частичного разрушения информации.

**ИБ** в условиях функционирования в России глобальных сетей.

**Уникальное положение в сети Интернет позволяет использовать её возможности в различных криминальных направлениях:**

 1) Среда для налаживания преступных контактов;

2) Среда для психологического воздействия;

3) Инструмент совершения право нарушения:

а) проникновение в кредитно - финансовую систему.

б) хищение электронной наличности.

в) нарушение авторских прав.

г) нелегальное получение товаров, услуг.

д) машинное поручение (нарушение).

е) нарушение законов связанных с ограничением азартных игр.

**Методы защиты информации.**

**Методы защиты информации (МЗИ) делятся на 3 большие классы:**

а) Законодательные;

б) Административные;

в) Технические.

**- Законодательные методы** - определяют кто и в какой форме должен иметь доступ к защищаемой информации, а так же какая будет ответственность за нарушение этого порядка, обычно правовые методы реализуются в виде законодательных актов.

**- Административные методы** - определяют процедуры доступа к защищаемой информации и строго следят за их выполнения.

Административные методы реализуются в рамках конкретного предприятия или организации их исполняет спец. обученный персонал.

-Технические методы защиты - призваны избавится от человеческого фактора.

В случае их применения, легитимный пользователь, получает лёгкий доступ к защищаемой информации, а перед злоумышленником ставится сложная, техническая (математическая, физическая) задача.

**Технич. методы делятся на 2 класса:**

1) Без математического обоснования стойкости (черный ящик).

2) С математическим обеспечением (криптография).

**Методы классификации распределяются по следующим признакам:**

**1)** **Препятствие** - метод физического преграждения пути злоумышленнику к информации;

**2) Управление доступом** - метод защиты с помощью регулирования использования информационных ресурсов системы;

**3) Маскировка** - метод защиты информации путём её криптографического преобразования;

**4) Регламентация** - метод защиты информации, создающий условия автоматизированный обработки, при которых возможности несанкционированного доступа сводится к минимуму.

**5) Принуждение** - метод защиты, при котором персонал вынужден соблюдать правила обработки, передачи и использования информации;

**6) Побуждения** - метод защиты, при котором пользователь побуждается не нарушать режимы обработки, передачи и использования информации за счёт соблюдения этических и моральных норм.

**Основными характеристиками защищаемой информации является:**

 конфиденциальность, доступность, и целостность.

**1) Конфиденциальность** - это известность содержания информации, только имеющим соответствием полномочием субъекта.

**2) Целостность информации** - это неизменность информации в условиях некорректного использования. (актуальность и непротиворечивость информации).

**3) Доступность** - эта возможность получении информации или услуги, за приемливого пользователя, для легитимных пользователей.

**Уязвимость информации** - это возможность возникновения на каком либо этапе жизненного цикла (ЖЦ) компьютерной системы, такого её состояния, при котором создаются условия для реализации угроз, безопасности информации.

**Атака** - это попытка реализации угрозы.

**Атака** - это действие предпринимаемые злоумышленником, которые заключается в поиске использования уязвимости информации.

**Угроза нарушения конфиденциальности** - это угроза утечки информации ограниченного доступа, хранящиеся в ИС или передается по каналам связи.

 **Угроза нарушения целостности** - это угроза преднамеренного воздействия хранения в ИС или передаваемых каналом связи.

**Нарушители делятся по одному из следующих критерий:**

1) Уровень из профильной подготовки противника и его возможностей (обычно пользователи, хакеры, правительственные агенты).

2) Тип доступа противника системы (внешний и внутренний).

3) Объем доступной противнику информации (общедоступная, внутренняя или корпоративная, закрытая).

4) Способы атаки, доступные противнику и наиболее часто применяемые им.

 Обычно пользователи не могут нанести серьёзный ущерб ИС, угроза представляет только внутренний доступ.

**Можно разбить 5 основных пользователей сети интернет:**

**Чайник** — это человек, который только начал делать свои первые шаги в мир информационных технологий. Главная его проблема — это боязнь. Именно страх мешает ему стать уверенным пользователем компьютера. Попробовать что-то новое, нажать на кнопку, подтверждающую удаление, — это целый стресс для него. На работе чайник становится насмешкой для коллег и системного администратора, и именно эти насмешки заставляют его перебороть свои страхи и стать юзером, и чем быстрее это произойдет — тем лучше! Все мы были (или и сейчас остаемся) чайниками, не нужно обижаться на это.

