канд. экон. наук, доцент
Е.Д. Чикина,
магистрант
Ю.А. Астахова,
студент
Н.А. Чикин
Белгородский государственный
технологический университет
им. В.Г. Шухова

ФИНЦЕРТ БАНКА РОССИИ КАК ОСНОВНОЕ ЗВЕНО ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ, ЭКОНОМИЧЕСКОЙ И ФИНАНСОВОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

В последнее время ключевой обязанностью любой страны мира является создание стабильной и эффективной финансовой системы, обеспечение информационной и экономической безопасности. Сегодня, когда масштабы и серьезность кибератак по всему миру неуклонно растет, это означает, что банкам необходимо уделять огромное внимание угрозам, исходящим от них.

Обзор финансовой системы за 2019–2020 гг., в котором выявляются ключевые уязвимости финансовой системы, выявил рост частоты, серьезности и сложности кибератак во всем мире, а также возможность повсеместных сбоев. Это также основная проблема тех, кто специализируется на управлении рисками в финансовом секторе. Как отмечают эксперты [8], киберинциденты по-прежнему считаются самым большим риском для финансовой системы абсолютно для всех стран мира.

Киберинциденты становятся все более частыми, усложняются и представляют реальную угрозу стабильности финансовой системы. Согласно данным, предоставленным компанией Advisen с 2014 по 2018 гг. в мировом финансовом секторе было совершено почти 5000 успешных кибератак. И эти атаки принесли убытки в размере более 4 миллиардов долларов.

Такие тревожные цифры подчеркивают, почему собственная кибербезопасность банка должна быть достаточно сильной, чтобы защитить ценные активы, будь то финансы, данные или сами клиенты.

«Около 90% ИТ-систем госорганов в России способны взломать не только высококвалифицированные хакеры, но и неопытные киберхулиганы. Такой вывод содержится в исследовании, подготовленном компанией «Ростелеком-Солар» по итогам анализа данных о 40 госорганизациях и органах власти федерального и регионального уровня» [2].

«По словам директора центра мониторинга и реагирования на кибератаки, киберхулиганы нацелены на несложную монетизацию и занимаются шифрованием серверов и компьютеров, скрытым майнингом криптовалюты, созданием из полученных ресурсов бот-сетей для организации DDoS-атак или фишинговых рассылок» [2].

«10 сентября 2020 года стало известно о создании Генеральной прокуратурой РФ межведомственной рабочей группы для борьбы с киберпреступлениями. В неё, помимо прокуроров, вошли представители МИДа, МВД, ФСБ, Следственного комитета и Минюста России» [2].

«Группа координирует деятельность всех правоохранительных органов в борьбе с киберпреступностью, а также вырабатывает консолидированную российскую позицию по проекту всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий (ИКТ) в преступных целях. Этот документ разрабатывается специальным межправительственным комитетом экспертов ООН» [6].

«Одной из наиболее актуальных проблем, требующих активизации международного сотрудничества, является значительный рост во всем мире, включая Россию, так называемой информационной преступности – криминальных посягательств, совершенных с использованием ИКТ» [6].

Именно государство является основным гарантом безопасности банковской системы. Основными функциями в этом случае являются: надежная законодательная база; сохранность банка и обеспечение его безопасности с учетом единого порядка, принципов и подходов во всей банковской системе; механизм, который будет связывать и координировать надзорные и исполнительные органы.

Для обеспечения выбранных государственных направлений в РФ существует ФинЦЕРТ Банка России который, являясь центральным звеном в обеспечении информационной, экономической и финансовой безопасности, противодействует кибератакам в банковской сфере и осуществляет развитие безопасности и киберустойчивости.

ФинЦЕРТ – «это Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере, специальное структурное подразделение Банка России (от CERT – computer emergency response team, группа реагирования на компьютерные инциденты)» [7]. Функции ФинЦЕРТ ЦБР представлены на рис. 1.

ФинЦЕРТ ЦБР обеспечивает следующие функции:

1. Обнаружение, предупреждение и ликвидация кибератак, осуществляемые на информационные и финансовые ресурсы в РФ.

2. Организация и координация деятельности организаций кредитно-финансовой сферы в качестве центра компетенций по противодействию кибератакам: автоматизированный сбор информации обо всех инцидентах поднадзорных субъектов; проведение эффективного технического анализа и экспертной оценки, в том числе компьютерные исследования и разбор вредоносных программ; оперативное распространение информации об инцидентах и правилах реагирования на них.

