- возможность многоразового использования (при чтении неограниченное число раз, при перезаписи до 100 000 раз);

- высокая надежность хранения информации (информация на карте не подвержена воздействию внешних полей и может храниться до 10 лет);

- высокая степень защиты от подделок (карточку практически невозможно подделать);

-возможная многофункциональность бесконтактных пластиковых карт (карточки могут нести большой объем перезаписываемой информации и использоваться одновременно для целого ряда приложений).

Однако данная технология имеет некоторые ограничения, связанные с безопасностью данной системы. Во-первых, платежные терминалы должны поддерживать технологию бесконтактного обмена информацией.

Во-вторых, многие банковские или платежные системы искусственно ограничили сумму платежа на уровне примерно 20 – 30 долларов в зависимости от страны. Хотя сумма *транзакции* не ограничена, при суммах, превышающих лимит, требуется вводить PIN – код, но *сам платеж в любом случае осуществляется бесконтактно.*

В Республике Беларусь выпускаются бесконтактные карты типа PayPass (платежная система - MasterCard) и PayWave (платежная система – VISA). По принципу действия они аналогично друг другу. Возможность покупок без PIN кода ограничена суммой до 200 000 BYR для карточек MasterCard и до 230 000 BYRдля карточек Visa.

Представляя определенное удобство пользователю бесконтактной карты, технология бесконтактных платежей имеет и определенные недостатки. Основным недостатком бесконтактной платежной карты является возможность незаконногоснятия денежных средств при помощи специального оборудования, Данные, передаваемые с бесконтактных карт, могут быть похищены с расстояния в 50 сантиметров. К такому выводу пришли исследователи из Суррейскогоуниверситета в Великобритании. Ученые подчеркивают, что расстояние в четыре с лишним раза превышает предусмотренную создателями дистанцию для считывания. Представители университета заявляют, что таким способом как минимум можно получить информацию о платеже.

В то же время Ассоциация производителей карт Великобритании заявляет, что такая возможность не представляет угрозы, поскольку мошенники не сумеют собрать достаточно данных, чтобы совершить хищение средств.Однако все не так просто, ведь мошенникам кроме терминала нужно зарегистрироваться в банке, открыв счет.

Учитывая статистику хищения средств с бесконтактных банковских карт, нельзя сказать, что этот вид мошенничества имеет массовый характер.

По статистике, за шесть месяцев 2015 года в Великобритании из 2.56 миллиардов фунтов стерлингов, потраченных с бесконтактных банковских карт, лишь 516.5 тысяч фунтов попали в руки к мошенникам, - это всего 0.2% от общего объема.

Однако хакерские технологии не стоят на месте. На одной из конференции по безопасности, прошедшей в США, был продемонстрирован взлом защиты, позволяющий снимать с бесконтактной платежной карты как минимум одного из известных британских банков до 999 999,99 долларов в иностранной валюте. В качестве платежного терминала при этом может выступать простой мобильник с поддержкой NFC и установленным на него хакерским программным обеспечением. Злоумышленнику требуется лишь поднести такой телефон к карману жертвы, где лежит кредитка. На транзакцию уходит менее секунды. Компания, осуществляющая процессинг взломанной карты, уже прокомментировала информацию об уязвимости, заявив, что у пользователей нет причин для беспокойства, а взлом невоспроизводим в условиях, отличных от лабораторных.

По мнению специалистов, существует достаточно простой способ защит от кражи средств с такой карты. Достаточно экранировать сигнал от RFID метки, например, купить специальный кошелек, или обернуть собственную карту алюминиевой фольгой. В продаже появились специальные экранирующие карты, которые кладутся в кошельки рядом с собственными. Также пользователям новых карт можно посоветовать придерживаться давно известных рекомендаций относительно того, чтобы быть внимательными с SMS-информированием и соблюдать другие известные правила при проведении трансакций.

Существует ряд зарегистрированных полезных моделей для защиты бесконтактной карты от считывания информации. В основном они построены на принципах экранирования сигнала RFID. Есть патенты по бесконтактным карточкам с встроенным источником питания, который активируется в момент проведения оплаты, что существенно повышает безопасность такого вида платежного инструмента.