**Юзер** (с английского user — пользователь) — наверное, самая многочисленная часть компьютерного населения нашей планеты. Юзера можно сравнить с птицей, просидевшей часть своей жизни в клетке и неожиданно получившей свободу. Word и Excel у него уже больше не вызывают трудностей, Интернет переходит из разряда страшных легенд о вирусах в разряд неотъемлемой части его жизни. Жесткий диск потихоньку забивается хламом, без которого, как ему кажется, прожить невозможно. Это определение подходит к «юзеру обыкновенному», а кроме того, бывает «уверенный юзер» — к вышеописанным качествам у него добавляются средние знания «железа» и программного обеспечения, друзья его уважают, и иногда обращаются за советом.

**Ламер (любитель)** — это недохакер-переюзер, который обычно с умным видом объясняет то, в чем сам ни черта не соображает, у него даже нет в лексиконе слова «не знаю». Так что будьте уверены, обратившись к нему с любым вопросом — вы обязательно получите ответ, но вот стоит ли к нему прислушиваться, решать вам! Среднестатистический ламер обычно берется за все что угодно. Скажем, попалась ему на глаза статья по разгону процессора, он недолго думая засучивает рукава и берется за дело… Обычно это заканчивается внеочередным походом в компьютерный магазин за новой деталью, ну что же, отрицательный результат — тоже результат! Большинство ламеров очень любят чайников. Почему? Да просто нравится вешать им компьютерную лапшу на уши. **Хакер**. А как вы себе его представляете? Наверное так: маленький щупленький очкарик с выпученными глазами, вбивающий в тело программы зловещий код нового вируса? Наверное, бывают и такие, но вообще это довольно небольшая группа людей, состоящая в основном из недоучек компьютерных факультетов. Основной род их занятий — поиск уязвимостей и делание гадостей другим. В общем, это довольно умные ребята, и одному Богу известно, почему они выбрали именно такую самореализацию.

**Хакер** - Высококвалифицированный специалист , стремящиеся обойти защиту компьютерной системы, вне зависимости от того, получает ли он от этого коммерческую выгоду и преследуется ли по закону его действия.

**IT специалисты** (знатоки) — в эту группу входят самые различные подклассы, здесь и Web-мастера, и программисты, и системные администраторы, и инженеры-техники, общее у них лишь то, что они асы в своем деле. По статистике, это самые модные специальности, еще бы — как гласит одна мудрость: «Только IT-шник может попросить у шефа 100 долларов на память, и получить их» И напоследок хочу сказать: если когда-нибудь из ящика программиста вывалится книга «Windows для чайников» — не смейтесь над ним, ведь возможно он тоже когда-то искал клавишу «any key».
"Давным-давно, на заре всеобщей компьютаризации, многие программы после выполнения какого-либо действия ждали от юзера нажатия любой кнопки и даже писали это внизу экрана: "PRESS ANY KEY".
Умные юзеры открывали словари, переводили эту фразу и понимали, что им надо нажать клавишу ANY. После многочасовых исследований клавиатуры они эту клавишу не находили и начинали звать программиста. Программист приходил и каждый раз объяснял, что клавиша ANY - это ЛЮБАЯ клавиша. Постепенно компьютеров, а значит и юзеров, становилось все больше и вопросов, соответственно, тоже прибавлялось. Многие программисты озлобились и перестали общаться с юзерами, но нашлись люди, способные выдержать град глупости и даже найти на него ответ, понятный юзеру. По имени первого вопроса их и прозвали - ЭНИКЕЙЩИКИ. "

«Эникейщик» (от англ. any key — «любая клавиша» ) — очень востребованный «специалист» во времена появления и распространения персональных компьютеров в нашей стране, поскольку большинство пользователей обладало весьма слабыми познаниями в области английского языка, при виде надписи «press any key to continue…» приходило в замешательство и пыталось отыскать клавишу «any key», в таких ситуациях и приходил на помощь пользователю наш «специалист» . Надпись «press any key to continue…» выводилась на экран в тех же случаях как и сегодня надпись «далее» («next»).
**Каналы утечки информации:**

Выделяют 2 - больших класса каналов утечки информации:

1) Непосредственные - которые предполагает физический доступ к элементам информационной системы (ИС).

2) Косвенные - которые не требует физического доступа к информационной системе.

 Ко 2 - му виду относятся различные виды разведки ( видеонаблюдение, прослушивание, электромагнитные наводки).