3. Выполнение функции центра координации деятельности по блокировке несанкционированных переводов денежных средств в платежной системе Банка России и иных платежных системах.

4. Прекращение функционирования фишинговых ресурсов и ресурсов, распространяющих вредоносное программное обеспечение, телефонных номеров и СМС-рассылок, используемых в мошеннических целях.

5. Взаимодействие с Центральными (Национальными) банками иностранных государств по вопросам мониторинга и реагирования на компьютерные атаки.

6. Взаимодействие с международными центрами реагирования на компьютерные атаки.

7. Повышение финансовой грамотности и пропаганды «компьютерной гигиены».

8. Взаимодействие с операторами по переводу цифровых финансовых активов (перевод на цифровую экономику).

Рис. 1. Функции ФинЦЕРТ ЦБР

Ключевыми показателями ФинЦЕРТ ЦБР являются:

1. «Уровень доверия клиентов и контрагентов финансовых организаций к безопасности реализуемых электронных платежных сервисов» [4]. Целевым ориентиром данного показателя в 2018г. был уровень равный 30%, а фактическое значение было на уровне 40%. В 2019г. целевой ориентир – 60%, а фактическое значение было получено в размере 70%. В 2020 г. уровень доверия клиентов и контрагентов вырос до 80%.

2. «Доля объема несанкционированных операций в общем объеме операций, совершенных с использованием платежных карт» [4]. Целевым ориентиром данного показателя является 0,005%. В 2019г. уровень несанкционированных операций был отмечен на уровне 0,0018%, что, к сожалению, больше запланированного. В 2020 г. также был отмечен рост данного показателя.

Как уже отмечалось выше, центр по реагированию на компьютерные чрезвычайные ситуации (ФинЦЕРТ ЦБР) – это группа экспертов по информационной безопасности, отвечающая за защиту от инцидентов кибербезопасности, обнаружение и реагирование на них. ЦЕРТ специализируется на разрешении инцидентов таких, как: утечка данных и атаки типа «отказ в обслуживании», а также на предоставлении предупреждений и рекомендаций по обработке инцидентов. ЦЕРТ также проводит постоянные кампании по информированию общественности и участвует в исследованиях, направленных на улучшение систем безопасности финансовой системы. Роль ФинЦЕРТ на чрезвычайные ситуации вполне сопоставима с подобными группами реагирования, которые существуют в мировой практике, например, универсальная модель реагирования на инциденты, которая используется в течение длительного времени, – это модель «защиты, обнаружения и реагирования».

В свете цифровой парадигмы ФинЦЕРТ является лидером в реализации национальной программы «Цифровая экономика Российской Федерации» по направлению «Информационная безопасность» и по противодействию компьютерным атакам.

Сигналы об угрозах в сфере безопасности «ФинЦЕРТ получает как от поднадзорных финансовых организаций, так и от компаний-интеграторов, разработчиков антивирусного программного обеспечения, иностранных финансовых организаций и регуляторов, групп реагирования на инциденты (в том числе иностранных), провайдеров и операторов связи, а также правоохранительных, иных государственных органов, курирующих информационную безопасность отрасли» [4].

Структура участников представлена на рис. 2 «Структура участников информационного обмена ФинЦЕРТ ЦБР» и рис. 3 «Структура участников информационного обмена ФинЦЕРТ ЦБР по видам деятельности».