Список использованных источников:
1.Лыньков Л.М., Мухуров Н.И. ЭУМКД «Основы управления интеллектуальной собственностью»
2.http://www1.fips.ru
3.http://www.belinvestbank.by/private-clients/plastic/new_products_and_services/virtual_card.php

МОШЕННИЧЕСТВО В ИНТЕРНЕТЕ: ВИДЫ И СПОСОБЫ ПРОТИВОДЕЙСТВИЯ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Метько Н.Е.

Власова Г.А. – канд. тех. наук, доц.

Согласно Уголовному кодексу Республики Беларусь, мошенничество – это завладение имуществом либо приобретение права на имущество путем обмана или злоупотребления доверием. Киберпреступность — преступления, совершаемые в сфере информационных технологий. Мошенничество в интернете также относится к категории киберпреступление.

Таким образом, мы можем сказать, что мошенничество в интернете – это завладение имуществом либо приобретение права на имущество путем обмана или злоупотребления доверием с использованием интернет технологий и ресурсов.

В настоящее время можно выделить наиболее популярные виды интернет- мошенничества:

- фишинг;
- вишинг;
- фарминг;
- кликфрод;
- «нигерийские письма»;
- мошенничество с помощью служб знакомств;
- мошеннические интернет-магазины.
- участие в MLM-схемах.

Русскоязычный и украиноязычный сектор Сети в меру своей малоразвитости в финансовом плане пока не очень подвержен атакам мошенников.

- Лже-благотворительность
- Секретные кошельки WebMoney
- Фонды помощи
- Бесплатная мобильная связь
- Финансовые пирамиды

Мошенники использую различные метода обмана. Зачастую это происходит через электронные письма или сообщения, но есть также и сайты-однодневки и тому подобное. Главное в таких ситуациях, быть предельно благоразумным, не доверять слишком легко незнакомым Вам сервисам и сайтам, следить за личной информацией, которую Вы размещаете в Интернете.

Список литературы:

1.Управление по раскрытию преступлений в сфере высоких технологий. Правонарушений в среде Интернет. [Электронный ресурс]. Режим доступа: http://mvd.gov.by/ru/main.aspx?guid=3291

2.Мошенничество в среде Интернет. [Электронный ресурс]. Режим доступа:https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D1%88%D0%B5%D0%BD%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D1%82%D0%B2%D0%BE

3.Уголовный кодекс Республики Беларусь. Статья 209. Мошенничество. Определение «мошенничество». [Электронный ресурс]. Режим доступа: http://kodeksy-by.com/ugolovnyj_kodeks_rb/209.htm

4.Наиболее распространенные способы мошенничества в интернете. [Электронный ресурс]. Режим доступа: http://moneymaster.ru/obman-v-internete.php

Управление по раскрытию преступлений в сфере высоких технологий. Правонарушений в среде Интернет. Интернет-мошенничество – памятка для граждан. [Электронный ресурс]. Режим доступа: http://mvd.gov.by/ru/main.aspx?guid=233903

ПРОБЛЕМЫ ПОСТИНДУСТРИАЛЬНОГО ОБЩЕСТВА

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Морозова В.Р., Муха П.П.

Жилинская Н. Н.- канд. экон. Наук, доц.

В современном мире новшества ожидают нас на каждом шагу. Куда бы мы ни посмотрели, не найдётся ни одна сфера жизнедеятельности, в которой не встречались бы современные технологии. Такое общество называют постиндустриальным, или информационным. Чтобы дать полное определение данному термину, необходимо исследовать, знает ли современный социум, что такое постиндустриальное общество.

В специально составленном опросе участие приняли 123 человека в возрасте от 14 до 60 лет. По результатам опроса в границы возрастного диапазона моложе 18 лет попали 74 % респондентов. Анализ последующих ответов показал, что большинство опрашиваемых сталкивались с понятием и знают, что такое постиндустриальное общество.

Ниже приведены графики №1 и №2сравнительного анализа: