УДК 004.056.5

# БЕЗОПАСНОСТЬ ДАННЫХ В ЦИФРОВОМ МИРЕ

О.Г. Аманова, А.А. Гелдиев, А.А. Мухамметныязов

**Аннотация.** Эта статья о развитии информационной безопасности в Туркменистане. Анализируются основные угрозы и вызовы, с которыми сталкиваются банки и государственные структуры в области информационной безопасности. Особое внимание уделяется мерам по защите информации и развитию кибербезопасности в контексте современных тенденций в области цифровизации.
**Ключевые слова:** банк, пластиковая карта, цифровизация, информационная безопасность, IT-отрасль.

# DIGITAL SECURITY IN A NETWORKED WORLD

O.G. Amanova, A.A. Geldiyev, A.A. Muhammetniyazov

**Abstract.** This article is about the development of information security in Turkmenistan. The main threats and challenges faced by banks and government agencies in the field of information security are analyzed. Particular attention is paid to measures to protect information and develop cyber security in the context of modern trends in the field of digitalization.
**Keywords:** cyber security, bank, plastic cards, digitalization, information security, IT industry.

На фоне осуществляемого перехода от индустриального к информационному обществу повышается значимость умения ориентироваться в постоянно возрастающем

потоке информации, эффективно работая с ней. Сегодня возможности глобальной сети, активно используется во всех сферах общественной жизни. Основаны на информационных ресурсах, представляющих собой совокупность данных, которые организованы в информационных системах для получения достоверных сведений в различных областях знаний и практической деятельности. Однако одновременно с увеличением роли информации повышается и важность ее передачи и защиты, обеспечивающейся посредством инструментов информационной безопасности.

Целью работы является изучение особенностей информационной безопасности. Для ее 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.

В Туркменистане приняты основополагающие законодательные акты Конституция Туркменистана, закон Туркменистана «Об информации и ее защите»,«О государственных секретах», «Об электронном документе и электронной цифровой подписи.

Наиболее распространенными случаями кибератак являются ботнеты: это сеть компьютеров, зараженных вредоносной программой, позволяющей злоумышленникам удаленно атаковать электронную систему платежей, управлять чужими пластиковыми картами без ведома их владельцев. С помощью ботнетов злоумышленники могут рассылать спам, распространять вирусы, атаковать компьютеры и серверы банков, а также совершать другие преступления.

Сегодня фишинг – один из самых распространенных 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 попытки.

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.

Моделируем угрозы и оценим риски пластиковых карт. Главные виды из преступлений против пластиковых карт это нарушение тайны частной жизни, вандализм и терроризм.

Нарушение тайны частной жизни происходит, когда кто-либо сообщает третьей стороне конфиденциальную информацию о некотором лице без его согласия. В зависимости от местного законодательства такие действия не везде считаются преступлением. Если разработчики пластиковых карт хотят, чтобы система распространилась по всему миру, имеет смысл составить перечень этих действий и не обращать на них внимания, если они считаются законными.

До тех пор, пока система не станет обладать средствами для предотвращения нарушения тайны частной жизни, банки будут иметь неограниченные возможности для получения информации о расходах клиентов. Этого можно избежать в некоторых случаях, если клиенты будут приобретать карты с фиксированной суммой денег на них, аналогично некоторым телефонным картам с предоплатой.

Продавец не сумеет непосредственно получить подобные сведения и узнать имя покупателя, однако с помощью других продавцов он может собрать информацию об использовании карты с известным ему идентификационным номером и, сопоставив данные, идентифицировать ее владельца.

Наконец, следует помнить и о возможности подслушивания: люди, вовсе не участвующие во взаиморасчетах, могут подслушивать и собирать информацию.

Следующий вид преступлений, вызывающих беспокойство, включает вандализм и терроризм. Эти правонарушения в первую очередь направлены против системы в целом, хотя могут совершаться и против отдельных владельцев карт, продавцов и банков. Главная цель таких преступлений –помешать правильному функционированию системы. То, что называется атаками, направленными на отказ в обслуживании, в этом случае может оказаться весьма любопытно.

Давайте рассмотрим в использовании системы для совершения преступлений, то есть о нарушениях закона с ее помощью. До сих пор мы рассматривали лишь возможность отмывания денег, но не менее заманчиво обсудить возможности других противозаконных действий.

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.

Сущность информационной безопасности заключается в формировании активной защиты в отношении приоритетных интересов, связанных с использованием информационных ресурсов, направленной на создание условий для нормального развития общества и экономики. Обеспечение информационной безопасности представляет собой комплексную задачу, что обусловлено сложностью и многоплановостью информационной среды. Если говорить кратко, 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 более 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.

## References

1 The President of Turkmenistan approved the Concept of the digital educational system. [electronic resource]. – Access mode: https://turkmenistan.gov.tm / – Access date: 09/15/2017.

2. Smirnov A.B. Cybersecurity: basic principles and methods of information protection. Moscow: NTC Infra-M Publishing House. 2018.

3. Turkmen Institute of Information Technologies. "Report on the state of project management in the IT sphere", 2018.

## Сведения об авторах

**Аманова О.Г.,** преподаватель кафедры информационные технологи. Государственный энергетический институт Туркменистана. begob3824@gmail.com.
**Гелдиев А.А.,** старший преподаватель кафедры общественных наук. Государственный энергетический институт Туркменистана. begob3824@gmail.com.
**Мухамметныязов А.А.,** преподаватель кафедры электроэнергетических систем. Государственный энергетический институт Туркменистана, akmammetmuhammedow3@gmail.com.

## Information about the authors

**Amanova O.G.,** Lecturer, Department of Information Technology. State Energy Institute of Turkmenistan. begob3824@gmail.com.
**Geldiyev A.A.,** Senior Lecturer, Department of Social Sciences, State Energy Institute of Turkmenistan. begob3824@gmail.com.
**Muhammetniyazov A.A.,** Lecturer. Department of Electric Power Systems. State Energy Institute of Turkmenistan.
akmammetmuhammedow3@gmail.com.