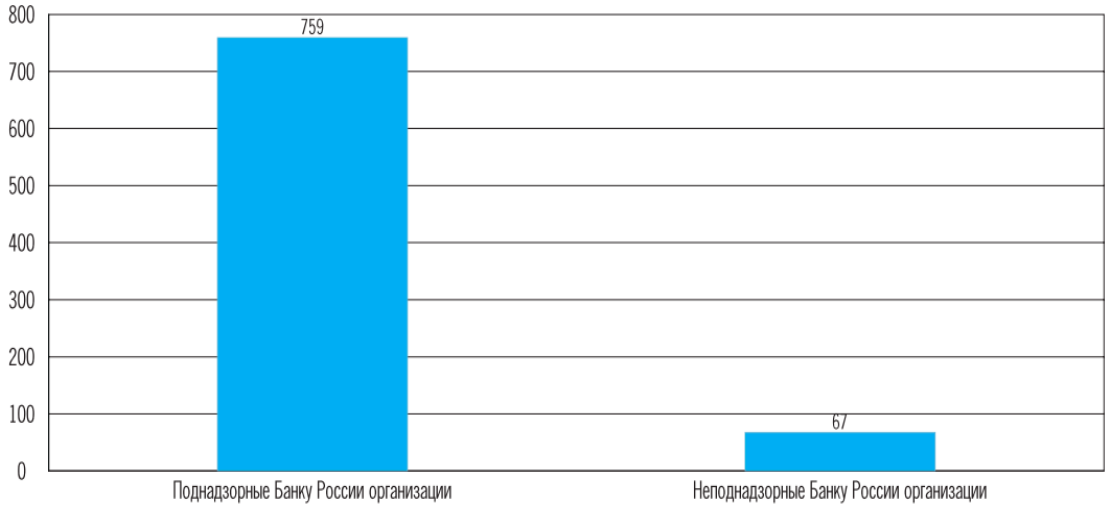

Рис. 2. Структура участников информационного обмена ФинЦЕРТ ЦБР

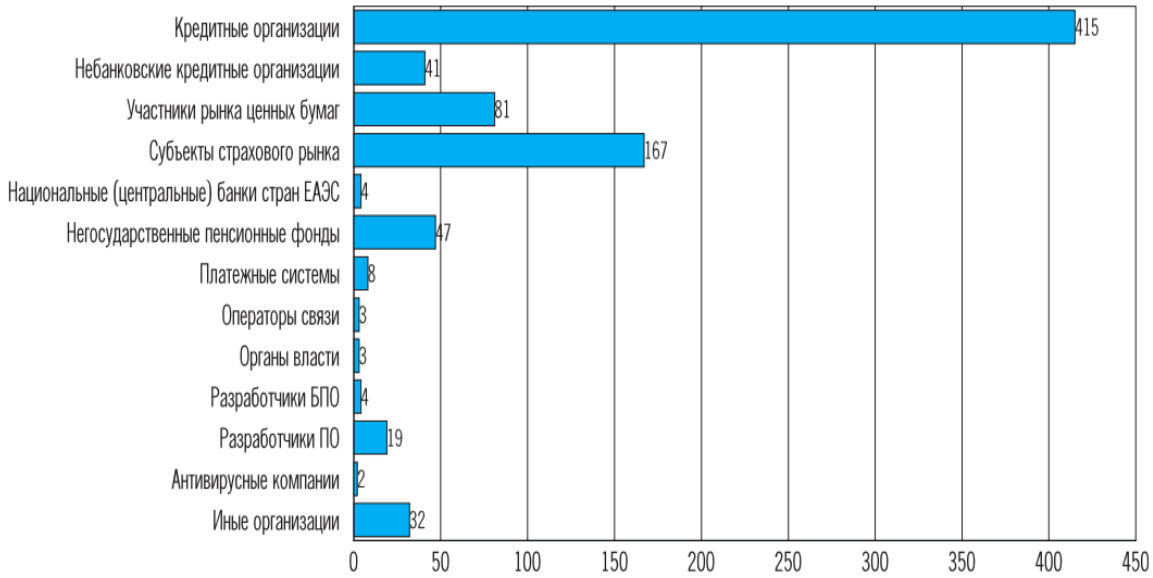

Рис. 3. Структура участников информационного обмена ФинЦЕРТ ЦБР по видам деятельности

Для упрощения процесса информационного обмена, а также повышения оперативности и уровня его защищенности используется АСОИ ФинЦЕРТ, к которой в настоящий момент подключены все банки Российской Федерации, также ведется подключение страховых организаций и других участников обмена (рис. 4 «Новые участники, которые не поднадзорны ЦБР»).

