Макарова Наталья Владимировна
магистрант,
Московский финансово-юридический университет (МФЮА)

Макарова Людмила Михайловна
кандидат психологических наук,
Московский финансово-юридический университет (МФЮА)

Makarova N.
master's student,
Moscow financial and legal University (MFUA)

Makarova L.
PhD in Psychology,
Moscow financial and legal University (MFUA)

ФИНАНСОВЫЙ МОНИТОРИНГ: ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ХОЗЯЙСТВУЮЩЕГО СУБЪЕКТА

FINANCIAL MONITORING: LEGAL SUPPORT OF INFORMATION SECURITY OF THE BUSINESS ENTITY

УДК 336.7

Аннотация: *В статье представлено, что в РФ идут постоянные работы по совершенствованию нормативного регулирования в соответствии с мировыми тенденциями обеспечения информационной безопасности хозяйствующего субъекта*

Abstract: *The article presents that the Russian Federation is constantly working on improving regulatory regulation in accordance with global trends in ensuring information security of an economic entity.*

Ключевые слова: *финансовый мониторинг, законодательство, регулирование, информационное обеспечение*

Key words: *financial monitoring, legislation, regulation, information support*

При обеспечении информационной безопасности успех может быть эффективным только при применении комплексного подхода к защите интересов субъектов информационных отношений необходимо сочетать меры следующих уровней[1]:

- законодательного;
- административного (приказы, распоряжения, политики и другие организационные действия руководства организаций, связанных с защищаемыми информационными ресурсами);
- процедурного (меры безопасности, ориентированные на персонал);
- программно-технического;
- физического (комплексная защита помещений, оборудования и персонала).

Законодательный уровень является важнейшим для обеспечения информационной безопасности и включает на этом уровне две группы мер:

меры, направленные на создание и поддержание в обществе негативного (в том числе с применением наказаний) отношения к нарушениям и нарушителям информационной безопасности ("мерами ограничительной направленности");

направляющие и координирующие меры, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности (меры созидательной направленности).

На практике обе группы мер важны в равной степени, но необходимо подчеркнуть аспект осознанного соблюдения норм и правил ИБ. Это важно для всех субъектов информационных отношений, поскольку рассчитывать только на защиту силами системных администраторов и сотрудников службы безопасности предприятия было бы неправильно. Необходимо это и тем, в чьи обязанности входит наказывать нарушителей, поскольку обеспечить доказательность при расследовании и судебном разбирательстве компьютерных преступлений без специальной подготовки невозможно[2].

Краткий обзор зарубежного законодательства в области информационной безопасности

Одним из важнейших законов в этом направлении является американский "Закон

об информационной безопасности" (Computer Security Act of 1987, Public Law 100-235, January 8, 1988). Цель закона — реализация минимальных, но достаточных действий по обеспечению безопасности информации в федеральных компьютерных системах, без ограничений спектра возможных действий.

В начале Закона называется конкретный исполнитель —Национальный институт стандартов и технологий, НИСТ (National Institute of Standardization — NIST), отвечающий за выпуск стандартов и руководств, направленных на защиту от уничтожения и несанкционированного доступа к информации, а также от краж и подлогов, выполняемых с помощью компьютеров. Документы, выпускаемые институтом, являются руководствами "симметричного действия", служащие как для регламентации действий специалистов, так и для повышения информированности общества.

Согласно Закону, все операторы федеральных информационных систем и баз данных, содержащих конфиденциальную информацию, должны сформировать планы обеспечения ИБ. Обязательным является и периодическое обучение всего персонала таких ИС. Институт, в свою очередь, обязан проводить исследования природы и масштаба уязвимых мест, вырабатывать экономически оправданные меры защиты. Результаты исследований применяются как в государственных системах, так и в частном секторе.

