РАЗВИТИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ФИНАНСОВО-КРЕДИТНОЙ СФЕРЕ

Морозов Ростислав Анатольевич

студент, Тольяттинский государственный университет, РФ, Республика Коми, г. Сыктывкар

DEVELOPMENT OF INFORMATION TECHNOLOGIES IN THE FINANCIAL AND CREDIT SPHERE

Rostislav Morozov

Student, Togliatti State University, Russia, Komi Republic, Syktyvkar

Аннотация. Банковская система - наиболее защищённая сфера экономики с точки зрения кибербезопасности. Причины вполне понятна- риски экономических потерь в случае кибератак прямые и наблюдаемые. В то же время финансовые компании имеют достаточно финансов и мотивацию для качественного ИТ развития и систем информационной безопасности.

Инциденты информационной безопасности, связанные с незаконными транзакциями, широко распространены и не теряют актуальности. Автор исследует процессы на данный момент в зоне риска, а какие хорошо продуманы, а их риски на сегодня минимизированы.

По статистике видно, что транзакции между клиентами и банковской системой являются безопасными и наиболее частыми целями киберпреступников.

Abstract. financial organizations are the most secure sector of the economy in terms of information security. The reasons are obvious - the risks of economic losses in the case of cyber incidents are direct and observable. At the same time, financial institutions have a sufficient budget and motivation for the qualitative development of it and information security systems.

However, information security incidents related to illegal transactions are now widespread and do not lose their relevance. The author examines which processes are currently at risk, and which are already well thought out, and their risks are currently minimized.

Statistics show that transactions between the user and the banking system are the least secure and most frequent targets of cybercriminals. Therefore, the transactions of the "client device - Bank backend" level are considered below. Internal and interbank payment transactions are not covered in this article.

Ключевые слова: облачные технологии, модель, метод STEM, принятие решений, многокритериальная оптимизация, сервис, линейное программирование.

Keywords: cloud technologies, model, STEM method, decision making, multi-criteria optimization, service, linear programming.

В прошлом году ЦБ обратил внимание на постоянный мониторинг информационной безопасности и развитие FinCERT фидов, а также защиту от мошеннических платёжных транзакций и переводов (мошенничества). Законодательно усилены полномочия систем по борьбе с мошенничеством и возможность банка оперативно приостанавливать подозрительные переводы и временно блокировать электронные средства платежа при подозрении на компрометацию на срок до двух рабочих дней (причины для подозрений: совпадение параметров платежа с базой данных мошеннические устройства или аккаунты, ненормальные параметры платежа (например, сумма и частота, место платежа и т. д.). Банк информирует клиента, запрашивает подтверждение о возобновлении платежа и, таким образом, блокирует или возобновляет платёж, даёт рекомендации по снижению риска возникновения подобных ситуаций. Аналогичный механизм запускается после уведомления о мошеннической транзакции пострадавшим клиентом банка - до 5 дней для подтверждения платежа (если средства еще не были переведены, крайне важно сообщать о подобных операциях оперативно!).

Постановление 683-Р напрямую связано с защитой платежей клиентов и противодействием денежным переводам без согласия клиента. Основные требования 683-П: сертификация прикладного программного обеспечения в ФСТЭК на отсутствие NDV или анализ уязвимостей на OUD4, обеспечение целостности и надежности защищаемой информации, защита при передаче по каналам связи, регистрация и хранение 5 лет информации. на все защищённые данные сотрудников и клиентов. Плюс отправка информации о происшествии в FinCERT.

В России в активной стадии разработки находится проект сервиса быстрых межбанковских платежей (FPS) - реализация межбанковских переводов между клиентами с использованием номера мобильного телефона, что значительно упрощает процедуру перевода. Подключение кредитных организаций к СПП в настоящее время является добровольным, но большое количество банков уже заявили о своем намерении. Центральный банк Российской Федерации, в свою очередь, уже ввёл некоторые нормативные и организационные концепции, связанные с этой системой, в Постановлении 672-П, то есть требования безопасности к такому виду переводов также уже активно прорабатываются.

Стандарты PCI SSC не закреплены на государственном уровне как обязательные, точнее, только некоторые штаты в США ввели их на законодательном уровне. Но, благодаря требованиям платежных систем, они выполняются в большом количестве организаций. Исследование компании Cisco по выполнению стандарта в США от 2011 года выявило следующее:

Из всех отраслей лучше всех выполняют требования PCI DSS предприятия розничной торговли и финансовые организации; розничная торговля самым серьёзным образом отнеслась к внедрению и реализации этого стандарта.

При этом 85% опрошенных считают, что в настоящий момент их организации способны успешно пройти аудит PCI DSS, а 78% успешно прошли такой аудит с первого раза.

Наиболее высокие результаты в данной области показали государственные организации: 85% госучреждений успешно прошли аудит PCI DSS с первого раза. Хуже всего проходили такой аудит медицинские организации (72%).

67% опрошенных руководителей компаний и членов советов директоров считают PCI DSS весьма важной инициативой; кроме того, 60% опрошенных подтвердили, что стандарт PCI DSS может стимулировать другие проекты, связанные с сетями и сетевой безопасностью.

