СТРАТЕГИЯ ПОВЫШЕНИЯ ФИНАНСОВОЙ ГРАМОТНОСТИ
В РОССИЙСКОЙ ФЕДЕРАЦИИ НА 2017-2023 ГОДЫ

ФИНАНСОВОЕ КОНСУЛЬТИРОВАНИЕ

МИНИСТЕРСТВО ФИНАНСОВ
Российской Федерации

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Тема 8.2. Кибербезопасность электронных платежей, NFC, электронного рубля и криптовалют

Термин **«Кибербезопасность»** – безопасность в киберпространстве.

Как известно, внедрение интернет-технологий в банковскую деятельность изменило способы банковского мошенничества.

Для обеспечения денежных средств на счетах в банке необходимо знать о новых способах хищения.

В таблице (Таблица 1) вы видите основные типы кибератак, их название и характеристики. Например Фишинг — «рыбная ловля».

Таблица 1. Основные типы кибератак

Типы кибератак	Описание
Отказ в обслуживании	Компьютерная атака из одного источника. Предполагает блокирование доступа для авторизированных пользователей к определенному компьютеру жертвы при помощи «перегрузки» количеством сообщений. Метод предназначен для блокирования легального трафика (обмена данными зараженного компьютера с другими компьютерами) и, возможно, блокирования загрузки компьютера в целом
Распределенный отказ в обслуживании	Вариант кибератаки типа «отказ в обслуживании», построенный на сосредоточенной атаке со многих распределенных в пространстве компьютеров. Организация такой атаки требует предварительного заражения специальными программами-«червями» участвующих в ней компьютеров
Инструменты взлома («отмычки»)	Открыто распространяемое программное обеспечение для взломщика любой степени подготовки, предназначенное для обнаружения уязвимостей в целевой киберсистеме и получения к ней доступа
Логические бомбы	Разновидность кибернарушения, при которой программист запускает написанный программный код, способный вызвать серьезные проблемы в работе выполняемой программы, вплоть до ее полной блокировки
Фишинг (phishing, от fishing — «рыбная ловля»)	Разработка, распространение и применение вирусных писем-сообщений и интернет-сайтов, аналогичных официальным сообщениям и сайтам предприятий, банков (центральных и коммерческих), правительственных ведомств и онлайн-магазинов. Делается это для дезориентации клиентов и с целью заставить их раскрыть свою конфиденциальную информацию. Такую, например, как пароль от личного кабинета в онлайн-банке. «Фишеры» используют собранную информацию в своих корыстных целях или просто перепродают ее

Метод (разновидность) фишинга	Данный метод использует дешевые web-технологии передачи звуковых (голосовых) файлов и АПО открытых call-центров. Благодаря дешевизне мошенники могут создать свои жульнические call-центры и от имени действующих ОКФС рассылать их клиентам-жертвам голосовые сообщения и электронные письма с требованием передать по телефону или SMS конфиденциальную информацию «в связи с непредвиденными проблемами для защиты средств на своей карте»
Сниффер (от англ. to sniff — «нюхать»)	Другое название — «пакетный сниффер». АПО, служащее хакеру для перехвата и фильтрации передаваемого трафика и поиска среди этой информации конфиденциальных данных о пользователе (например, «ловушки wi-fi», используемые в общественном транспорте)
Троянские программы	Компьютерные вредоносные программы, содержащие скрытый код. Обычно трояны маскируются под «здоровые» программы, необходимые для работы. Название произошло от древнегреческого мифа
Вирусы	АПО, служащее для инфицирования (заражения) компьютерных файлов, путем добавления в их программный код вредоносных команд, которые компилируются (исполняются) обычно при загрузке инфицированного файла в оперативную память компьютера и это заражает другие файлы. Для запуска размножения вирусов нужно неосознанное вмешательство пользователя. Чаще всего для активации вируса применяется фишинг
Черви	Вредоносные компьютерные программы, которые, в отличие от вирусов, не нуждаются во вмешательстве пользователя сети Интернет для своего размножения и, копируя самих себя, заражают компьютеры

Это разработка, распространение и применение вирусных писем-сообщений и интернет-сайтов, аналогичных официальным сообщениям и сайтам предприятий, банков, онлайн-магазинов.

Делается это **для дезориентации клиентов** и **с целью заставить их раскрыть свою конфиденциальную информацию.** Такую, например, как пароль от личного кабинета в онлайн-банке. «Фишеры» используют собранную информацию в своих корыстных целях или просто перепродают ее.

Троянские программы – это компьютерные вредоносные программы, содержащие скрытый код. Обычно трояны маскируются под «здоровые» программы, необходимые для работы.

