УДК 330.132.8

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В БАНКОВСКОЙ СФЕРЕ КЫРГЫЗСКОЙ РЕСПУБЛИКИ

Жусуева Наргиза Жолдошбековна, преподаватель КГТУ им. И. Раззакова, Кыргызстан, 720044, г.Бишкек, пр. Ч.Айтматова 66, e-mail: jusueva84@mail.ru

Саматова Ж.Б., магистрант, КГТУ им. И. Раззакова, Кыргызстан, 720044, г.Бишкек, пр. Ч.Айтматова 66, e-mail: pearl_96.06@list.ru

Аннотация. Данная статья посвящена определению влияния информационной безопасности на деятельность банков Кыргызской Республики. С того момента как банковская сфера начала развиваться, появился криминальный интерес. И этот интерес в основном связан не только с хранением денежных средств в банковских организациях, и так же там хранятся многозначительные и особенно конфиденциальные данные о финансовой жизни общества, фирм, учреждений и так же данные всей страны. Нынче в связи широким увеличением электронных пополнений и оплат, карточек авансовых платежей, как банков, так и их клиентов стали объектом информационных атак.

Ключевые слова: банковская сфера, защитные механизмы, банковские атаки, информационные данные, информационные системы, репутация, киберпреступность.

INFORMATION SECURITY IN BANKS OF KYRGYZSTAN

Zhusuyeva N. ZH., Lecturer of the department «Information Systems and Technologies» Faculty of Engineering and Economic at KSTU named after I.Razzakov, e_mail.: jusueva84@mail.ru

Samatova Zh. S., Master.... student of the group «Information Systems and Technologies» at KSTU named after I.Razzakov, tel. (+996) 705 12-34-07 e_mail.:pearl_96.96@list.ru

Abstract. This article is devoted to determining the impact of information security on the activities of banks in the Kyrgyz Republic. Since the banking sector began to develop, and criminal interest appeared. And this interest is mainly not related to only with the storage of funds in banking organizations, and also there significant and especially confidential data on the financial life of society, firms, institutions, as well as data from the entire country are stored. Today, due to the wide increase in electronic deposits and payments, advance payment cards, both banks and their customers have become the object of information attack.

Keywords: banking sector, security mechanisms, bank attacks, information data, information systems, reputation, and cybercrime.

Информационная безопасность банковской сферы в Кыргызской Республике

Информационная безопасность банка или например в других также сферах – это состояние защищенности всех его информационных данных от других конкурентов. [2] Именно репутация и конкурентоспособность среди других банков зависят от безопасности.

Безопасность информационных данных в банковской сфере и его защита необходимо защищать на максимально высоком ярусе, чтобы быть всегда готовым на атаку любых попыток преступников, и так же рабочего персонала самой корпорации. Хороший и высокий уровень информационная устойчивость кредитной корпорации позволяет предотвратить очередные факторы риска например, ссвоеобразностью банковских систем состоит:

- сбережение и обработка большущего размера данных о экономическом состоянии и работы банка.
- владеть денежными средствами и так же иметь инструменты для обороны информации, приводящие к безысходным денежным результатам.
- банки не имеют все шансы быть всецело прикрыты, например, как обязаны, отвечать прогрессивным притязаниям по уровню сервиса покупателей (владеть систему интернет-банкинга, сеть банкоматов, присоединенных к каналам связи совместного использования и др.).

Это своеобразность приводят к тому, собственно, что информационные данные кредитных корпораций считаются желанной целью злодеев и нуждаются в нешуточной обороне. Источниками опасностей информационной защищенности банков это:

- наружные и внутренние вредные и незлобные информационной защищенности данных
- неполадки и отклонение программных систем и аппаратных компонент
- природные и техногенные аварии, не соблюдающие обычную работу информационных систем и иных приборов.

Финансовые данные – самая популярная цель среди киберпреступников в информационном пространстве. Криминальный бизнес, как и легальный, направлен на получение и максимизацию денежной прибыли, а наиболее доходные данные находятся в распоряжении финансовых организаций. В отличие от кибератаке на критическую инфраструктуру, атаки на банки и кредитно-финансовые кооперативы осуществляются без какой-либо идеологической подоплеки, поэтому банки всегда подвергаются атакам, на всех уровнях их ИТ-инфраструктуры и в любой точке мира. [1]

Основной целью злодеев атакующих информационные системы банков, считается получение доступа над информацией кредитной организации для дальнейшего совершения нелегальных операций или же компрометации банка по заказу злонамеренных соперников. Важно помнить, что только одна уязвимость, используемая злоумышленником, может привести к успешной кибератаке на организацию, поскольку финансовые услуги взаимосвязаны и из цепочки единичных атак, не представляющих непосредственной опасности в каждом конкретном случае, можно успешно проникнуть в критические системы. Нашему государству необходимо уделить особое внимание концепции «кибербезопасности» – это осуществление мер по обороне систем, а так же программных обеспечений от цифровых атак. [4]. Эти атаки как правило ориентированы на получение контроля к секретной информации, ее перемена и устранение вымогательство денег у пользователей или нарушение нормальной работы компаний.