Закон обязывает НИСТ координировать свою деятельность с другими министерствами и ведомствами, включая Министерство обороны, Министерство энергетики, Агентство национальной безопасности (АНБ) и т.д., чтобы избежать дублирования и несовместимости. Помимо регламентации дополнительных функций НИСТ, Закон предписывает создать при Министерстве торговли США комиссию по информационной безопасности, которая должна[3]:

− выявлять перспективные управленческие, техническо-технологические, программные и физические меры, способствующие повышению ИБ;

− выдавать рекомендации Национальному институту стандартов и технологий, доводить их до сведения всех заинтересованных ведомств.

С практической точки зрения важен раздел № 6 Закона, обязывающий все правительственные ведомства сформировать план обеспечения информационной безопасности, направленный на то, чтобы компенсировать риски и предотвратить возможный ущерб от утери, неправильного использования, несанкционированного доступа или модификации информации в федеральных системах. Копии планов направляются в НИСТ и в Агентство национальной безопасности (АНБ, National Safety Agency — NSA).

В 1997 году появился законопроект "О совершенствовании информационной безопасности" (Computer Security Enhancement Act of 1997, H.R. 1903), направленный на усиление роли НИСТ и упрощение операций с криптографическими средствами[4].

В законопроекте констатируется, что частные компании-разработчики готовы предоставить криптографические средства для обеспечения конфиденциальности, целостности и аутентичности данных и что разработка и использование шифровальных технологий должны происходить на основании требований рынка, а не распоряжений правительства. Кроме того, здесь отмечается, что за пределами США имеются сопоставимые и общедоступные криптографические технологии, и это следует учитывать при выработке экспортных ограничений, чтобы не снижать конкурентоспособность американских производителей аппаратного и программного обеспечения.

Очень важен раздел 3, в котором закрепляется обязанность НИСТ готовить стандарты, руководства, средства и методы для инфраструктуры открытых ключей (ниже аналогичный закон РФ об ЭЦП) по запросам частного сектора. Эти нормативные документы позволяют сформировать негосударственную инфраструктуру, пригодную для взаимодействия с федеральными ИС. В разделе № 4 особое внимание обращается на необходимость анализа средств и методов оценки уязвимых мест других продуктов частного сектора в области ИБ. Законом поощряется разработка требований и правил

безопасности, нейтральных по отношению к конкретным техническим решениям, использование в федеральных ИС коммерческих продуктов, участие в реализации шифровальных технологий, позволяющее в конечном итоге сформировать инфраструктуру, которую можно рассматривать как резервную для федеральных ИС.

За четыре года (1997-2001 годы) на законодательном и других уровнях информационной безопасности США было сделано следующие важные разработки:

− смягчены экспортные ограничения на криптографические средства (январь 2000 г.);

− сформирована инфраструктура с открытыми ключами;

− разработано большое число стандартов (например, новый стандарт электронной цифровой подписи — FIPS 186-2, январь 2000 г.).

Программа безопасности, предусматривающая экономически оправданные защитные меры, синхронизированные с жизненным циклом информационных технологий и систем, неоднократно входит в законодательные акты США. Например, согласно пункту 3534 ("Обязанности федеральных ведомств") подглавы II ("Информационная безопасность") главы 35 ("Координация федеральной информационной политики") рубрики 44 ("Общественные издания и документы"), такая "Программа" должна включать[5]:

− периодическую оценку рисков с рассмотрением внутренних и внешних угроз целостности, конфиденциальности и доступности систем, а также данных, ассоциированных с критически важными операциями и ресурсами;

− правила и процедуры, позволяющие, опираясь на проведенный анализ рисков, экономически оправданным образом уменьшить риски до приемлемого уровня;

− обучение персонала с целью информирования о существующих рисках и об обязанностях, выполнение которых необходимо для их (рисков) нейтрализации;

− периодический аудит и (пере)оценку эффективности правил и процедур;

− порядок и действия при внесении существенных изменений в систему;

− процедуры выявления нарушений информационной безопасности и реагирования на них; эти процедуры должны помочь уменьшить риски, избежать крупных потерь; организовать взаимодействие с правоохранительными органами.

