УДК: 681.518: 004.056.5

НЕКОТОРЫЕ ВОПРОСЫ НЕПРЕРЫВНОСТИ ФУНКЦИОНИРОВАНИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ «ОПЕРАЦИОННЫЙ ДЕНЬ БАНКА» БИШКЕКСКОГО ФИЛИАЛА НАЦИОНАЛЬНОГО БАНКА ПАКИСТАНА

Табалдиев Уларбек Кичикович, *магистрант, Кыргызский государственный технический университет им. И. Раззакова, Кыргызстан, 720044, г. Бишкек, пр. Ч.Айтматова 66, e-mail: ular.tabaldiev@mail.ru*

Научный руководитель: Салиев Алишер Борубаевич, *д.ф.-м.н., профессор, Кыргызский государственный технический университет им. И. Раззакова, Кыргызстан, 720044, г. Бишкек, пр. Ч.Айтматова 66, e-mail: pocs@mail.ru*

Аннотация. В работе коротко отмечены характерные особенности ИБ в банковской сфере, автоматизированных систем обработки данных в ряде банков КР и в частности АБС Бишкекского филиала НБК Пакистана. На основе изучения состояния проблем и вопросов защиты информации выделены актуальные вопросы, наиболее важные угрозы, особенности модели нарушителя, а также ряд задач и мер, решение которых направлено на достижения основной цели политики ИБ и улучшения системы безопасности данного банка.

Ключевые слова: безопасность информации, информационные ресурсы, модель угроз, модель нарушителя, мониторинг.

Аббревиатуры:

АБС – автоматизированная банковская система;
ИБ – информационная безопасность;
ИС – информационная система;
ОДБ – операционный день банка;
НСД – несанкционированный доступ;
НРД – нерегламентированные действия в рамках предоставленных полномочий.

SOME ISSUES OF CONTINUITELLY FUNCTIONING AN AUTOMATED SYSTEM "OPERATING DAY OF THE BANK" OF THE PAKISTAN NATIONAL BANK'S BISHKEK BRANCH

Tabaldiev Ularbek Kichikovich, *Master's Degree student, Kyrgyz State Technical University I. Razzakov, Kyrgyzstan, 720044, Bishkek, 66 Aitmatov Ave., e-mail: ular.tabaldiev@mail.ru*

Scientific adviser: Saliev Alisher Borubaevich, *Dr. Sci. (Phys.–Math.), Professor, Kyrgyz State Technical University I. Razzakov, Kyrgyzstan, 720044, Bishkek, 66 Aitmatov Ave., e-mail: pocs@mail.ru*

Abstract. In the paper are briefly and in general outline the characteristic features of information security in the banking sector, automated data processing systems in a number of banks in the Kyrgyz Republic and, in particular, the ABS of the Bishkek branch of the NB of Pakistan. Based on the study of the state of problems and issues of information security, the most important issues of its provision, the most important threats, the features of the intruder model, as well as a some of tasks and measures, the solution of which is aimed at achieving the main goal of the information security policy and improving the security system of this bank, are identified.

Keywords: information security, information assets, model, threat, intruder, monitoring.

1⁰. Введение. Финансовый сектор Кыргызской Республики одним из первых активно начал переход к цифровизации, а в настоящее время здесь успешно развиваются онлайн-сервисы на базе систем электронных денег и мобильных приложений. К ним относятся банкоматы, платежные терминалы, интернет банкинг, мобильный банкинг. Кроме этого, набирают популярность безналичной оплаты – оплата с помощью QR-кода и бесконтактные оплаты – NFC – платежи.

Соответственно, большинство бизнес-процессов коммерческого банка и их эффективность сильно зависят от технологий хранения, обработки и обмена информацией. В то же время информационные активы, которые используются в этих процедурах сталкиваются с различными типами угроз и если этим угрозам удастся использовать уязвимости, присутствующие в информационных активах, то конфиденциальность, целостность и доступность этих активов могут быть нарушены. Чтобы снизить риски использования этих угроз, необходимо реализовать определенные меры контроля/мониторинга.

Главной целью злоумышленника является получение доступа и контроля над информационными активами на уровне бизнес-процессов. Прямые атаки на уровне бизнес-процессов более эффективны для злоумышленника и более опасны для банка, чем атаки, осуществляемые через иные уровни, требующие специфических опыта, знаний и ресурсов.