10 лет назад компания «Verizon» начала отслеживание выполнения стандарта PCI DSS среди компаний. Отчет «Verizon PCI Report» от 2019 года показывает, что динамика поддержания соответствия ранжируется от 22% (2009 г.) до 7,5% (2011 г.) и 55,4% (2016 г.) – см. рисунок 1. И сейчас, спустя 15 лет после выхода стандарта, более 35% поддерживают системы защиты в полностью актуальном соответствии стандарту, многие компании находятся в процессе проработки подобных процедур.

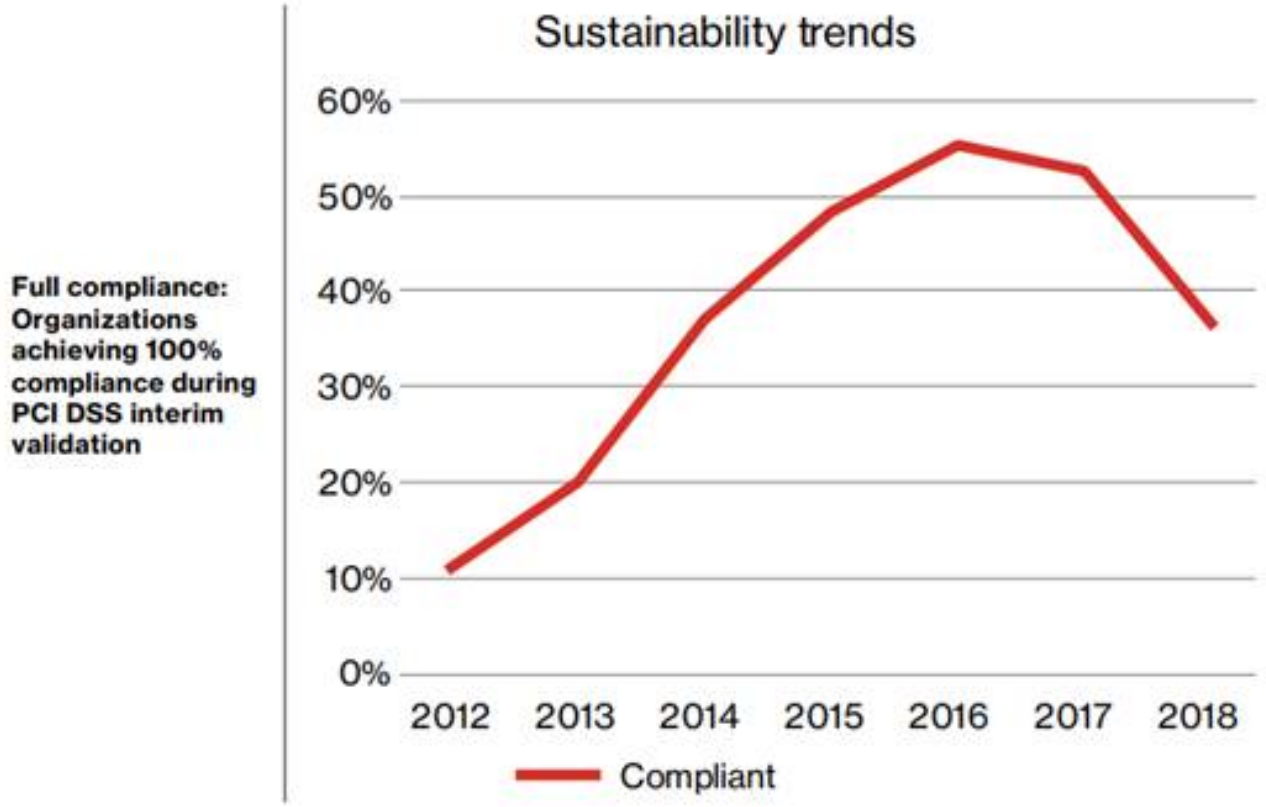

Рисунок 1. Динамика поддержания систем защиты на соответствие стандарту PCI DSS по годам

В условиях технологического рывка финансовой сферы технология 3D Secure получила достаточно широкое распространение благодаря удобству для пользователя при высоком уровне защищённости.

Кроме того, в России с 2020 года требования ЦБ РФ к финансовым организациям становятся обязательными. А с июля 2016 года действует закон «О внесении изменений в 54-ФЗ «Об использовании кассовых аппаратов при расчетах наличными и / или расчетах платежной картой» (кассовые аппараты – далее «ККТ»). действует, обязывая, в том числе, проводить все операции онлайн-платежей с использованием кассового аппарата, подключенного к системе онлайн-передачи налоговых данных в ФНС.

Для этого используются операторы налоговых данных (FDO), которые имеют специальные технические средства для обработки налоговых данных в реальном времени, создания, проверки и хранения налоговых баз данных, а также передачи их в налоговую администрацию. Для конечного пользователя этот закон полезен тем, что для любой онлайн-покупки он получает подтверждающий чек по почте или другим способом, который сам по себе является налоговым документом. ОФД, в свою очередь, обладает техническими средствами защиты налоговой информации и необходимыми лицензиями ФСТЭК и ФСБ.

Список литературы:

1. Официальный сайт компании Boston Consulting Group: https://www.bcg.com/ru-ru/ (дата обращения 04.09.2020)

2. Балдин, К.В. Информационные технологии в менеджменте / К.В. Балдин. - М.: Academia, 2018. - 203 с.

3. Гавриленкова, И.В. Информационные технологии в естественнонаучном образовании и обучении.Практика, проблемы и перспективы профессиональной ориентаци. Монографии / И.В. Гавриленкова. - М.: КноРус, 2018. - 284 с.