Непосредственные каналы делятся на:

 1) 1-й тип - Не требующие изменение элементов ИС:

а) хищение носителей информации;

б) сбор производственных отходов с информацией;

в) намеренное копирование файлов;

г) чтение остаточной информации после работы другого пользователя;

д) намеренное использование незаблокированных терминалов других пользователей;

е) маскировка под других пользователей;

ж) обход средств разграничения доступа.

2) 2-й тип - Предполагающие изменения элементов ИС:

а) незаконное подключение специальной регистрацией аппаратуры к устройствам связи;

б) злоумышленное изменение программ для выполнения или несанкционированного копирования информации при её обработке;

в) злоумышленный вывод из строя средств защиты информации.

**Классификация атак:**

Существует несколько классификаций, каждая из которых учитывает определенный фактор.

Наиболее распространенные следующие:

1) По месту возникновения:

а) локальные;

б) удаленные или сетевые;

2) По воздействию на ИС:

а) активные;

б) пассивные.

3) По направленности:

а) атака на уровне ОС;

б) атака на уровне сетевого ПО;

в) атака на уровне СУБД.

Защитой СУБД является одной из основных задач, так как:

1) БД имеет четкую структуру;

2) Обычно СУБД имеют ограниченный набор базовых операций;

3) При правильном администрировании БД будет жестко контролировать правила доступа.

**Основные функционирования глобальной сети Интернет.**

**ПАМЯТКА**

**«О МЕРАХ БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ БАНКОВСКИХ КАРТ»**

Итак, с созданием в 1993году первого широко загруженного Интернет-браузера Mosaic, который сделал Интернет доступным не только для узких специалистов-технарей, но и другому любому пользователю, началась новая эра в истории Интернета. В том же переломном 1993 году и Белый Дом, и даже Организация Объединенных Наций впервые вышли в онлайн, положив таким образом начало доменных имен .gov и .org.

С технической точки зрения **Интернет** - это всемирное объединение компьютерных или локальных сетей различных предприятий.

Что касается наполнение интернета, что сегодня наиболее популярны, такие ресурсы как электронная почта, телеконференции и всемирная паутина.

Тогда же в 1995 г. стали появляться первые Интернет магазины.

Одним из более популярных является ставший Амазон. ру.

За 2012 год количество пользователей в России достигало 60 млн. человек (IP адресов), а по всему Миру более 2 млд. человек.

Интернет стал универсальной деловой средой соединяющий компании друг с другом и со всей потребительской аудиторией.

Среди функции электронной коммерции можно выделить следующие:

1) Реклама; 2) Представление товара; 3) Провидение покупки; 4) После продажное обслуживание;

5) Налаживание долгосрочные отношения с клиентами.

**Интернет экономика:**

1) Доминирует знание и отношение людей;

2) Капитал - продукт потребления;

3) Инновации - достояние ответственности;

4) Электронные средства, общение между людьми.

Виртуальные магазины наиболее близки к нашей обыденной жизни и поэтому привлекают внимание в первую очередь.

Реальный же бизнес лежит в сфере "Бизнес - бизнес".

Достаточно сказать что на закупках при помощи интернета корпорации могут с экономить до 30%.

Очевидно что потенциал Бизнес - бизнес на много выше, потенциала розничной торговли.

**Сетевой маркетинг (Маркетинг в интернете)** - под маркетингом обычно понимается изучение рынка для размещения продукта, определение цены, вероятных покупателей.

**Платёжные системы в Интернете.**

Способы расчетов принимаемые для оплаты Рос. юр. лицами за приобретенные товары в Интернете, можно разделить на следующие группы:

1) Расчеты вне электронной сети.

2) Расчеты в рамках электронной сети.

К 1 -й категории относятся оплата наличными, по факту доставки (наличными).

Ко 2-й категории относятся прежде всего оплата на основании выставленного счета (банковый перевод).

**Безопасность систем платежей** - является важнейшим параметром жизнеспособности электронных систем платежей.

На сегодняшний день в банке пользуются так называемые платформенные протокола безопасных электронных сделок. (SAT).

Здесь речь идет о защите электронной подписью, так называемой криптацией.

Электронные деньги отвечают также всем признакам кредитных денег, к которым можно отнести:

1) Срочность.

2) Гарантированность.

3) Использование функции средства обращения или средств платежа.

4) Возвратность.

5) Разменность.