Другой целью злоумышленника может быть нарушение функционирования бизнес-процессов коммерческого банка, например, распространение вредоносных программ или нарушение правил эксплуатации компьютеров или их сетей.

Кроме того, более 80% всех преступлений связаны с использованием автоматизированных систем обработки информации коммерческого банка. Следовательно, при создании и модернизации таких систем необходимо уделять особое внимание обеспечению ее информационной безопасности.

Именно такие проблемы в настоящее время наиболее актуальны и наименее изучены.

2^0. Обзор и анализ существующих систем. По состоянию на 1 апреля 2021 года в Кыргызской Республике действуют 23 коммерческих банка [7], каждый из которых имеет свою систему управления информационной безопасностью и способы решения операционной деятельности банка.

В настоящее время существует не один вариант решения операционного дня банка, разработанные различными компаниями-разработчиками ПО для банков. Каждый из них имеет свои особенности, однако порядок выполнения банковских операций одинаков.

Для того чтобы охватить широкий круг пользователей в этой области компании-разработчики пытаются создать многофункциональную автоматизированную систему. Это значительно облегчает работу сотрудников коммерческого банка, но многофункциональность может способствовать утечке данных. Соответственно увеличивается количество объектов, подлежащих к защите.

Таблица 1.

Сравнение существующих систем

	АБС	Наименование банка
1.	Colvir, Великобритания	ОАО «Кыргызкоммерцбанк», ОАО Банк «Бай-Тушум», ОАО «Халык Банк Кыргызстан»
2.	ЦФТ-Банк, РФ	ОАО «Керемет Банк», ОАО «Коммерческий банк Кыргызстан»
3.	RS-Bank, РФ, R-Style Softlab	ОАО «Айыл Банк», ОАО «Оптима Банк», ОАО «РСК Банк»
4.	FLEXCUBE, Oracle Financial Services	ЗАО «Кыргызский Инвестиционно-Кредитный Банк»
5.	GNI, Азербайжан	ЗАО «ЭкоИсламикБанк»
6.	CDF, Турция	ЗАО «Демир Кыргыз Интернэшнл Банк»
7.	Аврора, Кыргызстан	ОАО «Евразийский Сберегательный Банк»
8.	Online Bank, Кыргызстан	ЗАО «Кыргызско-Швейцарский Банк», ОАО «Капитал Банк», ОАО РК «АМАНБАНК», ЗАО АКБ «Толубай», ОАО «Дос-Кредобанк», ОАО «ФинансКредитБанк», ЗАО «ФИНКА Банк», ЗАО «Банк Компаньон»
9.	ОДБ, Кыргызстан	ЗАО «Банк Азии», ОАО «Бакай банк», Бишкекский филиал Национального банка Пакистана

Основная цель коммерческих банков – отказаться от EXE – файлов и использовать онлайн режим. Из таблицы видно, что большинство коммерческих банков перешли на новую АБС «Online Bank», которая предлагает компания «Финанс Софт», Кыргызстан.

На текущий момент все изменения АБС ОДБ вносятся в головном офисе, затем готовится новый EXE-файл, и он передается по всем филиалам и удаленным сберкассам, занимая время и трафик каналов связи. И так каждое изменение. В новых условиях изменения делаются на сервере и все (филиалы и сберкассы) сразу их используют. В действующем АБС ОДБ не существует чистого онлайн – соединения с головной базой данных (каждый филиал работает со своим сервером и только

в конце дня данные с филиального сервера передаются в головной сервер). Таким образом, в течение дня невозможно получить совокупную информацию в программе о состоянии дел в филиалах.

Действующая АБС ОДБ написана на языке VISUAL FOXPRO, занимающем -согласно рейтингу TIOBE [8]- 33 место, и найти программистов знающих этот язык на сопровождение программы коммерческим банкам тяжело.

Преимуществом новой АБС «Online Bank» является то, что все смогут работать непосредственно с сервером головного офиса напрямую. АБС основана на архитектуре микро-сервисов с широким использованием современных технологий: WCF, ASP.Net, языка разработки C# и базы данных Microsoft SQL Server 2012 R2 и выше. Вся функциональность АБС доступна через любой веб-браузер.

