УДК 004.056:336.71 **Экономические науки**

Ефремова Лидия Ивановна, *к.э.н., доцент кафедры статистики, эконометрики и информационных технологий в управлении, ФГБОУ ВПО «Мордовский государственный университет им. Н.П. Огарёва»*

Еремкина Юлия Васильевна, *студентка 2 курса направления подготовки «Экономика», ФГБОУ ВПО «Мордовский государственный университет им. Н.П. Огарёва», г. Саранск*

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ НА ПРИМЕРЕ ПАО «СБЕРБАНК РОССИИ»

Аннотация: в статье рассматривается проблема обеспечения информационной безопасности банковской деятельности на примере ПАО «Сбербанк России», описываются источники угроз информационной безопасности, элементы системы информационной безопасности банка, а также способы увеличения информационной безопасности банка.

Ключевые слова: банк, банковская деятельность, информационная безопасность, угрозы безопасности.

Annotation: the article deals with the problem of information security of banking activity on the example of PJSC "Sberbank of Russia". The article examines the sources of information security threats, the elements of the information security system of the bank, and ways to increase the information security of the bank.

Keywords: bank, banking, information security, security threat.

Банковская деятельность – это банковские функции и другие действия кредитной организации, которые непосредственно направлены на извлечение прибыли из банковских операций и сделок. [7] В связи с развитием научно-технического прогресса, банковская система становится неотъемлемой частью денежного хозяйства, поскольку она непосредственно связана с потребностями воспроизводства. Банки – это не просто хранилище денег, это крупномасштабное явление, обладающее финансовой мощью, значительным денежным капиталом.

Обслуживание огромного количества информации приводит к тому, что в банковском бизнесе возникают проблемы, которые могут быть решены лишь благодаря использованию автоматизированных информационных систем. Они позволяют собирать, надежно хранить и оперативно обрабатывать информацию.

Политика информационной безопасности банков значительно отличается от политик других экономических объектов. Это связано с особыми видами угроз и публичностью банков, вынужденных создавать удобный доступ к счетам с целью упрощения пользования для клиентов.

Всю деятельность коммерческих банков контролировал и продолжает контролировать Центральный банк Российской Федерации. В 1990-х годах не наблюдалось его активного вмешательства в дела информационной безопасности банков, однако в последнее время ситуация кардинально изменилась. Это связано, главным образом, с развитием всемирной информационной сети Интернет.

Вместе с тем, за последние двадцать лет существенно поменялось законодательство в сфере информационной безопасности. Появилось множество законов, регулирующих информационную безопасность банковских систем.

Среди недавно принятых законов, большую роль в развитии информационной безопасности банковских систем сыграл Федеральный закон от 27 июня 2011 года 161-ФЗ «О национальной платежной системе», вступивший в силу в марте 2015 года, который регламентирует деятельность по переводу денежных средств.

Безусловно, к банкам представляется большое количество требований и рекомендаций по обеспечению информационной безопасности. Например, постановления Центрального банка Российской Федерации, различные стандарты: стандарт СТО БР ИББС-1.0-2006, СТО БР ИББС-1.0-2014, которые посвящены управлению информационной безопасностью банка, международные стандарты, требования Basel II; требования международных платежных систем и т.д.

В связи с усилением защиты банковской информации разработан настоящий стандарт по обеспечению информационной безопасности организаций банковской системы Российской Федерации. Разработанный стандарт является основным для развивающей и обеспечивающей его группы документов в области стандартизации по обеспечению информационной безопасности организаций банковской системы России.

Основными целями введения Стандарта «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0 являются:

- повышение доверия к банковской системе Российской Федерации;
- повышение стабильности функционирования организаций банковской системы Российской Федерации и на этой основе – стабильности функционирования банковской системы Российской Федерации в целом;
- достижение адекватности мер по защите от реальных угроз информационной безопасности;
- предотвращение и (или) снижение ущерба от инцидентов информационной безопасности. [3]

Среди основных задач Стандарта выделяют следующие:

- установление единых требований по обеспечению информационной безопасности организаций банковской системы Российской Федерации;
- повышение эффективности мероприятий по обеспечению и поддержанию информационной безопасности организаций банковской системы Российской Федерации. [3]

