Татаринцева А.А и Гамов Н.А
Студенты 2 курса магистратуры ЮЗГУ
Г.Курск, РФ
Научный руководитель: Таныгин М.О.
Канд.техн.наук, доцент ЮЗГУ,
Г.Курск, РФ

Политика информационной безопасности в российских банковских системах

До момента появления отечественных отраслевых стандартов информационной безопасности СТО БР ИББС банки управляли безопасностью, основываясь на положениях внутренних нормативных документов. Но и после принятия этих документов осталось много вопросов, требующих своего решения.

Ассоциация российских банков (АРБ) в феврале 2017 года обратилась в ЦБ РФ с просьбой разработать единую стратегию развития информационной безопасности кредитно-финансовых организаций, так как ответственность подразделений информационной безопасности банков регулируется примерно 130 документами, включающими около 50 Федеральных Законов, 20 Указов Президента и Постановлений правительства, 15 актов федеральных органов исполнительной власти, 25 нормативных актов Банка России, 20 стандартов и нормативных документов международных и российских платежных систем.

Назрела необходимость в упорядочении этих документов и в создании единого отраслевого документа по информационной безопасности, позволяющего кредитно-финансовым организациям оперативно реагировать на постоянно возникающие новые вызовы.

Банковские информационные системы и базы данных содержат конфиденциальную информацию о клиентах банка, состоянии их счетов и проведении различных финансовых операций.

Необходимость сохранять информационную безопасность этих данных очевидна, но без быстрого и своевременного обмена и обработки информации банковская система даст сбой. Поэтому необходима целая структура, которая

сможет обеспечить защиту банковской информации и конфиденциальность клиентской базы.

Последовательность мер по защите этих данных можно представить таким образом:

1) оценка и разработка конфиденциальной информации;

2) оборудование объекта для осуществления защиты;

3) контроль эффективности принятых мер.

Банк может полноценно осуществлять свою деятельность лишь в случае налаженного обмена внутренними данными и надежной системой защиты. Оборудование информационной защиты банковских объектов может иметь различные формы. [1]

Специалисты в области обеспечения информационной безопасности банка могут создавать как локальные системы, так и централизованные программы защиты.

Выбирая конкретную форму защиты, необходимо учитывать все возможные способы взлома и утечки данных. Грамотный и профессиональный подход к обеспечению безопасности подразумевает слаженную работу всех отделений банка и беспрерывное функционирование финансовых систем.

Разработка комплекса защитных мер по предотвращению нарушения конфиденциальности данных включает в себя ряд определенных действий.

– контроль обмена данных и строгая их регламентация;

– подготовка сотрудников банка и соблюдение ими требований безопасности;

– строгий учет каналов и серверов;

– анализ эффективности. [1]

Каждое направление включает в себя несколько этапов работы. К примеру, контроль обмена данных подразумевает не только обработку скорости передачи информации, но и своевременное уничтожение остаточных сведений. Эта мера также предполагает строгий контроль обработки данных и их криптографическую защиту.

Доступ к данным банка защищается с помощью системы идентификации, то есть паролями или электронными ключам. Работа с персоналом, использующим банковскую систему, включает в себя проведение инструктажей и контроль выполнения необходимых требований.

Строгий учет каналов и серверов, а также меры, обеспечивающие техническую защиту информации и безопасность банка подразумевают защиту резервных копий, обеспечение бесперебойного питания оборудования, содержащего ценную информацию, ограниченный доступ к сейфам и защиту от утечки информации акустическим способом.

Для анализа эффективности принятых мер необходимо вести учет или запись, которые будут отмечать работоспособность и действенность примененных средств защиты информации в банке.

Следует отметить, что в силу экономической важности банковских систем, обеспечение их информационной безопасности является обязательным условием. Поскольку информация, находящаяся в базе данных банков представляет собой реальную материальную стоимость, то требования к хранению и обработке этой информации всегда будут повышенными.

Специфика и особенности системы обеспечения безопасности, безусловно, индивидуальны для каждого отдельного банка, поэтому комплексное и профессиональное предоставление систем защиты является обязательным условием.

Несмотря на множество возможностей взлома и утечки информации, безопасность банковских данных и их конфиденциальность обеспечить вполне возможно.

Современные методы позволили усовершенствовать систему криптографии, а также реализовать такую меру, как электронная цифровая подпись (ЭЦП). Она служит аналогом собственноручной подписи и имеет непосредственную привязку к электронному ключу, который хранится у владельца подписи. Ключ состоит из двух частей: открытой и закрытой, и защищен специальным кодом.

Система безопасности в целом – это непрерывный процесс идентификации, анализа и контроля. Существует ряд основных принципов, согласно которым осуществляется обеспечение информационной безопасности банка:

- своевременное установление и обнаружение проблем;
- возможность прогнозирования развития;
- актуальность и эффективность предпринятых мер.

Также необходимо особо подчеркнуть важность тщательной и регулярной работы с персоналом, поскольку обеспечение безопасности информации во многом зависит от качественного и аккуратного выполнения требований, предъявляемых службой безопасности.

Человеческий фактор является основной и главной угрозой информационной безопасности, напрямую зависящей от человеческих отношений. Большая часть утечки информации объясняется халатностью персонала банка.

По статистике, около 80% правонарушений приходится на сотрудников банка, то есть на тех, кто непосредственно имел или имеет доступ к данным.

Однако, обеспечение внутренней информационной безопасности банка крайне необходимая мера не только для защиты конфиденциальности данных от профессиональной халатности и безалаберности, но и от намеренного взлома баз данных.

Кроме внутреннего фактора, существует также техническая угроза информационной безопасности, как банков, так и предприятий. К техническим угрозам относятся взломы информационных систем, лицами, не имеющими прямого доступа к системе, криминальными или конкурирующими организациями.

Съем и получение информации в данном случае производится с применением специальной аудио или видео аппаратуры. Одной из современных форм взлома является использование электрических и электромагнитных излучений, обеспечивающих злоумышленникам возможность получения

конфиденциальной информации, ЭЦП и представляющих техническую угрозу утечки.

Опасность и угрозу для программного обеспечения могут представлять также различные вредоносные для носителя информации компьютерные вирусы, программные закладки, которые способны разрушить введенные коды.

Самым известным способом решения вирусных проблем программного обеспечения являются лицензионные антивирусные программы, успешно справляющиеся с данной проблемой.

Защитить банковскую информацию от внутренних и внешних утечек поможет грамотный специалист в этой области и программное обеспечение, позволяющее отслеживать и блокировать передачу информации на съемные носители (например — флешки).

Банковская система сегодня — это основа всей рыночной экономики. Кругооборот ресурсов всей рыночной экономики невозможен без прямого участия банковских систем страны. Не только крупные суммы денег, но и небольшие срочные платежи проводятся преимущественно в электронном виде, а участие бумажных денег в процессе сводится к минимуму.

Банковская система является посредником в осуществлении большинства операций по оплате товаров\услуг, денежных переводов, а также непосредственно принимает участие в хранении и приумножении наличных денег физических и юридических лиц, кредитовании населения и предприятий и других операциях. В таких условиях вопрос защиты банковской информации становится особенно остро: ведь объем денежных средств, которыми оперирует банк, в наши дни очень высок. Угроза несанкционированно доступа со стороны мошенников заставляет банковские системы разрабатывать и применять новейшие разработки в области защиты информации, а также уже зарекомендовавшие себя простые и отработанные действия.

Количество европейских норм стандартизации по обеспечению и контролю информационной безопасности значительно превышает те правовые нормы, которые устанавливает РФ.

В национальных государственных стандартах преобладающими являются положения о защите информации от возможного взлома, утечки и угроз ее потери. Иностранные системы защиты специализируются на разработке стандартов доступа к данным и осуществления аутентификации.

Различия имеются так же и в положениях, относящихся к осуществлению контроля и аудита систем безопасности предприятий. Кроме того, практика применения и внедрения системы управления информационной безопасностью европейской стандартизации проявляется практически во всех сферах жизни, а стандарты РФ в основном направлены на сохранение материального благосостояния.

Тем не менее, постоянно обновляющиеся государственные стандарты содержат необходимый минимальный набор требований, позволяющий создать грамотную систему управления информационной безопасностью.

В заключении можно сказать, что для того, чтобы стандарты информационной безопасности сохраняли свою актуальность, они должны быть более гибкими и ориентироваться на базовые принципы защиты информации. Это проявляется в оперативном реагировании на постоянно модернизирующиеся угрозы в условиях совершенствования существующих и разработки новых информационных технологий.

Список использованной литературы

1. Обзор подходов к определению актуальных угроз телекоммуникационным системам и предложения по их совершенствованию (статья) Печатная Телекоммуникации – 2017. – №5 – С.27 – 34. 8. Калуцкий И.В., Фрундин А.Г., Ефремов М.А.,Таныгин М.О.

2. Информационная безопасность банков [Электронный ресурс] URL: https://tvoi.biz/biznes/informatsionnaya-bezopasnost/informatsionnaya-bezopasnost-bankov.html (Дата обращения 17.07.2017)

3. Виды защиты банковской информации [Электронный ресурс] URL: http://camafon.ru/informatsionnaya-bezopasnost/zashhita-banka (Дата обращения 18.07.2017)