# ТЕХНИЧЕСКИЕ НАУКИ

***Щербаков Александр Александрович***
студент
***Орлова Анна Юрьевна***
канд. экон. наук, доцент

ФГАОУ ВПО «Северо-Кавказский Федеральный университет»
г. Ставрополь, Ставропольский край

## INTERNET-БЕЗОПАСНОСТЬ

***Аннотация:*** *статья посвящена проблеме защиты денежных средств и конфиденциальной информации, передаваемой по сети Internet. Авторами обстоятельно обоснована актуальность проблемного вопроса, отмечены факторы защиты информационных систем, а также выделены правила поведения в сети Internet, необходимые для защиты от мошенников.*

***Ключевые слова:*** *Internet, Secure Socked Layer, CM2, CVK2, шифрование данных.*

В наше время Internet стал необходимым ресурсом для каждого человека. В этой всемирной паутине мы узнаем новости, ищем необходимую информацию для работы или учебы, совершаем покупки на различных торговых площадках. В современном 21 веке нет такого человека, который не пользовался бы услугами Internet. В наше время самой используемой частью глобальной сети стало ведение торговли или, проще говоря, ведение электронной коммерции. Абсолютно все пользователи, которые совершают покупки или думают совершить интернет покупку, переживают за свою информацию, а точнее, за средства, которые в них хранятся в электронном виде. Проще говоря, испытывают страх за свои деньги, хранящиеся на банковской карте. Именно поэтому на сегодняшний день актуально обеспечение безопасности и конфиденциальности граждан и их финансов. Что же стоит за сохранением денег, каким образом защитить конфиденциальную

информацию, как не купить кирпич стоимостью нового iPhone, и как не стать жертвой мошенников? Все это мы рассмотрим в данной статье.

Сама торговля в Internet – это не что иное, как заключение сделки между покупателем и продавцом без личного, прямого контакта. Осуществление покупок, таким образом, намного приятнее, быстрее. Самому покупателю не стоит тратить время по поездкам в торговые центры, стоит просто выйти в Internet, найти свой товар и купить его. Все вроде и хорошо, но есть следующие причины, по которым люди не спешат поступать таким образом. Абсолютно все бояться за свой капитал сознательно или подсознательно, недоверие к информационной среде, вдруг данными воспользуются иные лица. Почему их страхи являются порой бессмысленными или, наоборот, актуальными.

Рассмотрим, почему актуальна тема безопасности личных данных в Internet. Из-за Internet убытки понесли не только юридические и физические лица, но и сами банки. Пиком взлома различных компаний был 2010 год, хищения составляли в районе 250 000 рублей за 1 атаку, известны случаи с кражей 10000000 $ – и это за раз. Все это было проделано благодаря вирусному ПО, которое проникало на ПК банка через Internet. После адаптации вируса к программному обеспечению банка вредоносное ПО создавало свои платежные поручения и финансовые переводы. С тех пор безопасность и защита ПО ушла далеко вперед. Появились новые системы защиты, новые способы сохранения персональных данных. Но и способы кражи тоже не стоят на месте.

Банки стали использовать различные системы и механизмы для повышения безопасности использования online платежей и переводов через Internet. Основным механизмом защиты стало шифрование данных. Банки стали применять следующий тип шифрования: Secure Socked Layer. SSL работает следующим образом: данное ПО зашифровывает данные, которые передаются с одного компьютера на другой и обратно, то есть банк – пользователь и наоборот. Протокол SSL защищает информацию и позволяет спокойно ее передавать. Если в процессе передачи информации по Internet ее попытаются перехватить, то воспользоваться ею не получится. Передаваемые данные закрыты шифром, который взломать за

короткий промежуток времени невозможно. Но есть и обратная сторона медали. SSL надежно зашифровывает информацию, передаваемую через Internet. Но информация уязвима, когда она сохранена на сервере продавца. Если сервер незащищен и хранящиеся на нем данные не зашифрованы, то номер карты и информация о ее владельце становятся доступны 3-м лицам – мошенникам. Почему так? Все из-за того, что при проведении покупки сервер продавца сохраняет все данные, но не без использования протокола SSL. Как было указано выше, протокол Secure Socked Layer защищает данные во время передачи.

При передаче данных через Internet используются следующие два протокола шифрования. Это идентификаторы владельца карты или проверка кодов CM2 и CVK2. CM2 – это код для платежной системы VISA, а CVK2 – код для MasterCard.