В таблице (Таблица 2) представлены Виды компьютерных атак и их характеристика.

Таблица 2. Виды компьютерных атак и их характеристика.

Вид ВПО (угроза)	Характеристика
Потенциально нежелательные приложения (PUA)	PUA — это невредоносные приложения, которые во время установки основного программного обеспечения могут предлагать пользователям дополнительные программы путем социальной инженерии
Трояны-сбрасыватели (скрипты VBS)	Сбрасыватель — тип троянской программы, предназначенный для заражения компьютеров другими вредоносными программами
Вредоносные ссылки в социальных сетях	Сообщения со ссылками на вредоносные сайты, сопровождаемые правдоподобным текстом, заставляющим жертву атаки поверить, что ссылка безопасна и интересна
Загрузчики программ-троянов (скрипты)	Скрипт — это программный файл, содержащий сценарий, который автоматизирует некоторую задачу, облегчающую работу пользователя (в частности, злоумышленника)
Перенаправление браузера (JS)	Автоматическая переадресация на другую страницу с помощью скрипта, написанного на языке JavaScript, без участия пользователя. Может применяться как с продуктивной, так и с деструктивной целью

Обратите внимание на Вредоносные ссылки в социальных сетях, это сообщения со ссылками на вредоносные сайты, сопровождаемые правдоподобным текстом, заставляющим жертву атаки поверить, что ссылка безопасна и интересна

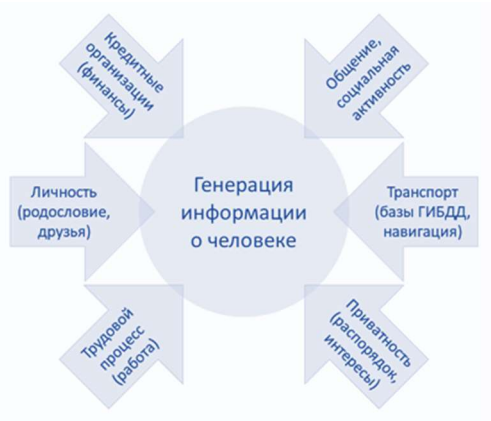

Рисунок 1. Генерация информации о человеке

Сегодня всем клиентам банка необходимо понимать, что «цифровой человек» все больше и больше использует устройства, фиксирующие информацию о его местонахождении и деятельности, при этом риски нарушения информационной безопасности возрастают.

На экране вы видите источники информации о «цифровом» человеке. Помните об этом, оставляя информацию о себе, **ей могут воспользоваться мошенники.**

Рассмотрим упрощенную схему (Рисунок 2), в которой пользователь выдает себя сам:

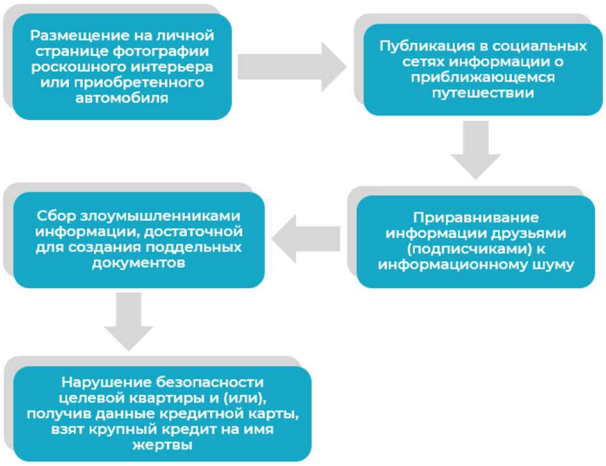

Рисунок 2. Упрощенная мошенническая схема

- **вначале** человек размещает на личной странице фотографии роскошного интерьера или приобретенного автомобиля;
- **потом** сообщает так называемым френдам и фолловерам, что через неделю уезжает в отпуск;
- друзья приравнивают такую откровенность к информационному шуму;
- злоумышленники собирают информацию, достаточную для создания поддельных документов;
- **после** чего грабителю остается нарушить безопасность целевой квартиры и (или), получив данные кредитной карты, взять крупный кредит на имя жертвы.

На рисунке (Рисунок 3) представлена Схема воздействия методов социальной инженерии.