3^0. Значение мониторинга ИБ для обеспечения защиты информации. В качестве наиболее актуальных выделим следующие аспекты, связанные с обеспечением информационной безопасности банка, которые в значительной степени определяют значимость своевременного и эффективного мониторинга.

1. Выявление нарушений информационной безопасности в режиме реального времени и адекватное реагирование на них.

2. Обеспечение регулярного мониторинга инцидентов, связанных с деятельностью сотрудников банка и внешних нарушителей. Постоянное и непрерывное наблюдение за происходящим в АБС позволяет обеспечить ее защищенность.

3. Возможность оперативного обнаружения применения злоумышленниками новых средств и методов несанкционированного получения конфиденциальных информаций, появившихся в результате развития новых информационных технологий.

Несвоевременное обнаружение нарушений ИБ и непринятие адекватных мер по защите информации может привести к существенному снижению уровня защищенности объектов, обеспечиваемой системой ИБ. Следовательно, необходимо разработать такую процедуру мониторинга и последующей ее реализации, которая позволила бы системе ИБ своевременно выявлять любые, в том числе и ранее неизвестные, угрозы ИБ.

В отсутствие такой процедуры, банк будет на несколько шагов отставать от действий злоумышленников и узнавать о произошедших утечках информации из внешних источников, что не может не повлечь за собой крупных финансовых и репутационных потерь [9].

4^0. Этапы построения системы защиты информации. Защищаться следует от всевозможных (внутренних и внешних) угроз, которые проявляются через действия нарушителей. Угрозы возникают в случае наличия в системе уязвимостей - свойств системы, которые могут привести к нарушениям информационной безопасности.

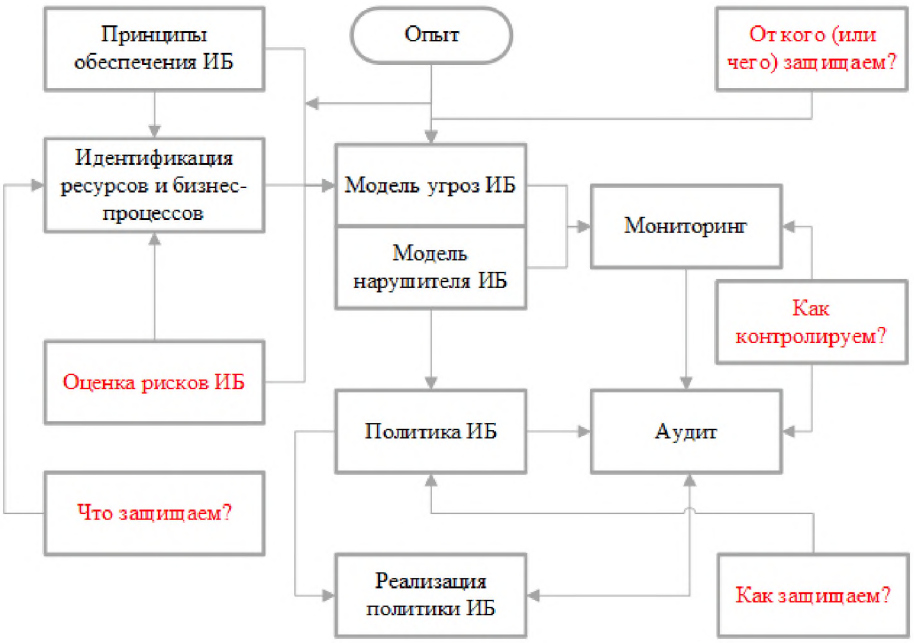

Рис.1. Принципы обеспечения ИБ.

Составление моделей угроз и нарушителя являются обязательным этапом проектирования системы защиты информационной безопасности. Для обнаружения и предотвращения атак необходим регулярный мониторинг, т.е. поиск и анализ уязвимостей системы, регулярный аудит (внешний и внутренний) информационной безопасности [1].