В законодательстве Германии можно выделить "Закон о защите данных" (Federal Data Protection Act of December 20, 1990 (BGBl.I 1990 S.2954), amended by law of September 14, 1994 (BGBl. I S. 2325)), который целиком посвящен защите персональных данных.

Законом устанавливается приоритет интересов национальной безопасности над сохранением тайны частной жизни. В остальном, права личности защищены весьма тщательно. Например, если сотрудник фирмы обрабатывает персональные данные в интересах частных компаний, он дает подписку о неразглашении, которая действует и после перехода на другую работу. Государственные учреждения, хранящие и обрабатывающие персональные данные, несут ответственность за нарушение тайны частной жизни "субъекта данных", как говорится в Законе. В материальном выражении ответственность ограничена верхним пределом в 250 тысяч немецких марок.

Из законодательства Великобритании можно выделить семейство так называемых "добровольных стандартов" BS 7799, помогающих организациям на практике сформировать программы безопасности. Ниже положения этого системообразующего стандарта будут рассмотрены подробнее.

Российское законодательство в области информационной безопасности

Основным законом Российской Федерации является Конституция, принятая 12 декабря 1993 года. В соответствии со статьей 24 Конституции, органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Статья 23 Конституции гарантирует право на личную и семейную тайну, на тайну

переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, статья 29 — право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Современная интерпретация этих положений включает обеспечение конфиденциальности данных, в том числе в процессе их передачи по компьютерным сетям, а также доступ к средствам защиты информации.

Статья 41 гарантирует право на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, статья 42 — право на знание достоверной информации о состоянии окружающей среды[6].

Отметим, что право на информацию может реализовываться средствами бумажных технологий, но в современных условиях наиболее практичным и удобным для граждан является создание соответствующими законодательными, исполнительными и судебными органами информационных серверов и поддержание доступности, актуальности и целостности, представленных на них сведений, то есть обеспечение их (серверов) информационной безопасности.

В сентябре 2000 года Президент Российской Федерации В.В.Путин утвердил "Доктрину информационной безопасности". Какую роль она сыграет в развитии отечественных информационных технологий и средств защиты информации?

"Доктрина информационной безопасности" закладывает основы информационной политики государства. С учетом существующих угроз для защиты национальных интересов России государство планирует активно развивать отечественную индустрию средств информации, коммуникации и связи с последующим выходом продукции на мировой рынок, обеспечивать гарантии безопасности для национальных информационных и телекоммуникационных систем и защиту государственных секретов с помощью соответствующих технических средств. Одновременно предусматривается повышать эффективность информационного обеспечения деятельности государства.

Перечислим некоторые основополагающие законы и нормативные акты Российской Федерации в области информационной безопасности в их первой редакции:

1. Закон РФ "О государственной тайне" от 21.7.93 г. № 5485-1.
2. Закон РФ "О коммерческой тайне" (версия 28.12.94 г.).
3. Закон РФ "Об информации, информатизации и защите информации" от 25.1.95 г.
4. Закон РФ "О персональных данных" (версия 20.02.95 г.).
5. Закон РФ "О федеральных органах правительственной связи и информации" от 19.2.93 г. № 4524-1.
6. Положение о государственной системе защиты информации в Российской Федерации от ИТР и от утечки по техническим каналам. (Постановление Правительства РФ от 15.9.93 г. № 912-51).
7. Положение о Государственной технической комиссии при Президенте Российской Федерации (Гостехкомиссии России). Распоряжение Президента Российской Федерации от 28.12.92 г. № 829-рпс.

В настоящее время практически все эти законы и положения уточнены и дополнены соответствующими главами, параграфами и поправками, отражающими реалии текущей ситуации.