Кыргызская Республика занимает 103-е место согласно исследованиям национального банка - 19% (статья с академии электронного управления Эстонии), и 96-е место по кибербезопасности – 28% [5]

Система информационной защищенности банка обязана:

- должна обеспечивать высокую надежность компьютерных систем даже в случае
- чрезвычайных ситуаций, поскольку банк несет ответственность не только за свои средства, но и за деньги клиентов − лиц не состоящих в списке для использования автоматизированной системы и доступ к его ресурсам должны регистрировать только в новый пользователь;
- все рабочие места и серверы банка должны использовать средства антивирусной защиты.
- создание виртуальных сетей (VPN) разрешает действенно гарантировать конфиденциальность данных, ее защиту от прослушивания или же затруднений при передаче данных.
- обеспечение комплекса процессуальных мер защиты от несанкционированный доступ пользователей интернета.

Количество устройств, которые могут быть заражены вредоносным кодом, который крадет финансовые данные или берет под контроль систему, чрезвычайно Практика показывает, что большинство злодеяния связанные с не техническими ситуациями совершаются работниками не знакомыми с компьютерной техникой. Однако они отличаются такими качествами: у них есть доступ к персональному компьютеру и им известно, какую роль играет в их учреждении. Преступления такого рода происходят в основном крадут пароль чтобы получить доступ к файлам информации банка, которые сохранены в памяти компьютера. Имея пароль и определенные навыки, вы можете вводить секретные файлы, изменять их содержимое и т. д. Эти преступления довольно просто расследовать, и, усиливая защиту системы, их легко предотвратить. [3]

Типы и субъекты угроз на примере карты Visa – жульничества продавца 27.6, потерянные карты 9.5, фальшифка карт 17.7, смена рельефа карты 9.1, неправильное использование 9.4, жульничества по телефону 6.3, жульничества при пересылке на электронную почту 8.5, сговор с собственником карты 2.4; так же нарушение может вызываться либо ошибкой людей, либо неправильным функционированием, либо природными факторами (например, пожар или наводнение), либо преднамеренными злоумышленными действиями, либо не соблюдением сохранности конфиденциальности информации, целостности, доступности, учетности или недоказуемости, влияющее на систему, сервис и/или сеть и их составные части. [6]

Решение. Исходя из этих наблюдений, я пришла к выводу, что уровень знаний по основам компьютерной безопасности очень низок в нашей стране. На самом деле риски будущих инцидентов

будут связаны не столько с технологическими уязвимостями, сколько с низкой компетенцией пользователей. В стране не хватает людских ресурсов в сфере информационной безопасности. Мы не применяем международные стандарты информационной безопасности – никто просто не считает нужным их соблюдать. Необходимо срочно приступить к разработке политики информационной безопасности нашего государства, постепенно внедрять международные стандарты и передовой опыт в области информационной безопасности, совершенствовать законодательную базу и вводить ответственность за несоблюдение требований ИГ. Подготовка кадров и внедрение специальностей «Информационной системы» в университетские программы позволит постепенно снизить риски до приемлемого уровня. Развитие информационных технологий позволяет существенно сократить дистанцию между производителем и потребителем банковских услуг, значительно обостряет межбанковскую конкуренцию.

Заключение

Многие инциденты остаются незамеченными. Коммерческий сектор пытается «замять» любую информацию об инцидентах-взломах, утечках или компрометации конфиденциальной информации, поскольку это приводит к значительным репутационным рискам. Серьезной проблемой является также слабая законодательная база в области информационной безопасности. В связи с отсутствием стандартных правил, потеря определенных и личных данных и другие нарушения не учитываются, и меры во избежания таких ситуаций не проводятся. За инциденты, которые уже произошли, никто не был привлечен к ответственности, никаких системных выводов сделано не было. Позитивным шагом стало введение. Национальным банком стандарта безопасности для банков второго уровня, но его необходимо пересматривать каждый год [1]. Насколько мне известно, стандарт Национального банка уже устарел. Как и для любого другого госоргана того же МВД или Государственной регистрационной службы, которая работает с очень чувствительными биометрическими данными – стандартов вообще нет. Когда речь заходит об ответственности в случае утечки данных, никто даже не будет оштрафован, потому что ни стандарты, ни ответственность за их нарушение не прописаны. Законы несовершенны, и шагов по исправлению ситуации пока не видно. Современный подход к безопасности в Кыргызской Республике-это безопасность через безвестность. Это ни к чему хорошему не приводит, потому что у людей и работников этой сферы нет общего знания по информационной безопасности в государстве.

Список литературы

1. О доступе информации, находящиеся в ведении государственных органов и органов местного самоуправления Кыргызской Республики: закон КР от 28 дек. 2006 г;
2. Об информации персонального характера: закон КР от 14 апр. 2008 г. No58
3. Дозлиев, М. И. Проблемы безопасности: теоретико-методологические аспекты 2001г;
4. Молдалиев, О. А. Современные вызовы безопасности Кыргызстана и Центральной Азии;
5. Нормативные акты Национального банка Кыргызской Республики [Электронный ресурс] – Режим доступа: https://www.nbkr.kg/contout.jsp?item=103&lang=RUS&material=259906
6. Нормативные акты Национального банка Кыргызской Республики [Электронный ресурс] – Режим доступа: https://www.nbkr.kg/contout.jsp?item=106&lang=RUS&material=90348