**ПАМЯТКА**

**«О МЕРАХ БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ БАНКОВСКИХ КАРТ»**

Соблюдение рекомендаций, содержащихся в Памятке, позволит обеспечить максимальную сохранность банковской карты, ее реквизитов, ПИН и других данных, а также снизит возможные риски при совершении операций с использованием банковской карты в банкомате, при безналичной оплате товаров и услуг, в том числе через сеть Интернет.

# Меры безопасности при пользовании банковскими картами

* Храните свою карту в недоступном для окружающих месте. Не передавайте карту другому лицу, за исключением продавца (кассира). Рекомендуется хранить карту отдельно от наличных денег и документов, особенно в поездках.
* Во избежание мошенничества с использованием Вашей карты требуйте проведения операций с ней только в Вашем присутствии, не позволяйте уносить карту из поля Вашего зрения.
* Если к вам обратились по телефону, в интернете, через социальные сети или другими способами, и под различными предлогами пытаются узнать данные о вашей банковской карте, пароли или другую персональную информацию, будьте осторожны: это явные признаки мошенничества. При любых сомнениях рекомендуем прекратить общение и обратиться в банк по телефону, указанному на обратной стороне вашей банковской карты.
* Не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении операций. При необходимости обратитесь к сотрудникам в филиале банка или позвоните по телефонам, указанным на устройстве или на обратной стороне Вашей карты.
* Уничтожайте чеки с паролями от систем интернет-банка, если Вы не планируете их использование. Не передавайте чеки третьим лицам, в т.ч. сотрудникам банка.
* Во избежание использования Вашей карты другим лицом храните ПИН-код отдельно от карты, не пишите ПИН-код на карте, не сообщайте ПИН-код другим лицам (в том числе родственникам), не вводите ПИН-код при работе в сети Интернет.

**Общие рекомендации**

1. Никогда не сообщайте ПИН третьим лицам, в том числе родственникам, знакомым, сотрудникам кредитной организации, кассирам и лицам, помогающим Вам в использовании банковской карты.

2. ПИН необходимо запомнить или в случае, если это является затруднительным, хранить его отдельно от банковской карты в неявном виде и недоступном для третьих лиц, в том числе родственников, месте.

3. При получении банковской карты распишитесь на ее оборотной стороне в месте, предназначенном для подписи держателя банковской карты, если это предусмотрено. Это снизит риск использования банковской карты без Вашего согласия в случае ее утраты.

4. Будьте внимательны к условиям хранения и использования банковской карты. Не подвергайте банковскую карту механическим, температурным и электромагнитным воздействиям, а также избегайте попадания на нее влаги. Банковскую карту нельзя хранить рядом с мобильным телефоном, бытовой и офисной техникой.

5. С целью предотвращения неправомерных действий по снятию всей суммы денежных средств с банковского счета целесообразно установить суточный лимит на сумму операций по банковской карте и одновременно подключить электронную услугу оповещения о проведенных операциях (например, оповещение посредством SMS-сообщений или иным способом).

6. При получении просьбы, в том числе со стороны сотрудника кредитной организации, сообщить персональные данные или информацию о банковской карте (в том числе ПИН) не сообщайте их. Перезвоните в кредитную организацию - эмитент банковской карты (кредитную организацию, выдавшую банковскую карту) и сообщите о данном факте.

7. Не рекомендуется отвечать на электронные письма, в которых от имени кредитной организации (в том числе кредитной организации - эмитента банковской карты (кредитной организации, выдавшей банковскую карту)) предлагается предоставить персональные данные. Не следуйте по "ссылкам", указанным в письмах (включая ссылки на сайт кредитной организации), т.к. они могут вести на сайты-двойники.

8. Помните, что в случае раскрытия ПИН, персональных данных, утраты банковской карты существует риск совершения неправомерных действий с денежными средствами на Вашем банковском счете со стороны третьих лиц.

В случае если имеются предположения о раскрытии ПИН, персональных данных, позволяющих совершить неправомерные действия с Вашим банковским счетом, а также если банковская карта была утрачена, необходимо немедленно обратиться в кредитную организацию - эмитент банковской карты (кредитную организацию, выдавшую банковскую карту) и следовать указаниям сотрудника данной кредитной организации. До момента обращения в кредитную организацию - эмитент банковской карты Вы несете риск, связанный с несанкционированным списанием денежных средств с Вашего банковского счета.

**Рекомендации при совершении операций**

**с банковской картой в банкомате**

1. Осуществляйте операции с использованием банкоматов, установленных в безопасных местах (например, в государственных учреждениях, подразделениях банков, крупных торговых комплексах, гостиницах, аэропортах и т.п.).