Порядок организации и осуществления Росфинмониторингом государственного контроля в сфере ПОД/ФТ регламентирован следующими нормативными правовыми актами:

- Кодексом Российской Федерации об административных правонарушениях;
- Федеральным законом № 115-ФЗ;
- Федеральным законом от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;
- Федеральным законом от 26 декабря 2008 г. № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля и муниципального контроля» (далее – Федеральный закон №

294-ФЗ);

− Федеральным законом от 23 июня 2016 г. № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации»;

− Указом Президента Российской Федерации от 13 июня 2012 г. № 808 «Вопросы Федеральной службы по финансовому мониторингу» (вместе с Положением о Федеральной службе по финансовому мониторингу);

− Указом Президента Российской Федерации от 12 августа 2002 г. № 885 «Об утверждении общих принципов служебного поведения государственных служащих»;

− постановлением Правительства Российской Федерации от 10 февраля 2017 г. № 166 «Об утверждении правил составления и направления предостережения о недопустимости нарушения обязательных требований, подачи юридическим лицом, индивидуальным предпринимателем возражений на такое предостережение и их рассмотрения, уведомления об исполнении такого предостережения»;

− постановлением Правительства Российской Федерации от 30 декабря 2016 г. № 1564 «О проведении субъектами профилактики правонарушений мониторинга в сфере профилактики правонарушений в Российской Федерации»;

− приказом Росфинмониторинга от 24 июня 2009 г. № 141 «О должностных лицах Федеральной службы по финансовому мониторингу, уполномоченных составлять протоколы об административных правонарушениях»;

В Гражданском кодексе Российской Федерации фигурируют такие понятия, как банковская, коммерческая и служебная тайна. Согласно статье 139, "информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности". Это подразумевает, как минимум, компетентность в вопросах ИБ и наличие доступных (и законных) средств обеспечения конфиденциальности.

В Уголовном кодексе Российской Федерации глава 28 "Преступления в сфере компьютерной информации" содержит три соответствующие статьи[7]:

− Статья 272. Неправомерный доступ к компьютерной информации

− Статья 273. Создание, использование и распространение вредоносных компьютерных программ

− Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

− Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации

В свете бурного развития локальных, региональных, национальных и всемирной сетей включение в сферу действия УК РФ вопросов доступности информационных сервисов является очень своевременным.

Статья 138 УК РФ, защищая конфиденциальность персональных данных, предусматривает наказание за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. Аналогичную роль для банковской и коммерческой тайны играет статья 183 УК РФ.

Основным нормативным правовым актом, устанавливающим обязательные требования к осуществлению деятельности юридических лиц и индивидуальных предпринимателей, в сфере противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (далее также – ПОД/ФТ), соблюдение которых подлежит проверке, является Федеральный закон от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем,

и финансированию терроризма» (далее – Федеральный закон № 115-ФЗ).

Федеральный закон № 115-ФЗ и иные нормативные правовые акты в сфере ПОД/ФТ разработаны в соответствии с требованиями международных стандартов в сфере ПОД/ФТ, в том числе рекомендаций Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ).

Российская Федерация как государство-член ФАТФ регулярно проходит взаимную оценку со стороны международных экспертов-оценщиков на предмет соответствия указанным стандартам.

По итогам взаимной оценки в 2019 году российской системе нормативно-правового обеспечения в сфере ПОД/ФТ присвоен высокий уровень технического соответствия, который характеризует имплементацию рекомендаций ФАТФ в национальное законодательство.

В соответствии со статьей 1 Федерального закона № 115-ФЗ его целью является защита прав и законных интересов граждан, общества и государства путем создания правового механизма ПОД/ФТ.

Федеральный закон № 115-ФЗ регулирует отношения граждан Российской Федерации, иностранных граждан и лиц без гражданства, организаций, осуществляющих операции с денежными средствами или иным имуществом, иностранных структур без образования юридического лица, а также государственных органов, осуществляющих контроль на территории Российской Федерации за проведением операций с денежными средствами или иным имуществом, в целях предупреждения, выявления и пресечения деяний, связанных с легализацией (отмыванием) доходов, полученных преступным путем, и финансированием терроризма.

Информация при обеспечении информационной безопасности в зависимости от порядка её предоставления или распространения подразделяется наИнформацию, свободно распространяемую[8].

1) Информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

2) Информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

3) Информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Законодательство определяет субъектов правовых отношений, участвующих в процессах производства, поиска, получения, передачи и распространения информации, применения информационных технологий и обеспечения защиты информации, к которым относятся:

обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

оператор информационной системы – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в её базах данных.