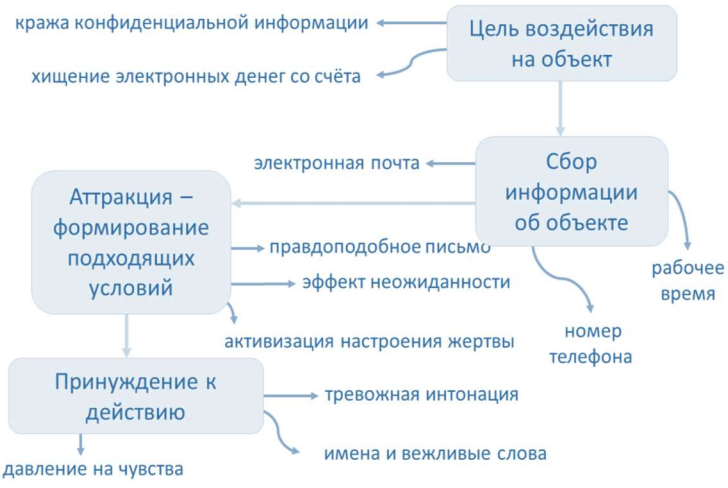

Рисунок 3. Схема воздействия методов социальной инженерии

Сегодня довольно распространена следующая схема кибершпионажа:

- На телефон **приходит SMS-сообщение такого содержания:** «Пароль XXXXXX. Это код активации приложения «Легкий платеж». Если это не вы совершаете активацию, срочно обратитесь в службу поддержки».
- **После этого звонит мошенник,** представляется любым именем (тем самым ослабляя бдительность жертвы, поскольку новое имя вызывает интерес у абонента – аттракция) **и просит назвать пароль,** который по чьей-либо ошибке пришел на «чужой» телефон.

Как поступить – зависит от осведомленности абонента.

Запомните, если абоненту звонят по телефону и просят перезвонить по другому номеру, то абонент, звонящий по этому телефону, опять **пассивная сторона.** Поэтому если представляются сотрудниками банка, то **перезвонить обязательно следует, но только по официальному номеру** телефона — он есть на банковской карте или сайте банка

Следующий вопрос о безопасности новых явлений на финансовом рынке криптовалют и цифрового рубля.

В таблице (Таблица 2) вы видите Основные различия между электронными деньгами и криптовалютой.

Таблица 2. Основные различия между электронными деньгами и криптовалютой

	Электронные деньги	Криптовалюта
Регулирующий орган	Центральный банк, Федеральная резервная система, SWIFT	Отсутствует
Совершение операции	Снятие наличных в банкоматах, расчет по пластиковым картам или напрямую в онлайн-магазинах	Необходим перевод в традиционную валюту для получения наличных или расчеты в соответствующих магазинах
Передача валюты возможна между...	Любыми лицами с индивидуальным лицевым счетом в коммерческом банке	Только внутри системы Blockchain и между ее пользователями напрямую
Возможность противоправных операций	Средняя; контролируется надзорными органами	Очень высокая
Инвестиции	Инвестиционная активность снижена ввиду неблагоприятной экономической конъюнктуры и курса валют	Инвестиционная активность имеет место и набирает популярность
Валютный курс зависит от...	Экономические, политические и другие факторы	Спрос и предложение пользователей
Предел эмиссии	Ограничен Центральным банком государства	Ограничен определённой валютой

Данные в таблице свидетельствуют, что криптовалюты являются не безопасным финансовым инструментом, без эмитента, с высокой волатильностью. Поэтому, для операций с ней необходимы дополнительные знания.

Безопасность криптовалют связана с **технологией распределенных реестров, или Блокчейн.**

Как устроена система Blockchain показано на рисунке (Рисунок 3).

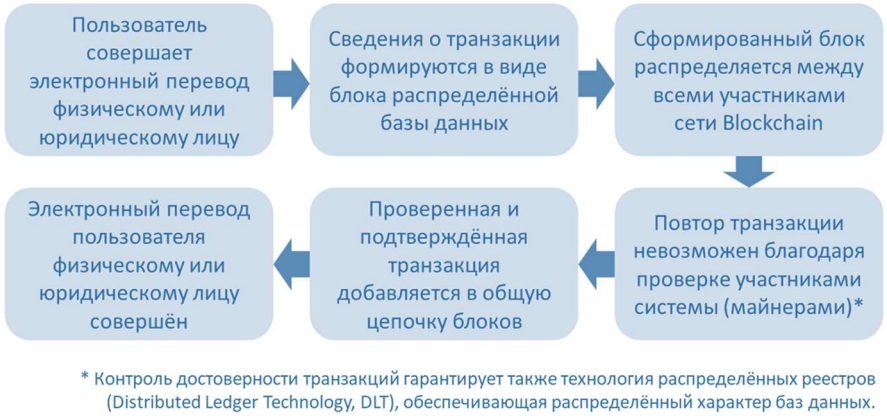

Рисунок 3. Как устроена система Blockchain

Но серия кибератак, направленных против цифровых валют, оставила отрасль финансовых услуг в недоумении: может ли новая технология Blockchain быть достаточно защищенной от компьютерных преступников? **Помните об этом.**

Киберпреступники уже нацеливаются на компании, использующие Blockchain и цифровую валюту, атакуя компании DAO и Bitfinex.