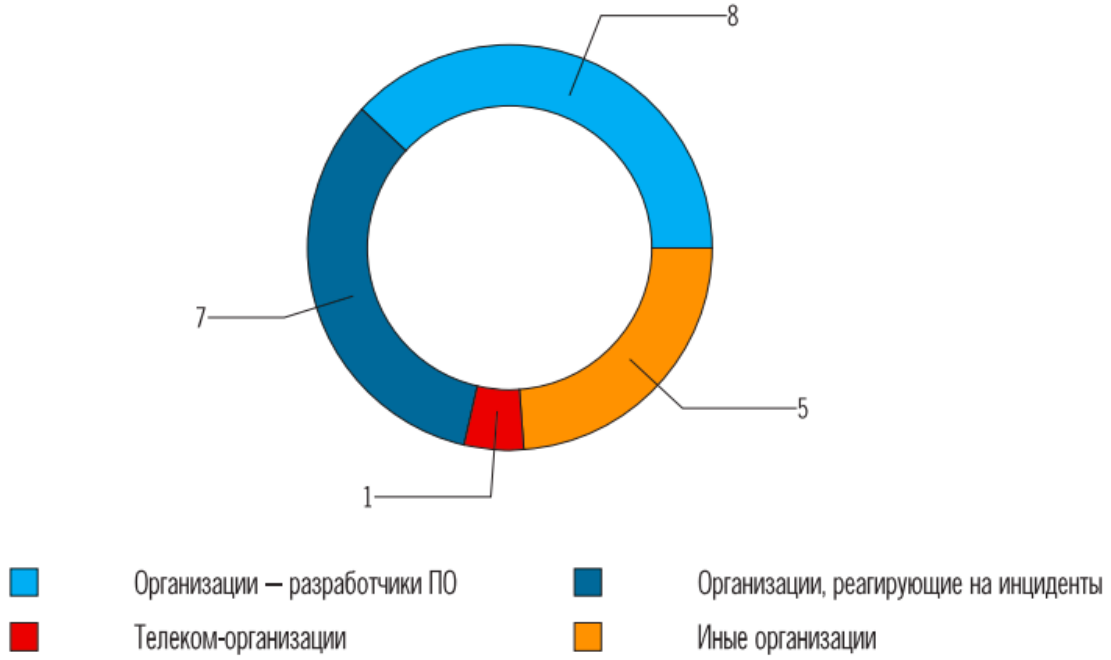

Рис. 4. Новые участники, которые не поднадзорны ЦБР

Рис. 5. Активные участники информационного обмена

Следует отметить, что среди участников информационного обмена, которые относятся к категории «Некредитные финансовые организации или НФО», стало больше (по сведениям ЦБР на 100 организаций), поскольку увеличился уровень доверия к ФинЦЕРТ со стороны надзорных органов. Также следует отметить об увеличении активных участников информационного обмена (на 48%), которые регулярно передают информацию о выявленных угрозах и возможных нарушениях информационной и экономической безопасности (рис. 5 «Активные участники информационного обмена»).

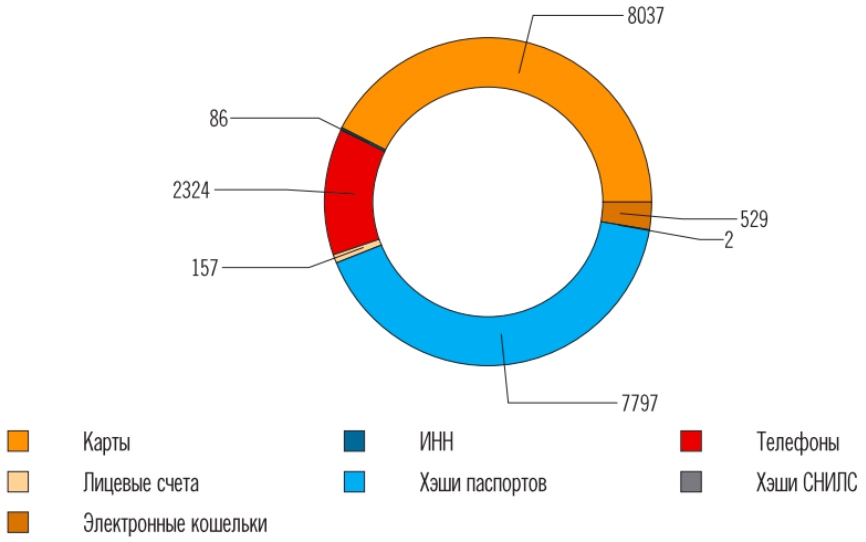

Рис. 6. Несанкционированные операции, переданные в ФинЦЕРТ ЦБР к началу 2020г.