Основными источниками угроз ИБ являются:

- неблагоприятные события природного, техногенного и социального характера;
- террористы и криминальные элементы;
- зависимость от поставщиков/провайдеров/партнеров/клиентов;
- сбои, отказы, разрушения/повреждения программных и технических средств;
- работники банка, реализующие угрозы ИБ с использованием легально предоставленных им прав и полномочий (внутренние нарушители ИБ);
- работники банка, реализующие угрозы ИБ вне легально предоставленных им прав и полномочий, а также субъекты, не являющиеся работниками банка, но осуществляющие попытки НСД и НРД (внешние нарушители ИБ);
- несоответствие требованиям надзорных и регулирующих органов, действующему законодательству.

Классические угрозы безопасности информации – это вывод системы из строя, отказ в обслуживании и компрометация или подмена данных. И эти угрозы слишком реальны.

Таблица 2.

Модель угроз ИБ

Угроза ИБ	ИА	Среда обработки ИА	Последствия реализации угрозы ИБ для ИА
Сбои в электро-снабжении	База данных	СУБД	Прекращение работы БД
	Несохраненные данные о клиенте	АРМ	Утеря несохраненных данных
Внедрение вредоносной программы	Служебная тайна	АРМ, серверы, системные ПО	Нарушение доступности, целостности, конфиденциальности информации
Сбой в работе ПК	Несохраненные данные о клиенте	АРМ	Нарушение целостности и/или доступности информации
Перехват аутенти-фикационных данных	Аутентификацио нные данные	Интернет-шлюз	Компрометация аутентификационных данных
Угроза хищений информации	Информация о клиенте	АРМ	Нарушение конфиденциальности информации
	Информация о клиенте	Периферийные устройства	Компрометация данных, отправленных на печать. Нарушение конфиденциальности

У различных ИС, а также объектов одной ИС может быть разный спектр угроз, определяемый особенностями конкретной ИС и её объектов и характером возможных действий источника угрозы.

Модели угроз составляются на основе постоянно меняющихся данных и поэтому должны регулярно пересматриваться и обновляться.

Таблица 3.

Модель нарушителя ИБ

Тип нарушителя	Доступные ресурсы для реализации угрозы ИБ	Мотивация	Метод реализации угроз ИБ
Внутренний	Физический доступ в здание/ помещение, в котором находятся компоненты	Любопытство или желание самореализации; Выявление компрометирую щей информации	Атака непосредственно на инфраструктуру сети
			Осуществление НСД к ресурсам при физическом доступе
			Умышленное внедрение вредоносных программ

		для дальнейшей ее продажи и получения финансовой выгоды	Недопустимое изменение характеристик технических средств, в том числе, разрушение или уничтожение технических средств
Внешний	Логический доступ к сети, физический доступ к сетевому оборудованию		Атака непосредственно на инфраструктуру сети
			Осуществление логического НСД к ресурсам при физическом доступе
			Умышленное внедрение вредоносных программ
			Использование утраченных/похищенных носителей информации
			Недопустимое изменение характеристик технических средств, в том числе, разрушение или уничтожение технических средств
Внутренний	Физич. доступ к оборудованию для работы сети, логич. доступ сети, физич. доступ в здание/помещение, где находятся главные компоненты		Неисполнение или ненадлежащее исполнение своих должностных обязанностей
			Несоблюдение требований внутренних документов, регламентирующих деятельность по ИБ
			Умышленное внедрение вредоносных программ
			Умышленное использование активов в целях, отличных от целей функционирования сети по причине отсутствия персонала

С точки зрения защиты информации НСД может иметь следующие последствия: утечка обрабатываемой конфиденциальной информации, а также ее искажение или разрушение в результате умышленного нарушения работоспособности АБС.

Нарушителем может быть любой человек из следующих категорий сотрудников:

- штатные пользователи АБС;
- программисты, сопровождающие системное, общее и прикладное программное обеспечение системы;
- обслуживающий персонал (инженеры);
- системные и сетевые администраторы, администраторы БД;
- и другие сотрудники, имеющие санкционированный доступ к ИТ (в том числе подсобные рабочие, уборщицы и т.д.).

Под безопасностью АБС понимается защищенность от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, модификации или разрушения ее компонентов. Следует отметить, что природа воздействия может быть самой различной. Это и попытки проникновения злоумышленника, и ошибки персонала, и стихийные бедствия (ураган, пожар), и выход из строя составных частей АБС.