К числу важнейших обязанностей обладателя информации и оператора информационной системы в случаях, установленных законодательством Российской Федерации, относятся:

4) Предотвращение несанкционированного доступа к информации и (или) передачи её лицам, не имеющим права на доступ к информации.

5) Своевременное обнаружение фактов несанкционированного доступа к информации.

6) Предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации.

7) Недопущение воздействия на технические средства обработки информации, в

результате которого нарушается их функционирование.

8) Возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней.

9) Постоянный контроль за обеспечением уровня защищенности информации.

Росфинмониторинг выступает как обладатель информационных ресурсов (ИР) в отношении:

− федеральных структурных подразделений, входящих в состав Росфинмониторинга;

− государственных ИР, совместного ведения на основании договоров о разграничении полномочий;

− ИР, созданных на средства бюджета Росфинмониторинга;

− ИР, входящих в ИР федеральных органов государственной власти, органов субъектов Российской Федерации, муниципальных образований и формирующихся во взаимодействии с федеральными органами власти, органами власти субъектов РФ и муниципальных образований соответственно;

− ИР, предоставленных Росфинмониторингу федеральными органами государственной власти, органами власти субъектов Российской Федерации и муниципальных образований, а также другими организациями независимо от их организационно-правовой формы и форм собственности, гражданами, международными организациями и институтами по линии информационного взаимодействия.

К сведениям (информации), подлежащим защите, относятся:

− сведения, составляющие государственную тайну (относимые к таким сведениям в соответствии с требованиями законодательства Российской Федерации о государственной тайне);

− сведения конфиденциального характера, определенные Перечнем сведений Росфинмониторинга, составляющих служебную, банковскую, налоговую, коммерческую тайну, тайну связи, иную конфиденциальную информацию, а также персональные данные;

− сведения, составляющие в соответствии с действующим законодательством другие виды тайн (профессиональные тайны);

− сведения, определенные как конфиденциальные в соответствии с соглашениями о конфиденциальности собственниками информации (взаимодействующими министерствами, ведомствами и организациями, в том числе иностранными организациями) при их передаче в Росфинмониторинг.

Основным нормативным правовым актом, регулирующим деятельность Росфинмониторинга, в том числе осуществление контрольных мероприятий в отношении поднадзорных субъектов, а также устанавливающим обязательные требования в сфере ПОД/ФТ, соблюдение которых подлежит проверке, является Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее – Федеральный закон № 115-ФЗ).

Нормативными правовыми актами, устанавливающими обязательные требования к осуществлению деятельности юридических лиц и индивидуальных предпринимателей, соблюдение которых подлежит проверке в процессе осуществления Росфинмониторингом контроля в сфере ПОД/ФТ, помимо вышеназванных, являются:

− постановление Правительства Российской Федерации от 30 июня 2012 г. № 667 «Об утверждении требований к правилам внутреннего контроля, разрабатываемым организациями, осуществляющими операции с денежными средствами или иным имуществом, и индивидуальными предпринимателями, и о признании утратившими силу некоторых актов Правительства Российской Федерации»;

− постановление Правительства Российской Федерации от 19 марта 2014 г. № 209 «Об утверждении Положения о представлении информации в Федеральную службу по финансовому мониторингу организациями, осуществляющими операции с денежными

средствами или иным имуществом, и индивидуальными предпринимателями и направлении Федеральной службой по финансовому мониторингу запросов в организации, осуществляющие операции с денежными средствами или иным имуществом, и индивидуальным предпринимателям»;

− постановление Правительства Российской Федерации от 6 августа 2015 г. № 804 «Об утверждении Правил определения перечня организаций и физических лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности или терроризму, и доведения этого перечня до сведения организаций, осуществляющих операции с денежными средствами или иным имуществом, и индивидуальных предпринимателей»;