Благодаря действиям ФинЦЕРТа выявляются несанкционированные операции, когда происходит использование функций хеширования номеров паспортов получателей денежных средств кредитной системы без согласия клиента, СНИЛСов, ИНН-предприятий (организаций), БИК-банков, номеров карточек получателей денежных средств, номеров телефонов и многое другое (рис. 6. «Несанкционированные операции, переданные в ФинЦЕРТ ЦБР к началу 2020г.»).

К сожалению, в условиях пандемии кибератаки и активность злоумышленников только увеличились. Так, например, по мнению аналитиков Group-IB, «фишинговые рассылки по итогам первой половины 2020 года приобрели популярность у кибермошенников. Исследования, проведенные аналитиками данной предметной области, показали, что мошенники в условиях эпидемии стали в несколько раз чаще пользоваться вирусными рассылками, которые позволяют получить доступ к различным серверам. Доля фейковых сайтов в Интернет-сети оставляет почти 50%. Рассылки злоумышленников содержат программы-шпионы, которые воруют важную информацию у клиентов [5].

Как мы и указывали выше, «одним из самых популярных способов завладения личными данными жертв через рассылку стали «загрузчики», которые после попадания на компьютер через письмо загружают другое вредоносное программное обеспечение, а также бэкдоры, позволяющие киберпреступникам удаленно подключатся к захваченному компьютеру» [8].

Вирусные программы, по мнению аналитиков, содержат банковский троян RTM, который перехватывает данные о реквизитах и делает снимки с экранов (это 30% вредоносных рассылок). Далее следует программа-шпион Loki PWS, которая крадет логины и пароли пользователей, и на третьем месте – бэкдор Formbook.

Для предотвращения угроз информационной и экономической безопасности ФинЦЕРТ должен принять необходимые меры предосторожности до того, как возникнут какие-либо проблемы с кибербезопасностью. В этой области основное внимание уделяется проактивным стратегиям, а не стратегиям реагирования. Такими стратегиями защиты могут быть [1,3,7]:

1. Составление плана реагирования на инциденты в организации (кредитной или коммерческой).
2. Анализ и оценка риска.
3. Создание резервов.
4. Внедрение инструментов сканирования уязвимостей и системы обнаружения вторжений (IDS).
5. Проведение обучение по вопросам безопасности для всех сотрудников.

6. Формирование планов безопасности, политики, процедур и учебных материалов по реагированию на инциденты (угрозы).

7. Формирование инструкций для пользователей о том, какие проблемы безопасности следует сообщать.

8. Создание инструкций по реагированию на инциденты для распространенных типов инцидентов (угроз).

9. Регулярное обновление внутренних и внешних защитных мер с учетом текущих угроз.

10. Повторный анализ и оценка эффективности процедур каждый раз, когда происходит инцидент (угроза).

На угрозу нельзя реагировать пока она не обнаружена. Фактически выявление угроз безопасности для многих организаций может занять недели или месяцы. Распространенной стратегией выявления и предотвращения является реализация защитной сетевой архитектуры с использованием таких технологий, как: маршрутизаторы, межсетевые экраны, системы обнаружения и предотвращения вторжений, сетевые мониторы и операционные центры безопасности (SOC).

Эффективное предотвращение угроз требует времени и усилий, а также понимания того, как на самом деле работает вся система организации. Для разработки стратегии выявления и предотвращения угроз безопасности необходимо решить ряд вопросов, например: какие приложения всегда используются в организации; как выглядит обычный сетевой трафик; какие сетевые протоколы используются; какие сетевые протоколы никогда не должны появляться в сети; каковы нормальные модели использования полосы пропускания, включая объем и направление; какие устройства предполагается подключить к сети; кто является владельцем системы и данных для этих подключенных хостов и устройств; как работает вся система организации и многие др. Чтобы определить, не работает ли сеть должным образом, размещает ли она нежелательные приложения или испытывает ненормальные шаблоны трафика, необходимо иметь возможность полностью охарактеризовать, как работает сеть и подключенные к ней системы. В противном случае, нет возможности определить правильность работы сети.

Системное управление требует, чтобы каждая часть сети была задокументирована и базировалась на локально-нормативных актах.

Также необходима программа управления активами банка, которая устанавливает владельца сети, структуру всей организации, приложения и бизнес-процессы, которые поддерживаются каждым активом организации. Кроме того, программа управления должна включать систему управления приложениями и безопасностью, владельцев приложений, авторизирован-

ных пользователей, характеристику передачи данных и другого трафика, за который отвечают приложения организации.

