**Способы защиты от преступлений, совершаемых с использованием ИТ-технологий**

Развитие информационных технологий достигло высокого уровня, в связи с чем большинство сфер жизни стало немыслимым без их использования. Указанное повлияло также и на способы совершения преступлений.

Как правило, к категориям преступлений, которые могут быть совершены с использованием ИТ-технологий относят мошенничество (ст. 159, ст. 159.3, ст. 159.6 Уголовного кодекса) и кражи (ст. 158 УК РФ).

Если преступление уже совершено, эффективность его расследования зависит от своевременности обращения в компетентные правоохранительные органы и от первичной фиксации следов преступления.

У организаций, которые работают с данными клиентов, есть системы хранение информации о том, кто, откуда и с каких адресов заходит в сервис, какими телефонами пользовался для доступа. Эту информацию важно сохранять для того, чтобы можно было восстановить цепочку действий. Правоохранительные органы в случае происшествия запрашивают такую информацию.

В ситуации, когда совершенное преступление связано с хищением денежных средств, потерпевшему необходимо получить выписку из своего банка с подтверждением факта перевода денежных средств и указанием реквизитов лица, их получившего.

Также необходимо зафиксировать все точки соприкосновения и взаимодействия с преступниками – адрес сайта и электронной почты, номер телефона, физический адрес офиса. При этом в случаях, где мошенничество связано с хищением денежных средств или конфиденциальной банковской информации, самым первым шагом должен быть звонок обслуживающему банку и блокировка карт. Чем раньше банк будет уведомлен о произошедшем неправомерном списании денежных средств, тем больше шансов, что он сможет оказать содействие клиенту на дальнейших этапах.

**Чтобы не оказаться жертвой мошенников необходимо знать следующее:**

– сотрудники любого банка никогда не просят сообщить данные вашей карты (номер карты, срок её действия, секретный код на оборотной стороне карты), так как у них имеются ваши данные;

– хранить пин-код отдельно от карты, ни в коем случае не писать пин-код на самой банковской карте;

– не сообщать пин-код третьим лицам;

– лучше избегать телефонных разговоров с подозрительными людьми, которые представляются сотрудниками банка;

– внимательно читайте СМС сообщения приходящие от банка;

– никогда и никому не сообщайте пароли, и секретные коды, которые приходят вам в СМС сообщении от банка;

– сотрудники банка никогда не попросят вас пройти к банкомату;

– никогда не переводите денежные средства, если об этом вас просит сделать ваш знакомый в социальной сети, возможно мошенники взломали аккаунт, сначала свяжитесь с этим человеком и узнайте действительно ли он просит у вас деньги;

– в сети «Интернет» не переходите по ссылкам на неизвестные сайты.