Антюфьева Анастасия Валерьевна, студентка,
Финансовый университет при правительстве РФ, г. Москва

Каракич Антон Алексеевич, студент,
Финансовый университет при правительстве РФ, г. Москва

Резниченко Сергей Анатольевич,
кандидат технических наук, доцент, доцент департамента информационной безопасности Финансового университета при Правительстве РФ, Финансовый университет при правительстве РФ, г. Москва

ПРОБЛЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ИНФОРМАЦИОННЫХ СИСТЕМ ОРГАНИЗАЦИЙ КРЕДИТНО-БАНКОВСКОЙ СФЕРЫ

Аннотация. Главными проблемами, представляющими риск для конфиденциальности ИС организаций кредитно-банковской сферы, являются постоянно совершенствующиеся способы атак злоумышленников, халатность сотрудников, а также технические неисправности. Актуальные способы решения этих проблем: постоянное обучение и контроль сотрудников в области ИБ и установка антивирусного ПО на рабочие компьютеры.

Ключевые слова: информационная безопасность, безопасность в банковской сфере, информационная система.

Информационная безопасность.

Информационная безопасность включает в себя такие мероприятия как: предотвращение несанкционированного доступа к информации, ее использование или распространение.

У организации могут содержаться различные данные. Это может быть клиентская база или же личная информация организации. А для того чтобы все эти данные были защищены от посторонних лиц, информационная безопасность должна ограничить доступ к информации.

На сегодняшний день для защиты информации специалисты начали использовать защитное ПО, криптографическое шифрование и так далее.

Но не стоит останавливаться только на виртуальной защите. К сожалению, если помещение, в котором находится сервер с важной информацией, плохо охраняем, то похититель сможет украсть этот же сервер. Поэтому должны быть предусмотрены иные способы защиты.

Для того чтобы информационная безопасность была действительно действенная, то она должна включать в себя некоторые пункты.

Первый пункт – это конфиденциальность. Она должна регулировать доступ к информации. Доступ должен быть у тех, кто имеет на это право. Конфиденциальность включает в себя те же самые пароли, например, от личного кабинета.

Второй пункт – это доступность. Она должна отвечать за предоставление информации только тем людям, которым это разрешено. Например, при хакерской атаке личный кабинет может быть недоступен, тем самым доступность нарушается.

Третий пункт – это целостность. Она отвечает за сохранность информации. Например, если, при хакерской атаке, в личном кабинете удалена какая-нибудь информации, то целостность нарушается.

Одной из основных задач специалистов по информационной безопасности является защита конфиденциальной информации. Если же защита не является действенной, то в результате могут быть такие последствия как: кража денег, разглашение тайн компании и так далее.

Конфиденциальная информация делится на:

1) Коммерческая тайна. В ней может содержаться информация о клиентской базе или же какие-либо методы управления.

2) Персональные данные. В них содержится информация о человеке, его личные или паспортные данные.

3) Профессиональная тайна. В ней может содержаться, например, врачебная или адвокатская тайны.

4) Служебная тайна. Информация, которая входит в эту тайну является охраняемой гос. органами и ее нельзя получить без определенного доступа.

5) Государственная тайна. В ней могут содержаться информации о политике государства или какие-либо военные сведения. Доступ к этой информации также ограничен.

В чем заключается работа банковских систем?

Банковская система обеспечивает защиту и хранение данных. Поскольку из-за утечки информации могут распространиться данные о клиентах, на сегодняшний день вопрос обеспечения информационной безопасности банковских систем очень актуален.

В банковских системах могут содержаться базы данных клиентов с конфиденциальной информацией, счета клиентов и важные документы.

В банковской системе все должно быть хорошо организовано. Например, если нарушится обработка информации, то может произойти сбой банковской системы. Поэтому в этом деле должна быть выработана целая система, благодаря которой будет создано хорошее обеспечение информационной безопасности банковской системы.

Утечка конфиденциальной информации

Благодаря хорошо развитым системам, например, дорогостоящее ПО, утечки в банках происходят крайне редко, но не исключены.

В основном распространение данных происходит из-за человеческого фактора. Например, кто-то из персонала допустил ошибку и данные находились в свободном доступе.

Информацию можно поделить на менее ценную и очень ценную. Например, если произошла утечка информации, в которой был предоставлен номер телефона клиента или просто его ФИО, то информация считается менее ценной.

А если произошла утечка информации, в которой были сведения о банковском счете, то это уже считается очень ценной информацией.

Иногда мошеннику удается получить данные из различных баз данных, разных банков. В таком случае ему удастся заполучить намного больше ценной информации, так как везде она отличается.

Также банк имеет право передавать личные данные своих клиентов следующим организациям:

1) Центральный банк Российской Федерации в целях осуществления контроля;

2) Страховые компании, которые страхуют риски по кредитным договорам;

3) Федеральная служба по финансовому мониторингу, осуществляющая мониторинг отмывания денежных средств;

4) Судебные приставы или следственные органы в некоторых случаях.

Способы утечки конфиденциальной информации

Мошенники могут заполучить конфиденциальную информацию довольно просто. Например, рассылка. Злоумышленник отправляет вредоносную ссылку, при переходе по этой ссылке клиента просят ввести данные от его банковской карты. Если человек ввел данные, то они будут доступны мошеннику, который сможет ими воспользоваться.

Существует еще один способ как можно получить информацию. На сегодняшний день он является распространенным. Мошенник звонит человеку, представляется сотрудником банка и начинает говорить, что обнаружена подозрительная активность. И под этим предлогом злоумышленник запрашивает все нужные данные. В этой ситуации человек сам предоставляет все свои данные мошеннику.

Проблемы информационной безопасности в банковской сфере

Проблемы ИБ включают в себя:

1) Развитие методов атак. Развитие методов атак происходит постоянно. С каждым днем появляются новые способы мошенничества. Например, тот же звонок мошенника от лица сотрудника банка.

2) Распространение банковской тайны. Банковская тайна запрещает разглашать любую информацию о клиентах. Исключение может быть только в интересах правосудия.

3) Проблемы доступа к данным. Порой возникают технические проблемы в банковских системах, по причине которых могут возникнуть проблемы доступа к данным. Банковская система требует постоянного контроля.

Способы борьбы с проблемами безопасности банковских систем

На сегодняшний день благодаря социальным сетям, телевидению, то есть, информированию, люди уже осведомлены о существующих способах мошенничества. Нужно больше информировать людей, возможно проводить инструкции, в которых будет сказано, как нужно правильно реагировать или как отличить мошенников от реальных сотрудников банка.

Для домашних компьютеров можно установить антивирусное ПО. Оно сможет защитить ваш компьютер от незащищенного доступа.

Иногда банки узнают номера, с которых звонили мошенники с целью дальнейшего реагирования. Благодаря полученным номерам, банки предотвращают подобные атаки, так как из-за этого уменьшается уровень доверия со стороны клиентов.

Чтобы ограничить мошенникам доступ к личной информации нужно не переходить по подозрительным ссылкам и не писать свои личные данные в интернет.

Также можно увеличить контроль над сотрудниками банка, чтобы обнаружить сотрудников, которые могут передавать информацию третьим лицам.

Список литературы:

1. https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/informatsionnaya-bezopasnost-v-otraslyakh/bezopasnost-informatsionnykh-sistem/informatsionnaya-bezopasnost-v-finansovykh-sistem/

2. https://www.klerk.ru/buh/articles/563447/

3. https://elvis.ru/upload/iblock/ccd/porodin_ibbank.pdf