В настоящее время безопасность российских банков обеспечивается на основе отечественных нормативных требований отраслевых стандартов Центрального банка Российской Федерации СТО БР ИББС -1.0-2014. Данный стандарт принят и введен действие Распоряжением Банка России от 17 мая 2014 года. Согласно данному стандарту выделяются основные требования к гарантированию безопасности, предоставляются определенные списки мер информационной безопасности в связи с назначением и разделением ролей и установлением доверия к сотрудникам банка, при регулировании доступа и регистрации клиентов, при применении источников сети Интернет и средств криптографической безопасности информации, а также при обработке персональных данных и т.д. [6]

Основными источниками угроз информационной безопасности являются:

- неблагоприятные события природного, техногенного и социального характера;
- террористы и криминальные элементы;
- зависимость от поставщиков, провайдеров, партнеров, клиентов;

– сбои, отказы, разрушения или повреждения программных и технических средств;

– работники организации банковской системы России, которые реализуют угрозы информационной безопасности с применением легально предоставленных им прав и полномочий;

– работники организации Банковской системы России, которые реализуют угрозы информационной безопасности вне легально предоставленных им прав и полномочий, а также субъекты, не являющиеся работниками организации банковской системы Российской Федерации, но осуществляющие попытки несанкционированного доступа;

– несоответствие требованиям надзорных и регулирующих органов, действующему законодательству. [6]

В настоящее время стало необходимым наличие в каждом банке «Политики информационной безопасности банка», главного документа при формировании системы его информационной безопасности. В данном документе выделяются серьезные угрозы безопасности информации в банке, представляется описание объектов защиты, устанавливаются ключевые задачи информационной безопасности, а также меры по обеспечению информационной безопасности банковской системы.

Главными элементами системы информационной безопасности банка являются:

– авторизация и аутентификация;

– защита от несанкционированного доступа к системам, в том числе и внутренняя защита от незаконного доступа сотрудников банка;

– защита каналов передачи данных, обеспечение целостности и актуальности данных при обмене информацией с клиентами;

– обеспечение юридической значимости электронных документов;

– управление инцидентами информационной безопасности;

– управление непрерывностью ведения бизнеса;

– внутренний и внешний аудит системы информационной безопасности.[5]

При формировании системы информационной безопасности банка следует учесть и такие функциональные требования к системе:

– получение от должностных лиц в зависимости от их иерархической подчиненности той информации, которая необходима им для решения поставленных задач;

– возможность использования должностными лицами всего арсенала средств математического и программного обеспечения в интересах принятия решений;

– обеспечение диалогового взаимодействия участников при работе с системой;

– соответствие процессов функционирования и применения системы методам и логике деятельности должностных лиц;

– соответствие особенностей хранения информации свойствам ее источников и потребителей, обеспечение требуемой срочности, периодичности и очередности ее представления;

– возможность объективного контроля и проверки промежуточных данных и результатов на основе протоколирования. [1]

Долгосрочное адекватное функционирование системы информационной безопасности способно обеспечить только систематическое поддержание баланса между всеми составляющими системы и элементами ее окружения. Такое соответствие является основной задачей поддержания информационной безопасности в банковской деятельности. [2]

Одним из крупнейших банков Европы и России является российский публичный акционерный банк «Сбербанк России». Он контролируется Центральным банком Российской Федерации и оказывает широкий спектр банковских услуг.

С целью обеспечения безопасности информации в ПАО «Сбербанк России» создана система защиты информации, представляющая собой совокупность направлений, требований, средств и мероприятий, сокращающих уязвимость информации и противодействующих незаконному доступу к информации и её утечке.

Для увеличения экономической безопасности ПАО «Сбербанк России» концентрируется на выборе персонала, периодически организовывает инструктажи по безопасности. В контрактах ПАО «Сбербанк России» отчетливо выделены персональные требования, функции к персоналу, а также ответственность за различные нарушения, так как в большинстве случаев именно он существенно влияет на информационную безопасность банка. Также, в деятельности Сбербанка широкое распространение получает введение в служебных документах грифа секретности и назначение увеличения суммы оклада для соответствующих категорий персонала. [9]

Самым крупным и развивающимся банком Приволжского федерального округа является Волго-Вятский банк Сбербанка России. В его составе находится примерно 2 300 филиалов, что гарантирует удобный доступ к услугам банка для всех клиентов. В состав Волго-Вятского банка входят банки Республики Мордовии, Чувашии, Татарстана, Марий-Эл, а также Нижегородской, Кировской и Владимирской областей.