2. Не используйте устройства, которые требуют ввода ПИН для доступа в помещение, где расположен банкомат.

3. В случае если поблизости от банкомата находятся посторонние лица, следует выбрать более подходящее время для использования банкомата или воспользоваться другим банкоматом.

4. Перед использованием банкомата осмотрите его на наличие дополнительных устройств, не соответствующих его конструкции и расположенных в месте набора ПИН и в месте (прорезь), предназначенном для приема карт (например, наличие неровно установленной клавиатуры набора ПИН). В указанном случае воздержитесь от использования такого банкомата.

5. В случае если клавиатура или место для приема карт банкомата оборудованы дополнительными устройствами, не соответствующими его конструкции, воздержитесь от использования банковской карты в данном банкомате и сообщите о своих подозрениях сотрудникам кредитной организации по телефону, указанному на банкомате.

6. Не применяйте физическую силу, чтобы вставить банковскую карту в банкомат. Если банковская карта не вставляется, воздержитесь от использования такого банкомата.

7. Набирайте ПИН таким образом, чтобы люди, находящиеся в непосредственной близости, не смогли его увидеть. При наборе ПИН прикрывайте клавиатуру рукой.

8. В случае если банкомат работает некорректно (например, долгое время находится в режиме ожидания, самопроизвольно перезагружается), следует отказаться от использования такого банкомата, отменить текущую операцию, нажав на клавиатуре кнопку "Отмена", и дождаться возврата банковской карты.

9. После получения наличных денежных средств в банкомате следует пересчитать банкноты полистно, убедиться в том, что банковская карта была возвращена банкоматом, дождаться выдачи квитанции при ее запросе, затем положить их в сумку (кошелек, карман) и только после этого отходить от банкомата.

10. Следует сохранять распечатанные банкоматом квитанции для последующей сверки указанных в них сумм с выпиской по банковскому счету.

11. Не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении операций с банковской картой в банкоматах.

12. Если при проведении операций с банковской картой в банкомате банкомат не возвращает банковскую карту, следует позвонить в кредитную организацию по телефону, указанному на банкомате, и объяснить обстоятельства произошедшего, а также следует обратиться в кредитную организацию - эмитент банковской карты (кредитную организацию, выдавшую банковскую карту), которая не была возвращена банкоматом, и далее следовать инструкциям сотрудника кредитной организации.

**Рекомендации при использовании банковской карты**

**для безналичной оплаты товаров и услуг**

1. Не используйте банковские карты в организациях торговли и услуг, не вызывающих доверия.

2. Требуйте проведения операций с банковской картой только в Вашем присутствии. Это необходимо в целях снижения риска неправомерного получения Ваших персональных данных, указанных на банковской карте.

3. При использовании банковской карты для оплаты товаров и услуг кассир может потребовать от владельца банковской карты предоставить паспорт, подписать чек или ввести ПИН. Перед набором ПИН следует убедиться в том, что люди, находящиеся в непосредственной близости, не смогут его увидеть. Перед тем как подписать чек, в обязательном порядке проверьте сумму, указанную на чеке.

**Рекомендации при совершении операций с банковской**

**картой через сеть Интернет**

1. Не используйте ПИН при заказе товаров и услуг через сеть Интернет, а также по телефону/факсу.

2. Не сообщайте персональные данные или информацию о банковской(ом) карте (счете) через сеть Интернет, например ПИН, пароли доступа к ресурсам банка, срок действия банковской карты, кредитные лимиты, историю операций, персональные данные.

3. С целью предотвращения неправомерных действий по снятию всей суммы денежных средств с банковского счета рекомендуется для оплаты покупок в сети Интернет использовать отдельную банковскую карту (так называемую виртуальную карту) с предельным лимитом, предназначенную только для указанной цели и не позволяющую проводить с ее использованием операции в организациях торговли и услуг.

4. Следует пользоваться интернет-сайтами только известных и проверенных организаций торговли и услуг.

5. Обязательно убедитесь в правильности адресов интернет-сайтов, к которым подключаетесь и на которых собираетесь совершить покупки, т.к. похожие адреса могут использоваться для осуществления неправомерных действий.

6. Рекомендуется совершать покупки только со своего компьютера в целях сохранения конфиденциальности персональных данных и (или) информации о банковской(ом) карте (счете).

