УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БАНКОВСКОМ СЕКТОРЕ

А.А. ГЕЛДИЕВ, О.Г. АМАНОВА

Гелдыев Ахмет Аманмырадович[1], Аманова Огулжан Гурбангелдиевна[2], преподаватели; Государственный энергетический институт Туркменистана, г. Мары.

Аннотация. В данной статье рассматривается проблема кибербезопасности в сфере информационных технологий в Туркменистане. Анализируются основные угрозы и вызовы, с которыми сталкиваются организации и государственные структуры в области информационной безопасности. Особое внимание уделяется мерам по защите информации и развитию кибербезопасности в контексте современных тенденций в области цифровизации.

Новые технологии, глобальные коммуникационные сети, охватывая практически все сферы деятельности человека и общества, меняют не только качество жизни людей, но и многократно увеличивают риски и угрозы в информационной сфере, несут реальные угрозы информационной безопасности личности, общества и государства.

Информационная безопасность в Туркменистане стоит так же остро, как и вопросы динамичного экономического развития и интеграции в мировое сообщество. Информация, наряду с финансовыми и природными ресурсами, является важнейшим фактором конкурентоспособности страны на международной арене. До недавнего времени проблемам информационной безопасности внутри страны и во внешнем пространстве уделялось крайне мало внимания.

В связи с этим в последние годы органами законодательной и исполнительной власти Туркменистана были приняты законы по вопросам защиты государственной тайны, обеспечение сохранности информационных ресурсов государства, их рационального использования, регламентации международного информационного обмена. К туркменским законам, регулирующим информационную безопасность в нашей стране относятся: Конституция Туркменистана, закон Туркменистана «Об информации и её защите», «О государственных секретах», «Об электронном документе и электронной цифровой подписи» и т.д.

Целью работы является изучение особенностей информационной безопасности. Для её достижения были использованы методы анализа и синтеза научных публикаций и литературных источников по рассматриваемой теме.

В статье рассмотрим два различных механизма защиты: смарт-карты и запоминающие карты с магнитной полосой. Определим, с какой картой будет более безопасно пользоваться смарт-картами с микропроцессором или картой с памятью магнитной полосой.

Информационная безопасность характеризуется способностью государства, общества, социальной группы, личности обеспечить защищенность

информационных ресурсов для поддержания своей жизнедеятельности и жизнеспособности, противостоять информационным опасностям и угрозам, неблагоприятным информационным воздействиям на личное и общественное сознание и психику людей, а также на компьютерные сети и другие технические источники информации.

Сегодня фишинг — один из самых распространённых в мире видов киберпреступлений, с помощью которого чаще всего похищают аккаунты и банковскую информацию.

Электронная система платежей, основанная на использовании смарт-карты, на которой ведется баланс средств. Их часто называют «stored-value cards» электронный бумажник. Некоторые такие карты уже опробованы на практике: система MasterCard, VisaCard.

Основная идея таких карт состоит в том, чтобы использовать ее в денежных расчетах. Специальные терминалы стали неотъемлемой частью нашей жизни: они появились в банках, в магазинах и присоединены к компьютерам, подключенным к Интернету. Такие карты обладают тем преимуществом, что они не обязательно должны работать в режиме онлайн, то есть находиться на связи с каким-либо центральным сервером. При использовании обычных платежных карточек торговый автомат обязан связаться с банковским компьютером в режиме реального времени. Их недостаток состоит в том, что утрата или повреждение карты означают потерю денег.

Как и всякая другая система электронных платежей, электронный бумажник имеет полный набор средств защиты. В их защите использует криптография, меры компьютерной безопасности, средства защиты от подделки и. т. д. Они обеспечивают необходимый уровень целостности данных, конфиденциальность и анонимность. Мы не будем вдаваться в подробности, но рассмотрим, как используются карты двух различных типов.

Карты с магнитной полосой. Пользователь помещает карту в считывающее устройство и вводит PIN (личный идентификационный номер), пароль или код. Устройство считывает данные с магнитной полосы и использует PIN для расшифровки данных. Затем эти данные обрабатываются устройством для выполнения системой разнообразных действий, для которых она предназначена: вхождение в систему, подписывание электронного чека, плата за стоянку и т. п.

Смарт-карты. Пользователь помещает карту в различные считывающие устройства и вводит тот же личный идентификационный номер. Устройство посылает PIN в смарт-карту, которая расшифровывает данные. Затем они используются картой для выполнения системой нужных действий, а само устройство выполняет в системе функцию ввода-вывода данных.

В чем же различия? В обоих случаях примененное в преступных целях считывающее устройство в состоянии разрушить систему, так как это устройство является единственной связью карты с внешним миром. Как только станут известны секретные данные карты с магнитной полосой, устройство может делать все, что пожелает. Как только смарт-карта получит правильный PIN, считывающее устройство может заставить всех поверить всему, что оно захочет.