Важным этапом процесса обеспечения безопасности АБС является разработка Политики информационной безопасности. Если отсутствует Политика ИБ, невозможно даже четко провести разграничение между санкционированным (легальным) доступом к информации и НСД [2].

Политика ИБ – это совокупность правил, процедур, практических методов и руководящих принципов в области ИБ, используемых организацией в своей деятельности. Политика ИБ определяет цели и задачи обеспечения ИБ при ее работе и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуются сотрудники банка в своей деятельности.

Основной целью, на достижение которой направлены все положения Политики ИБ, является защита информационных ресурсов от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, её носители, процессы обработки и передачи, а также минимизация рисков ИБ. Для

достижения этой цели необходимо обеспечивать эффективное решение следующих задач:

- своевременное выявление, оценка и прогнозирование источников угроз ИБ;
- создание механизма оперативного реагирования на угрозы ИБ;
- предотвращение и/или снижение ущерба от реализации угроз ИБ;
- защита от вмешательства в процесс функционирования ИС посторонних лиц;
- обеспечение непрерывности бизнес-процессов;
- достижение адекватности мер по защите от угроз ИБ;
- изучение партнёров, клиентов, конкурентов и кандидатов на работу;
- недопущение проникновения структур организованной преступности и отдельных лиц с противоправными намерениями;
- выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности сотрудников;
- соответствие требованиям законодательства, нормативно-методических документов и договорным обязательствам в части ИБ;
- повышение деловой репутации и корпоративной культуры.

Политика ИБ распространяется на все бизнес-процессы банка и обязательна для применения всеми сотрудниками и руководством банка, а также пользователями его информационных активов.

Банк должен реализовать все меры обеспечения информационной безопасности в строгом соответствии с действующим законодательством Кыргызской Республики и договорными обязательствами.

Заключение. В процессе исследования данной работы изучены, АБС «ОДБ», меры и средства для ее защиты, официальные документы банка, нормативная и методическая документации, которые позволили решить многие поставленные задачи.

По итогам проведенной работы для дальнейшего улучшения системы безопасности банка считаем необходимым провести следующие мероприятия:

- установить программное обеспечение для защиты от спама и фишинга;
- контролировать соблюдения правил хранения документов;
- использовать специальные сетевые оборудования;
- ограничить доступ к файлам, каталогам;
- регулярный мониторинг работы всех информационных систем и информационных инфраструктур.

Список литературы

1. Вострецова Е.В. Основы информационной безопасности: Учебное пособие для студентов вузов – Е. : Изд-во Уральского университета, 2019. – 204 с.
2. Нестеров С.А. Информационная безопасность: Учебник и практикум для СПО – М. : Издательство Юрайт, 2018. – 321 с.
3. Методический документ "Методика оценки угроз безопасности информации" (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.)
4. СТО БР ИББС-1.0-2014. Обеспечение информационной безопасности организаций банковской системы РФ. М. 2014.
5. Стандарты по обеспечению информационной безопасности учреждений банковской системы КР. Б. 2004.
6. Информационные технологии в управлении банковской деятельностью [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/informatsionnye-tehnologii-v-upravlenii-bankovskoy-deyatelnostyu (дата обращения 01.04.21).
7. Перечень коммерческих банков Кыргызской Республики и их филиалов по состоянию на 1 апреля 2021 года [Электронный ресурс]. URL: https://www.nbkr.kg/index1.jsp?item=69&lang=RUS (дата обращения 01.04.2021).
8. Индекс TIOBE на апрель 2021г. [Электронный ресурс]. URL: https://tiobe.com/tiobe-index/ (дата обращения 01.04.2021).
9. Попов С.В., Шамкин В.Н. О влиянии состояний функционирования средств защиты информации на эффективность мониторинга инцидентов информационной безопасности банка //Вестник Тамбовского государственного технического университета. - 2011. - Т. 17. - №2.
10. Бексултанов, А. А. Совершенствование системы государственного бюджетного контроля / А. А. Бексултанов, Б. У. Абдыкадырова, Н. Р. Тойбаева // Известия Кыргызского государственного технического университета им. И. Раззакова. – 2020. – № 1(53). – С. 105-112.