− приказ Росфинмониторинга от 3 июля 2010 г. № 203 «Об утверждении положения о требованиях к подготовке и обучению кадров организаций, осуществляющих операции с денежными средствами или иным имуществом, в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;

− приказ Росфинмониторинга от 17 февраля 2011 г. № 59 «Об утверждении Положения о требованиях к идентификации клиентов и выгодоприобретателей, в том числе с учетом степени (уровня) риска совершения клиентом операций в целях легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма»;

− приказ Росфинмониторинга от 8 мая 2009 г. № 103 «Об утверждении Рекомендаций по разработке критериев выявления и определению признаков необычных сделок»;

На официальном сайте Росфинмониторинга в информационно-телекоммуникационной сети «Интернет» на главной странице размещены тексты нормативных правовых актов и их отдельных положений, содержащие обязательные требования, соблюдение которых оценивается при проведении мероприятий по контролю.

Кроме того, тексты нормативных правовых актов размещены в личных кабинетах организаций на сайте Росфинмониторинга (далее – Личный кабинет) с комментариями в виде информационных писем.

В случае неисполнения организациями законодательства в сфере ПОД/ФТ к нарушителям применяются меры административной ответственности.

Нормами Кодекса Российской Федерации об административных правонарушениях (далее – КоАП РФ), в частности, статьей 15.27 КоАП РФ предусмотрены меры ответственности организаций, должностных лиц и индивидуальных предпринимателей за неисполнение требований законодательства о ПОД/ФТ.

Положения, содержащие признаки коррупциогенности, либо требования к гражданам и организациям, создающие условия для проявления коррупции, отсутствуют.

Таким образом, в РФ идут постоянные работы по совершенствованию нормативного регулирования в соответствии с мировыми тенденциями обеспечения информационной безопасности хозяйствующего субъекта

Банковская экосистема

Кроме традиционных финансовых услуг (денежных расчетов, кредитов и вкладов) банки внедряют нефинансовые сервисы: доставку еды, продажу театральных билетов, ремонт квартир, предоставление услуг телефонной связи с целью получения дополнительного дохода.

В современных условиях банковская сфера развивает новые направления, создавая экосистему, в определение термина которой каждый банк вкладывает собственное понимание в меру своих возможностей.

По мнению председателя правления Тинькофф Банка Оливера Хьюз "Экосистема — это современные технологии, общий бренд, использование данных, быстрое

масштабирование сервисов, снижение стоимости привлечения за счет экосистемного эффекта и масштаба. Это много сервисов, и не только в одной области".

Ориентирами для большинства банков в стремлении создавать экосистемы стали Сбербанк и Тинькофф Банк. Они активно приобретают доли в сервисных и IT–компаниях или заключают партнерские соглашения для внедрения на собственных платформах разнообразных небанковских сервисов[9]

Наличие у банка широкого набора нефинансовых услуг повышает лояльность к нему и значительно расширяет клиентскую базу.

Так, Тинькофф Банк приобрел долю в компании "Кассир.ру". Сбербанк вошел в капитал компании "ДокДок" (телемедицина) и VisionLabs (специализируется на распознавании лиц), а в рамках партнерства с "Яндексом" запустил интернет–магазин с доставкой товаров "Беру".

В ближайшее время Сбербанк планирует зайти в новые ниши: от путешествий до управлениями данными. Так Сбербанк пытается соединить жизнь человека, свой бренд и компанию.

Экосистема Сбербанка — это разветвленная сеть организаций, которая создана на единой цифровой платформе. В экосистему входит свыше 40 компаний.

В 2018 году Сбербанк объявил о создании отдела SberX для развития экосистемы нефинансовых сервисов[10].

Сбербанк вложил в небанковские сервисы 3% от чистой прибыли за три года.

Небанковские сервисы Сбербанка в основном построены на базе совместных предприятий с крупными игроками отрасли, такими как с Mail.Ru Group, с которой банк в конце июля 2019 года создал совместные предприятия в области еды и транспорта.

Также с 2019 года кредитная организация развивает совместный бизнес с «Яндексом» и стала владельцем 46,5% акций интернет-холдинга Rambler Group.