Основное различие между этими картами состоит в том, что смарт-карта умеет осуществлять некоторый контроль, так как имеет внутреннюю защиту. Например, если кто-нибудь украдет карту с магнитной полосой, он сможет грубыми приемами завладеть данными этой карты. Он может сделать это автономно, на компьютере, так что ее владелец даже не узнает о случившемся.

Смарт-карту нельзя взломать подобным образом, поскольку ее можно запрограммировать так, что она будет выключаться после нескольких неправильных вводов пароля подряд. Так, если кто-нибудь похитит смарт-карту, узнать пароль с легкостью у него не получится. Он получит возможность сделать только три попыток.

Другое существенное различие состоит в том, что смарт-карта не выдает свои секреты. Например, при использовании карт для подписи документов смарт-карта будет более безопасна, чем карта с магнитной полосой. Карта с магнитной полосой передает считывающему устройству функцию подписания документа, тем самым сообщая ему все секретные данные. В этом случае остается только надеяться на лучшее. Преступник с помощью устройства чтения может украсть шифр подписи. Смарт-карта же самостоятельно ставит подпись. Сканирующее устройство может загружать в карту для подписи подложные документы, но оно не получит шифр подписи.

Есть и другие, более тонкие различия. Смарт-карта позволяет опереться на некоторые основные правила выполнения действий. В принципе это можно использовать и в системе, которая обращается к базам данных, и для карт с магнитной полосой, но смарт-карты позволяют добиться лучшей реализации.

Известно, что смарт-карты распространены как платежное средство по всей Европе, но не в Туркменистане. Почему? Все объясняется особенностями телефонной связи. Система проверки туркменских карточек работает в режиме онлайн. Когда вы покупаете что-нибудь, продавец использует модем, чтобы убедиться в том, что ваша карточка действительна и вы платежеспособны. Двадцать лет назад эта система не могла бы работать ни в одной европейской стране. Плата за телефон была высока, многие магазины их даже не имели, а в Италии, например, их установки приходилось дожидаться год или два. Связь была дорогой и ненадежной. Создание онлайновой системы в Европе было невыгодно, поэтому индустрия кредитных карт отдала предпочтение смарт-картам, позволявшим хоть как-то обезопасить сделки. Дело не в том, что смарт-карты защищены лучше, чем карты с магнитными полосами, просто туркменский способ борьбы с мошенничеством был менее практичным.

Некоторые люди получают банковские карточки под вымышленными именами, но нетрудно склонить кого-либо к тому, чтобы он использовал свое настоящее имя. Несомненно, в мире найдется много желающих открыть банковский счет, который, как они понимают, будет контролироваться другими людьми и использоваться для отмывания денег, если им предложат несколько тысяч долларов. Если на такие карточки положить деньги, их можно использовать как компактное платежное средство, и не существует очевидного способа воспрепятствовать этому.

Обратите внимание на то, что решение вопросов морали и законности в этой сфере далеко не очевидно. Требования о предоставлении финансовой отчетности в государственные органы США и Великобритании. России, Белоруссии и Туркменистана могут причинять некоторые неприятности гражданам, но власти редко злоупотребляют этим. Во многих других странах, таких как Китай, Турция. Мексика или Сирия, дело принимает совсем другой оборот. Последнее обстоятельство чревато политическими и юридическими проблемами для тех компаний, которые обязаны предоставлять такие сведения, и способно привести к большему распространению мошенничества в этих странах.

Важно иметь законы и нормативные акты, регулирующие область кибербезопасности, включая защиту персональных данных, наказание за киберпреступлений и другие аспекты. Участие в международных и региональных платформах по обмену информацией о киберугрозы позволяет Туркменистану получать актуальные данные о современных угрозах и применять соответствующие меры защиты. Эти аспекты важны для создания эффективной системы кибербезопасности в стране и обеспечения защиты информационной инфраструктуры.

Если говорить о пластиковых картах, то существует определенное различие между картами с магнитными полосами и смарт-картами, но насколько это важно зависит от их применения. Сопротивление вторжению в смарт-карту при достаточных затратах времени и средств, всегда может быть преодолено, поэтому не имеет смысла создавать систему, безопасность которой основана на средствах сопротивления вторжению. Большинство людей не способны взломать смарт-карту, потому что она боле защищена. Но обе карты создавались в предположении, что считывающему устройству следует доверять, поэтому они могут пострадать от действия устройств, используемых злоумышленниками. И все же, смарт-карта лучше защищена от взлома. И до тех пор, пока сопротивление вторжению не преодолено, смарт-карта надежно хранит свои секреты.

Список использованных источников

1. Президент Туркменистана утвердил Концепцию цифровой образовательной системы. [Электронный ресурс]. – Режим доступа: https://turkmenistan.gov.tm/ – Дата доступа: 15.09.2017.

2. Смирнов А.Б. Кибербезопасность: основные принципы и методы защиты информации. – М.: Издательство НТЦ "Инфра-М", 2018.

3. Туркменский институт информационных технологий, "Отчет о состоянии проектного управления в IT-сфере", 2018.