В случае если покупка совершается с использованием чужого компьютера, не рекомендуется сохранять на нем персональные данные и другую информацию, а после завершения всех операций нужно убедиться, что персональные данные и другая информация не сохранились (вновь загрузив в браузере web-страницу продавца, на которой совершались покупки).

7. Установите на свой компьютер антивирусное программное обеспечение и регулярно производите его обновление и обновление других используемых Вами программных продуктов (операционной системы и прикладных программ), это может защитить Вас от проникновения вредоносного программного обеспечения.

**Как защититься от мошенников?**

АКБ «Алмазэргиэнбанк» ОАО рекомендует всем владельцам пластиковых карт следовать правилам безопасности:

**ПИН-КОД – КЛЮЧ К ВАШИМ ДЕНЬГАМ**
Никогда и никому не сообщайте ПИН-код Вашей карты. Лучше всего его запомнить. Относитесь к ПИН-коду как к ключу от сейфа с Вашими средствами. Набирая ПИН-код, прикрывайте клавиатуру рукой.
Нельзя хранить ПИН-код рядом с картой и тем более записывать ПИН-код на карту – в этом случае Вы даже не успеете обезопасить свой счёт, заблокировав карту после кражи или утери.

**ВАША КАРТА – ТОЛЬКО ВАША**
Не позволяйте никому использовать Вашу пластиковую карту – это всё равно что отдать свой кошелёк, не пересчитывая сумму в нём.

**НИ У КОГО НЕТ ПРАВА ТРЕБОВАТЬ ВАШ ПИН-КОД**
Если Вам позвонили из какой-либо организации, или Вы получили письмо по электронной почте (в том числе из банка) с просьбой сообщить реквизиты карты и ПИН-код под различными предлогами, не спешите её выполнять. Ни одна организация, включая банк, не вправе требовать Ваш ПИН-код. Не переходите по указанным в письме ссылкам, поскольку они могут вести на сайты-двойники. Помните: хранение реквизитов и ПИН-кода в тайне – это Ваша ответственность и обязанность.

**НЕМЕДЛЕННО БЛОКИРУЙТЕ КАРТУ ПРИ ЕЕ УТЕРЕ**
Если Вы утратили карту, срочно свяжитесь с банком по тел: 34-22-22 или 8-800-100-34-22, сообщите о случившемся и следуйте инструкциям сотрудника банка. Для этого держите телефон банка в записной книжке или в списке контактов Вашего мобильного телефона.

**ПОЛЬЗУЙТЕСЬ ЗАЩИЩЁННЫМИ БАНКОМАТАМИ**
При проведении операций с картой пользуйтесь только теми банкоматами, которые расположены в безопасных местах и оборудованы системой видеонаблюдения и охраной: в государственных учреждениях, банках, крупных торговых центрах и т.д. Граждане, пользующиеся банкоматами без видеонаблюдения, могут подвергнуться нападениям злоумышленников.

**ОПАСАЙТЕСЬ ПОСТОРОННИХ**
Совершая операции с пластиковой картой, следите, чтобы рядом не было посторонних людей. Если это невозможно, снимите деньги с карты позже, либо воспользуйтесь другим банкоматом. Набирая ПИН-код, прикрывайте клавиатуру рукой. Реквизиты и любая прочая информация о том, сколько средств Вы сняли, и какие цифры вводили в банкомат, могут быть использованы мошенниками.

**БАНКОМАТ ДОЛЖЕН БЫТЬ «ЧИСТЫМ»**
Обращайте внимание на картоприемник и клавиатуру банкомата. Если они оборудованы какими-либо дополнительными устройствами, то от использования данного банкомата лучше воздержаться и сообщить о своих подозрениях по указанному на нём телефону.

**СОВЕТУЙТЕСЬ ТОЛЬКО С БАНКОМ**
Никогда не прибегайте к помощи либо советам третьих лиц при проведении операций с банковской картой в банкоматах. Свяжитесь с банком – мы предоставим консультацию по работе с картой. Телефон указан на оборотной стороне карты.

**НЕ ДОВЕРЯЙТЕ КАРТУ ОФИЦИАНТАМ И ПРОДАВЦАМ**
В торговых точках, ресторанах и кафе все действия с Вашей пластиковой картой должны происходить в Вашем присутствии. В противном случае Вы можете, подвергнуты мошенническим действиям со стороны персонала: сканирование реквизитов. Вашей карты при помощи специальных устройств и использовать их в дальнейшем для изготовления подделки.