В случае, если инцидент угрозы безопасности случился, может начаться формальное реагирование на инцидент. Реагирование должно состоять из нескольких шагов. Первый шаг – это когда группа безопасности получает отчет об инциденте от участника, например, пользователя, делового партнера или сотрудника центра безопасности. Второй шаг – члены группы безопасности анализируют отчет об инциденте, чтобы понять, что происходит, и разрабатывают немедленную стратегию восстановления контроля и предотвращения дальнейшего ущерба. Третий шаг – это когда стратегия превращается в план, который реализуется для восстановления после инцидента, для возврата к нормальной работе организации.

В завершение еще раз отметим, что при использовании методов защиты и обнаружения угроз безопасности необходимо, чтобы все элементы взаимосвязанных процессов организации были смоделированы заранее прежде, чем можно будет предпринять какие-либо действия по реагированию. Многие организации не могут самостоятельно спланировать реагирование на угрозы или не могут реализовать стратегии защиты (обнаружения, выявления) и поэтому не знают, насколько безопасны их системы.

В следующих своих работах мы рассмотрим основные механизмы выявления и предотвращения угроз информационной и экономической безопасности.

Библиографический список

1. Глаголев С.Н. Система экономических показателей в стратегическом анализе для целей стратегического планирования и прогнозирования предпринимательской деятельности / С.Н. Глаголев, В.Л. Курбатов, С.М. Бухонова // Региональные проблемы преобразования экономики (РППЭ) РАН Дагестанский науч. центр ИСЭИ. 2019. № 11 (109). С. 291.

2. Киберпреступность и киберконфликты: Россия / TAdviser.ru – деловой портал [Электронный ресурс]. URL: https://www.tadviser.ru /index.php/Статья:Киберпреступность_и_киберконфликты_:_Россия

3. Ольхова Р.Г. Банковское дело: управление в современном банке: учебное пособие. М.: Изд-во КНОРУС, 2019. 282 с.

4. Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере департамента информационной безопасности БАНКА РОССИИ [Электронный ресурс]. URL: http://cbr.ru/Content/Document/File/84354/FINCERT_report_20191010.PDF

5. Риски скимминга банковских карт в РФ снижаются [Электронный ресурс]. URL: https://1prime.ru/Financial_market/ 20200118/830810650

6. Создание межведомственной группы для борьбы с хакерами/ TAdviser.ru - деловой портал [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Компания:Генеральная_прокуратура_РФ

7. Центральный банк Российской Федерации [Электронный ресурс]. URL: https://www.cbr.ru/information_security/fincert/

8. Эксперты назвали наиболее популярные у мошенников фишинговые рассылки [Электронный ресурс]. URL: https://iz.ru/1062305/2020-09-18/eksperty-nazvali-naibolee-populiarnye-u-moshennikov-fishingovye-rassylki

Рекомендовано кафедрой
финансового менеджмента
БГТУ

ст. преподаватель
М.В. Шевченко,
Р.Н. Шевченко
Белгородский государственный
технологический университет
им. В.Г. Шухова

ОСОБЕННОСТИ РАЗВИТИЯ ЦЕНТРАЛИЗОВАННОЙ ИНФОРМАЦИОННО-ТЕХНИЧЕСКОЙ ПЛАТФОРМЫ ДЛЯ УПРАВЛЕНИЯ ОБЩЕСТВЕННЫМИ ФИНАНСАМИ НА ПРИМЕРЕ БЕЛГОРОДСКОЙ ОБЛАСТИ

В настоящее время процессы информатизации охватывают практически все основные сферы экономики. В том числе, это касается и системы управления общественными финансами, автоматизация которой позволяет сформировать единое информационное пространство для всех участников бюджетного процесса, повысить качество управления общественными финансами, укрепить стабильность бюджетной системы, а также минимизировать риски, возможные при исполнении бюджета [5,6].

Сегодня управление финансово-бюджетной системой осуществляется на базе централизованной информационно-технологической платформы. Если рассматривать ее структуру более детально, то основой является интеграционное взаимодействие региональных систем планирования, исполнения бюджета и управления закупками, созданных на базе программных продуктов линейки АЦК Компании БФТ.