Так как Сбербанк России отводит много времени на обеспечение информационной защиты, то для наиболее результативной организации ею и увеличения быстроты реагирования на, различного рода, угрозы нужен был инструмент, объединяющий информационную инфраструктуру банка. С данной целью был сформирован центр управления информационной безопасности SOC (Security Operation Center), который основывался на базе решения компании ArcSight ESM – лидера в сфере решений по контролю случаев нарушения безопасности и уровня исполнения норм отраслевого регулирования.

Обычно под определением Security Operation Center (SOC) понимают некоторую систему, которая построена на основе продукции класса SIEM (Security Information and Event Management), предназначенной, в свою очередь, для сбора и хранения лог-файлов устройств и приложений для их дальнейшего анализа и обнаружения инцидентов. [4]

В настоящее время SOC на основе SIEM-продуктов помогает компаниям решать некоторые важнейшие задачи:

– собирать и хранить лог-файлы в едином централизованном хранилище;

– предъявлять специализированные отчеты аудиторам для соответствия требованиям законодательства и отраслевым стандартам;

– определить некоторую "базовую линию" сетевой активности организации, превышение которой может свидетельствовать о различных атаках;

– выполнять корреляцию событий между различными источниками. [4]

Это предоставило возможность Волго-Вятскому банку осуществить ряд задач, в числе которых и мониторинг безопасности прикладных систем и сервисов, введение сбора необходимой информации. [10]

Кроме того, была создана система оповещения персонала банка об угрозах информационной безопасности. Благодаря этому в настоящее время специалисты быстро реагируют на различные угрозы. Данные системы информационной безопасности

необходимы для больших федерально-распределенных компаний, нуждающихся в надежности и бесперебойности работы информационных систем. [10]

Таким образом, за последние 20 лет произошли существенные изменения в сфере информационной безопасности банковских систем. Однако, с огромной ролью информационных технологий в жизни общества, появляется всё большая необходимость в безопасности, так как риски и угрозы воздействия на информационную безопасность постоянно растут. А особенности банковской системы Российской Федерации таковы, что отрицательные последствия сбоев в деятельности отдельных организаций приводят к моментальному развитию системного кризиса платежной системы Российской Федерации, и, кроме того, могут нанести ущерб интересам собственников и клиентов. При наступлении инцидентов информационной безопасности существенно увеличивается риск и вероятность нанесения ущерба организациям банковской системы Российской Федерации. Следовательно, для организаций банковской сферы Российской Федерации данные угрозы являются очень опасными.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Ефремова Л. И. Формирование информационно-аналитической системы в области энергосбережения // Информационное общество. –М., 2013. – № 3. – С. 49–57.

2 Ефремова Л. И. Формирование корпоративной информационной системы энергетической компании с использованием геоинформационной системы // Информационные системы и технологии. – 2014. – № 3 (83). С. 39-43.

3 Информационная безопасность организаций банковской системы Российской Федерации [Электронный ресурс] // Центральный банк Российской Федерации. – Режим доступа: http://www.cbr.ru/credit/gubzi_docs/ (дата обращения: 27.11.2015).

4 Новые технологии в Security operation center [Электронный ресурс]. – Режим доступа: http://www.bytemag.ru/articles/detail.php?ID=22469 (дата обращения: 10.12.2015).

5 Обеспечение информационной безопасности современного банка [Электронный ресурс]. – Режим доступа: http://www.topsbi.ru/?artID=943 (дата обращения: 28.11.2015).

6 Особенности обеспечения информационной безопасности в банковской системе [Электронный ресурс]. – Режим доступа: http://www.anti-malware.ru/analytics/Technology_Analysis/Features_information_security_in_the_banking_system (дата обращения: 29.11.2015).

7 Содержание банковской деятельности [Электронный ресурс] // Юридический портал. – Режим доступа: http://lawtoday.ru/razdel/biblo/ban-prav/DOC_017.php (дата обращения: 27.11.2015).

8 Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» [Электронный ресурс] // Центральный банк Российской Федерации. – Режим доступа: http://www.cbr.ru/credit/Gubzi_docs/st-10-14.pdf (дата обращения: 08.12.2015).

9 Ханнанова Е.Н. «Информационная безопасность Сбербанка России» [Электронный доступ]. – Режим доступа: http://www.scienceforum.ru/2015/1005/9978 (дата обращения: 5.12.2015).

10 Центр управления информационной безопасности в Волго-Вятском банке Сбербанка России [Электронный ресурс]. – Режим доступа: http://www.nvg.ru/projects/ib-center-sberbank/ (дата обращения: 10.12.2015).