Следующий способ защиты Internet-бизнеса – это одноразовые пароли, получаемые в банкомате. При этом, кроме ввода обычного логина и пароля при совершении платежных операций или при входе в систему, пользователь обязан ввести одноразовый пароль. Если смотреть на это со стороны безопасности, то такой способ действительно хорош. При совершении операции в сети Internet лицо должно иметь карту, знать PIN код и иметь одноразовые пароли, которые можно получить только в банкомате. Но и тут не все гладко, а недостатки заключены в следующем. Список одноразовых паролей распечатан на чеке, и его необходимо хранить для подтверждения будущих операций. Из этого следует, что в случае его потери необходимо будет распечатать новый. К всеобщему счастью, одноразовые пароли не являются единственным способом защиты, существуют SMS-пароли с одноразовым кодом.

Одноразовые SMS-пароли – это система, при которой каждая выполняемая операция будет запрашивать код, который приходит на телефон. При этом сам номер должен быть привязанным к номеру счета. В этой системе можно выделить следующие плюсы:

– простота в использовании, процедура подтверждения занимает мало времени;

– защищает учетную запись от мошенников, так как при попытке выполнить операцию приходит SMS-сообщение.

Но все это меркнет перед самым эффективным способом защиты, которым является криптография, широко использующаяся в различных сферах деятельности, как в государственных, так и коммерческих структурах.

В чем же заключено отличие от традиционных способов шифрования. Заключено оно в том, что при криптографическом шифровании используются два ключа. Один ключ зашифровывает отправляемую информацию, а второй ключ, наоборот, расшифровывает получаемую информацию. Главное преимущество в том, что один ключ невозможно вычислить без другого.

К всеобщему сожалению, решить проблему обеспечения безопасности с использованием аппаратных и технических средств различного ПО полностью в Internet невозможно. Как сообщает статистика, защита информационных систем зависит от следующих факторов:

– на 30% от применяемых технических решений;

– на 40% от проводимых мероприятий по защите в организациях;

– на 30% от морально-нравственного состояния общества, и как не странно общекультурного уровня пользователя.

Ознакомившись со способами защиты информации, передаваемой в сети Internet, рассмотрим и то, почему все же происходит утечка, в чем заключены основные ошибки.

К несчастью, большая часть различных кредитных организаций не имеет специалистов по обеспечению информационной безопасности. Чаще всего банки контролируют и управляют своими филиалами из головных офисов. Но все это носит только частичный, неполный характер. Как показывает практика, вопросы по обеспечению безопасности не решаются. Незащищенными являются те предприятия, где система безопасности не настроена правильным образом. К такой главной ошибке банка и к большой радости мошенника можно отнести неправильно настроенную внутреннюю сеть, которая соединена с внешней. Неправильно настроенные межсетевые экраны и АРМ-клиента банка. Принимаются

неквалифицированные работники, для которых сама работа по защите носит второстепенный характер.

Но все свое «злато» можно потерять в сети Internet и другими различными способами. Как показывает практика, чаще всего именно сами юридические и физические лица допускают ошибки, которые и ведут к потере средств или важной информации, проходящей через Internet. Это, прежде всего, неосторожность и невнимательность. Следует быть более внимательным при работе с финансами в сети Internet. Главной ошибкой всех жертв мошенников стали те, которые отвечали на электронные письма с просьбой передать свои персональные данные, логин и пароль, или же перейти по ссылке для проверки личности на сайт. Для предотвращения и недопущения печальных последствий стоит соблюдать некоторые правила, такие как:

– использование знакомых Internet ресурсов;

– ознакомление с порядком представления услуг и доставки товара;

– проверка Internet коммерсанта на использование им сертифицированных протоколов защиты.

Многие различные причины порой тормозят развитие электронных банковских услуг в сети Internet, но и, наоборот, заставляют не стоять на месте. Отсутствие стандартизированных шифровальных протоколов для передачи данных через Internet не прибавляет большой активности для потенциальных клиентов. К счастью, на данный момент с целью осуществления безопасности банки и организации для проведения online операций и защиты данных пользуются профессиональными средствами защиты. Но, к сожалению, еще многое предстоит сделать для защиты данных в Internet. Осуществление и создание новых способов защиты не стоит на месте, а идет вперед, впрочем, как и способы взлома и обхода.

***Список литературы***

1. Голдовский И. Безопасность платежей в Internet. – 2001.

2. Букин М. Активная безопасность ДБО технологии. – 2010.

3. Калемберг. Ключевой элемент информационной безопасности в новых условиях. – 2010.

4. Гончаров В.В. Безопасность и защита Internet. – 2010.

5. ГОСТ Р 34.10-94 Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма