- американская научная школа-конференция «Моделирование и оптимизация химико-технологических процессов»: сб. тр. науч.-практ. конф. – Казань, 2016. – с. 35.
19. Monsanto Accelerator Rheographs, Brussels, 1987; Measuring visco-elastic properties using the MDR 2000 rheometer, Louvain-la-neuve, 1989. – 20 p.
  20. Дорохов, И.Н. Системный анализ процессов химической технологии. Интеллектуальные системы и инженерное творчество в задачах интенсификации химико-технологических процессов и производств. /И.Н. Дорохов, В.В. Меньшиков // М. Наука, 2005. 582 с.
  21. Бельдеева Л.Н. Технологические измерения на предприятиях химической промышленности. В 2-х частях Учебное пособие. - Барнаул: изд-во АлтГТУ, 2002. - (73+76) с.
  22. Bauman J.T. Fatigue, stress, and strain of rubber components. A guide for design engineers Hanser Publishers, 2008. — 214 p. ISBN: 978-1-56990-431-2.
  23. Dick J.S. How to Improve Rubber Compounds. 1800 Experimental Ideas for Problem Solving 2nd Edition. — Munich: Hanser Publishers, 2013. — 407 p. — ISBN 978-1-56990-533-3
  24. Morton Maurice. Rubber technology Springer-science+business media, B.V., 1999. — 643 p.
  25. White J.L., Coran A.Y., Moet A. Polymer Mixing. Techology and engineering HANSER, 2001. 258 p.

Медведев А.Р.

Особенности обеспечения безопасности электронного платежного средства

*Волгоградский государственный университет
(Россия, Волгоград)*

doi: 10.18411/lj-03-2021-07

ids: lj-03-2021-07

Аннотация

Статья посвящена вопросам изучения особенностей обеспечения безопасности электронного платежного средства. Рассматриваются основные уязвимости, которым подвержено ЭПС, их виды в зависимости от источника происхождения угрозы, механизмы обеспечения защиты и противодействия некоторым видам атак на электронные денежные средства, также обзореваются достоинства и недостатки, характерные для ЭПС.

Ключевые слова: информация, информационная безопасность, электронное платежное средство, транзакция, электронные деньги, уязвимости, техническая защита информации (ТЗИ), организационно-правовая защита информации (ОПЗИ), фишинг, претекстинг, атаки, автоматизированная банковская система.

Abstract

The article is devoted to the study of the features of ensuring the security of an electronic means of payment. The main vulnerabilities to which the EMP is exposed, their types depending on the source of the threat, mechanisms for ensuring protection and counteraction to certain types of attacks on electronic money are considered, the advantages and disadvantages characteristic of the EMP are also reviewed, automated banking system.

Keywords: information, information security, electronic means of payment, transaction, electronic money, vulnerabilities, technical protection of information (TPI), organizational and legal protection information (OLPI), phishing, pre-texting, attacks.

Введение

Актуальность нижеследующего изыскания состоит в том, что все сферы современной жизни пронизывает нескончаемый поток самой различной информации: будь то загрузка фотографий на страницу в социальной сети, заполнение анкеты на обработку персональных данных, или же совершение покупки в магазине посредством банковской карты (иначе, электронного средства платежа). И поскольку безналичный расчет в нашей стране в последнее время набирает особую популярность, с каждым днем расширяется область возможного применения электронных денег (начиная от транспортных карт и заканчивая многомиллионными банковскими транзакциями),

активизируется также и деятельность различных криминальных структур и способствующих им теневых организаций, деятельность которых сфокусирована на мошенническом изъеме средств клиентов банков. Подобному развитию событий способствует относительная молодость законодательной базы в области применения электронных платежных средств(ЭПС), что оставляет лазейки для избежания злоумышленниками наказания, а также несколько следующих немаловажных факторов: недостаточная оснащенность мелких и средних кредитных организаций средствами, необходимыми для всесторонней защиты банковской инфраструктуры (в т.ч. и инструментами по отражению атак на ЭПС), массовая утечка данных клиентов банков, невысокая цифровая культура населения по безопасному обращению с банковскими картами.

В связи с этими обстоятельствами становится понятно, что без должного внимания к обеспечению информационной безопасности электронных платежных средств не позволит обществу развиваться сразу в нескольких критически важных сферах: в малом, среднем и крупном бизнесе, в сфере наукоемких производств, в научной деятельности, а также во многих других областях.

Обширная техническая оснащенность злоумышленников средствами, позволяющими безнаказанно похищать безналичные денежные сбережения, заставляет задуматься о создании целого набора механизмов, эффективно предотвращающих большинство известных и используемых на практике атак на ЭПС.

Среди мер как защиты информации в целом, так и применимо к банковской сфере, наибольшую эффективность доказывает техническая защита информации, основанная на внедрении специализированных средств обеспечения информационной безопасности. Также хорошо себя зарекомендовали криптографические и организационно-правовые меры предотвращения киберпреступлений.

Анализ преимуществ и недостатков электронных платежных средств

Для более глубокого понимания процессов, приводящих к несанкционированному доступу(НСД) к безналичным денежным средствам, проанализируем существующие и актуальные на данный момент времени преимущества и недостатки ЭПС. Электронные деньги имеют ряд неоспоримых преимуществ перед своими наличными собратьями, и вот некоторые из них:

- Высокий комфорт при использовании подобного вида оплаты товаров и услуг
- ликвидность электронных денег
- малые затраты при их изготовлении
- сложность в подделке
- отсутствие человеческого фактора при выполнении операций с ними (все расчеты выполняются посредством математических алгоритмов и автоматизации)
- возможность расплачиваться удаленно и через сеть „Интернет ”
- относительная конфиденциальность при совершении транзакций

Однако, существует также и совокупность очевидных недостатков электронных денег, которые ставят под сомнение безопасность этого вида денежных средств:

- неоднозначность правового регулирования в отношении ЭПС
- привязанность к наличию электропитания и доступа в сеть „Интернет”
- недостаточная распространенность среди торговых организаций (особенно среди малого и среднего бизнеса) оборудования для осуществления безналичного расчета
- малая поддержка электронных средств платежа со стороны государства

- возможность заморзки счетов и, как следствие, невозможность осуществления доступа к собственным безналичным денежным сбережениям
- широкий простор для различного рода махинаций с электронными платежными средствами со стороны злоумышленников

На основании приведенного сравнения можно сделать вывод о том, что в настоящее время у электронных денег хотя и есть комплекс убедительных преимуществ, также имеется ряд изъянов, не позволяющих ЭПС считаться самым безопасным средством оплаты на сегодняшний день.

Анализ уязвимостей, наиболее актуальных для Электронных платежных средств

При выявлении уязвимостей ЭПС и атак, спланированных на их основе, стоит разделить все уязвимости на две большие группы:

1. Уязвимости технической, а также программной и аппаратной части электронного платежного средства
2. Уязвимости, построенные на финансовом мошенничестве и включающие человеческий фактор

Под уязвимостями первой категории будем понимать источники угроз, напрямую зависящие от свойств технического оснащения оборудования, прямо или косвенно участвующего в обработке безналичных расчетов, а также от программного обеспечения, установленного на данном оборудовании и наличия (или его отсутствия) дополнительных атрибутов защищенной информационной системы (средства управления доступом, средства оперативного наблюдения, средства регистрации критических событий и др.)

К уязвимостям второго сорта отнесем блок угроз, носящих антропогенный характер и связанных непосредственно с субъектом, деяния которого могут быть расценены как преднамеренные или непроизвольные преступления. Эта категория уязвимостей наиболее многочисленна и представляет наибольший интерес с точки зрения построения системы защиты, так как действия субъекта всегда можно оценить, спрогнозировать и принять соответствующие ответные меры. Методы противодействия в этом случае вариативны и напрямую коррелируют с волей организаторов, обеспечивающих защиту информации.

Диаграмма конкретных уязвимостей, относящихся к категории 1 и категории 2 соответственно представлена ниже:

Анализ методов защиты электронного платежного средства

Для создания эффективной, грамотно выстроенной системы защиты и отражения атак на электронное платежное средство, нужно использовать дифференцированный подход к созданию и использованию таковых средств обороны:

сложно защититься лишь техническими средствами от финансового мошенничества, также как и не удастся отразить массированную атаку на сервера банка технологиями, предназначенными для фишинга или социальной инженерии.

Для выделения набора определенных механизмов для каждой из типов уязвимостей выделим операции, которые подвержены наибольшему риску и меры предосторожности, помогающие нейтрализовать негативное воздействие

Операции, подверженные наибольшему риску и меры предосторожности

№	Операции, подверженные наибольшему риску	Меры предосторожности
1	Редактирование внешнего получателя платежа	Введение запрета на изменение данных после прохождения стадии контроля и до электронной подписи отправляемого рейса
2	Начисление процентов счёта до востребования и расчётные счета	Создание службы контроля автоматических операций по закрытым для остальных сотрудников методикам
3	Хищение денежных средств в системе клиент-банк	Ограничение максимального ежедневного объема платежей, совершаемых по системе клиент-банк, для каждого клиента
4	Поражение системы автоматизации или её отдельного модуля	Обязательное создание резервных копий, введение запрета на доступ бывших сотрудников в информационную систему

На текущий момент во исполнение закона от 27 июля 2006 года № 152 ФЗ, «О персональных данных», большинство кредитных организаций использует следующий набор технических средств защиты информации, обрабатываемой в ЭПС:

- SSL-шифрование данных, которое происходит в самой банковской системе от компьютера пользователя и обратно.
- Наиболее инновационно-развитые банки представляют к применению токены – usb-ключи, которые внешне напоминают флеш-карту и позволяют надежно сохранить различную информацию такую, как цифровые сертификаты, ключи ЭПЦ и иные авторизационные данные.
- Резервирование и дублирование всех подсистем, которые содержат важную информацию.
- Перераспределение сетевых ресурсов, в случае отказа какого-то из модулей системы
- Обеспечение возможности применять резервные системы электрического питания.

Для обеспечения безопасности ЭПС в рамках организационно-правового поля, применимы следующие меры:

- Разработка внутренней документации, устанавливающей правила обработки конфиденциальной информации электронного платежного средства
- Проведение периодических инструктажей, позволяющих повышать грамотность персонала банковских учреждений в сфере информационной безопасности
- Разграничения сфер ответственности для исключения вероятности возникновения ситуации, при которой большая часть учетных данных (паролей и т.д.) может оказаться в руках одного субъекта.
- Составление графика резервного копирования наиболее важных модулей АБС (автоматизированной банковской системы)
- Просвещение населения с применением СМИ и Интернета в сфере безопасного применения ЭПС.

Можно сделать вывод о том, что для того, чтобы электронное средство платежа стало безопасным видом совершения транзакций наука, технологии, законодательная база, а также общество в целом должны сделать немало шагов на пути к развитию и усовершенствованию различных методов защиты информации от посягательств криминальных элементов.

***

1. Федеральный закон от 31 июля 2020 г. N 259-ФЗ "О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации"
2. Стандарт Банка России СТО БР ИББС-1.0-2014 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации/ Общие положения"
3. Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности» (СТО БР ИББС-1.1-2007)
4. Атаманов, Г. А. О банковской безопасности и безопасности банков [Текст] / Г. А. Атаманов // право и безопасность . – 2013. – № 1-2. – С. 79–85.
5. Годовой отчет 2016 [Электронный ресурс] // Сбербанк. – Режим доступа: <http://www.sberbank.com/ru/investor-relations/reports-and-publications/annual-reports>, свободный
6. Меры безопасности [Электронный ресурс] // РоссельхозБанк. – Режим доступа: <http://www.rshb.ru/security/>, свободный.

Митина О.А., Карклис А.Д.

Цифровые двойники как «передовая технология» в современном мире

*МИРЭА – Российский технологический университет
(Россия, Москва)*

doi: 10.18411/lj-03-2021-08

idsp: ljjournal-03-2021-08

Аннотация

В эпоху Четвертой промышленной революции («Индустрии 4.0») лидирующие мировые позиции занимают те высокотехнологичные предприятия, которые осуществляют цифровую трансформацию производства, тем самым открывая возможности достижения принципиально нового уровня разрабатываемой и производимой продукции.

В статье показано, что термин «цифровой двойник» (ЦД, Digital Twin, DT) получил большое распространение в настоящее время. Возникла ситуация, когда без рассмотрения истории становления термина, практики его применения в разных отраслях и разных научных школах было трудно осмыслить, что же вкладывается в это понятие в том или ином случае [5].

Ключевые слова и фразы: цифровой двойник, Индустрия 4.0, киберфизическая система, передовая технология.

Abstract

In the era of the Fourth Industrial Revolution («Industry 4.0»), the leading global positions are occupied by those high-tech enterprises that carry out the digital transformation of production, thereby opening up opportunities to achieve a fundamentally new level of developed and manufactured products.

The article shows that the term «digital twin» (DD, Digital Twin, DT) has become widely used at the present time. There was a situation when without considering the history of the formation of the term, the practice of its application in different industries and different scientific schools, it was difficult to understand what is meant by this concept in this or that case [5].

Key words: digital twin, Industry 4.0, cyber-physical system, advanced technology.