В конце июля 2019 года в экосистему Сбербанка входят 20 компаний, среди которых — агрегатор «Яндекс.Маркет», медицинский сервис DocDoc и корпоративный мессенджер Dialog.

В 2019 году выручка входящих в экосистему компаний составила около 70 млрд рублей. По словам Германа Грефа, из неё доля, причитающаяся Сбербанку, - более 35 млрд рублей.

По итогам 2020 года Сбербанк прибыль равна 70 млрд. рублей при выручке компаний экосистемы в 130 млрд. рублей.

В соответствии с прогнозами Сбера потенциальная аудитория экосистемы в России составит 100,8 миллионов активных клиентов.

По итогам 2020 года количество активных розничных клиентов Сбера увеличилось на 3 миллиона и на 200 тысяч - корпоративных клиентов.

«Сбер» к 2023 году планирует получить нефинансовой выручки в размере 570 млрд. рублей, что принесет около 130 млрд. рублей валовой прибыли.

Бизнес-экосистемы предлагают три важнейших преимущества: доступ к широкому спектру возможностей, быстрое масштабирование, гибкость и устойчивость.

По данным исследовательского агентства McKinsey в течении нескольких лет более трети экономической деятельности в мире будут покрывать возможности цифровых платформ, основанных на принципе экосистемы.

Библиографический список

1. Макарова, Л. М. Особенности информационной безопасности в банковской сфере / Л. М. Макарова, Ш. Н. Гатиятулин // Форум. Серия: Гуманитарные и экономические науки. – 2019. – № 2(17). – С. 201-205.
2. Макарова Л.М., Гатиятулин Ш.Н. Надзор и регулирование деятельности страховых компаний // Форум. Серия: Гуманитарные и экономические науки. 2019. № 2 (17). С. 205-208.
3. Макарова Л.М., Гатиятулин Ш.Н. Информационное обеспечение процедур контроля налогообложения: теоретический аспект // Форум. Серия: Гуманитарные и экономические науки. 2019. № 2 (17). С. 210-214.
4. Экономика: вчера, сегодня, завтра : Сборник трудов по материалам II конференции (с международным участием) преподавателей и студентов Московского финансово-юридического университета (МФЮА), Москва, 27 ноября 2020 года / Руководители секций конференции: В.А. Ключко, Т.В. Фурсова, Е.Е. Родина, Ш.Н. Гатиятулин, О.В. Чабанюк, И.В. Чеботарева. – Москва: Московский финансово-юридический университет МФЮА, 2020. – 541 с. – ISBN 978-5-94811-325-8.
5. Макарова, Л. М. SWOT-анализ инструмент управления экономической системой / Л. М. Макарова, Д. Гетьман // Поиск (Волгоград). – 2019. – № 1(10). – С. 229-234.
6. Revitalization of depressed industrial areas based on ecological industrial parks / E. E. Rodina, V. V. Filatov, V. S. Berezniakovskii [et al.] // Eurasian Journal of Analytical Chemistry. – 2018. – Vol. 13. – No 1. – P. em88. – DOI 10.29333/ejac/102253.
7. Макарова, Л. М. Развитие информационного общества как условие повышения эффективности функционирования экономики / Л. М. Макарова, Л. А. Челмакина // Экономика и предпринимательство. – 2017. – № 9-2(86). – С. 46-49.
8. Макарова, Л. М. Анализ функциональных возможностей решений 1С для малого бизнеса / Л. М. Макарова, И. Г. Ельмеева, И. В. Трифонова // Молодой ученый. – 2015. – № 4(84). – С. 373-376.

9. Макарова, Л. М. 1С для государственных учреждений / Л. М. Макарова, Е. С. Колмыкова // Молодой ученый. – 2015. – № 5(85). – С. 289-292.
10. Макарова, Л. М. Защита персональной информации в программных продуктах фирмы "1С" / Л. М. Макарова, А. Д. Королева // Вестник магистратуры. – 2014. – № 1(28). – С. 80-83.