DAO был своего рода краудсорсинговым фондом венчурного капитала, который позволял людям делать инвестиции с использованием криптовалюты Ethereum.

В мае 2016 г. он собрал более 150 млн дол., а только в июне того же года более 50 млн дол. было похищено киберпреступниками — треть добытой валюты.

Bitfinex – цифровая валютная биржа, находящаяся в Гонконге, потеряла около 65 млн дол. после кибератаки в августе 2016 г.

Следующая проблема, это Риски бесконтактных платежей (NFC).

NFC, или Near field communication, «ближняя бесконтактная связь» – технология беспроводной высокочастотной связи малого радиуса действия, с помощью которой можно обмениваться данными между устройствами в пределах 10 сантиметров, не боясь потерять данные или быть перехваченным.

На рисунке (Рисунок 4) вы видите возможности данной технологии, она используется в различных сферах жизни человека: покупка билетов, обмен информацией и широко применяется для бесконтактных платежей.

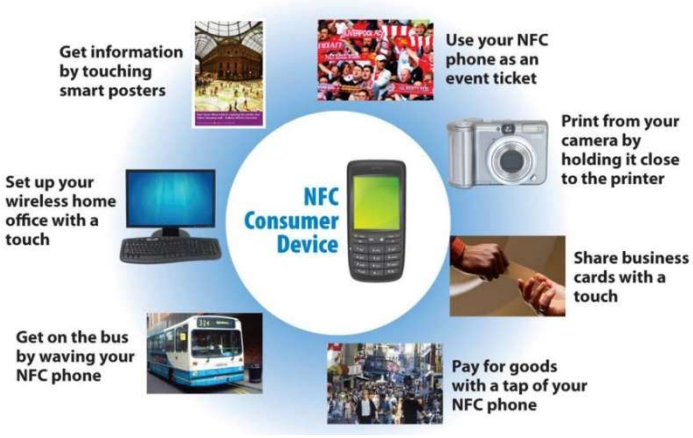

Рисунок 4. Возможность NFC

Существует три наиболее популярных варианта использования NFC технологии в мобильных телефонах:

- **эмуляция карт** – телефон прикидывается картой, например пропуском или платежной картой;
- **режим считывания** – телефон считывает пассивную метку (Tag), например для интерактивной рекламы;
- **режим P2P** – два телефона связываются и обмениваются информацией.

На рисунке (Рисунок 5) представлены другие устройства часы, браслеты, кольца с NFC.

Рисунок 5. Устройства с NFC

В качестве «носителя» NFC-чипа зачастую выступает мобильный телефон – устройство столь же массовое, сколь и индивидуальное, а главное неразлучное со своим владельцем, выступая как:

- платежное средство (виртуальный кошелек),
- средство идентификации владельца,
- ключ,
- бонусная карта,
- проездной билет.

У NFC есть свои темные стороны – они представлены в таблице (Таблица 3).

Таблица 3. Риски использования NFC

Уязвимость	Атака	Методы снижения риска	Примечание
Угроза модификации данных	Замена метки на другую с измененными данными	Цифровая подпись NFC Forum RTD обеспечивает гарантию целостности данных	Не увеличивает стоимость продукта или услуги
Ограничение доступа к конфиденциальным данным	Получение доступа к конфиденциальным данным	Использование шифрования данных или защиту паролем	Алгоритм шифрования добавляет стоимости продукту или услуге
Физическое разрушение	Физическая порча или разрушение метки	Использовать физическую защиту, например располагать метку под упаковкой или этикеткой	Дополнительные меры физической защиты добавляют стоимости продукту или услуге
Перехват данных	Пиратство	Использование крипто-механизмов, шифрование данных, цифровая подпись	Алгоритм шифрования добавляет стоимости продукту или услуге

Но не бойтесь ездить в метро с картами с NFC.

Часто описываемый пример в интернете – злоумышленники крадут средства через мошеннический мобильный POS-терминал или специальное устройство, которое создаст фейковую покупку и «вынудит» карту жертвы ее оплатить.

Однако, **такой способ практически не реализуем.**

Злоумышленнику нужно иметь счет в банке, оформленный на юрлицо, и платежный терминал, зарегистрированный в налоговой инспекции. Кроме того, из-за жалоб клиентов счет вероятнее всего заблокируют до того, как мошенники успеют заполучить деньги.

МИНИСТЕРСТВО ФИНАНСОВ
Российской Федерации

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