**Информационная безопасность в банках**

В нынешнем мире банковская информация, ее цена и значение намного возросли. Именно по этой причине к ней и возникает преступный интерес.

Неотъемлемая часть работы любого банковского учреждения – это обеспечение безопасности хранения данных, наличие регулярной смены и проверки паролей. Также контролируется вероятность утечки информации.

Чтобы совершить кражу и взлом банковской системы, злоумышленник совсем не обязательно должен ворваться в банковское учреждение. Осуществление взлома пользователем сети может производиться с помощью своего персонального компьютера. Таким образом, вопрос информационной банковской безопасности стал достаточно острым.

В банковских информационных системах и базах данных содержится конфиденциальная информация о банковских клиентах, о состоянии их счетов и о том, какие ими проводятся финансовые операции.

То, что информационная безопасность таких данных должна быть превыше всего – факт очевидный. При этом, если быстрый и своевременный обмен и обработка информации отсутствуют – произойдет сбой банковской системы. Поэтому необходимо наличие целой структуры, благодаря которой возможно обеспечение защиты банковской информации и конфиденциальности клиентской базы.

**Меры по защите данных такого типа должны осуществляться последовательно:**

1. Сперва оценивается и разрабатывается конфиденциальная информация;
2. Оборудуется объект для осуществления защиты.
3. Контролируется эффективность принятых мер.

Банком может полностью осуществляться его деятельность лишь тогда, когда есть налаженный обмен внутренними данными и присутствует надежная защитная система. Оборудование такой защиты банковских объектов обладает различными формами.

Специалистами в сфере обеспечения информационной банковской безопасности могут создаваться как разновидности локальных систем, так и централизованных защитных программ.

При выборе конкретной защитной формы стоит уточнить следующее: нужно продумать вопрос о всевозможных способах взлома и утечки данных. В случае грамотного и профессионального подхода к обеспечению безопасности работа всех банковских отделений будет слаженной – а, значит, финансовые системы будут функционировать беспрерывно.

**Комплекс защитных мер, направленный на предотвращение нарушения конфиденциальности данных** обладает следующими конкретными действиями:

1. Контролируется обмен данных, они строго регламентированы.
2. Банковские сотрудники проходят подготовку и соблюдают все требования безопасности
3. Каналы и сервера подвергаются строгому учету
4. Анализируется эффективность.

В каждом направлении есть различные рабочие этапы. Например, при контроле обмена данных, проводится не только обработка скорости передачи информации, - также своевременно уничтожаются остаточные сведения.

Чтобы открыть ООО – необходимо наличие учредителей. Учредитель – любое юридическое лицо, то есть какая-либо фирма, либо же физическое лицо, то есть гражданин.

Решившись на открытие своей фирмы, и составляя бизнес-план, большинство граждан не знают, что именно им необходимо проделать для получения государственной регистрации.

Доступ к банковским данным защищен с помощью идентификационной системы, то есть ее охраняют пароли или электронные ключи. Работа с сотрудниками, пользующимися банковскими данными, включает в себя различные инструктажи и слежку за выполнением нужных регламентов.

Принципы информационной безопасности банка

Несмотря на то, что возможностей взломать и забрать информацию всегда много, обеспечение безопасности банковских данных – процедура вполне реальная.

Благодаря наличию современных методов теперь усовершенствована система криптографии, а также реализована такая мера, как электронная цифровая подпись (ЭЦП). Она так называемый аналог и заменяет собственноручную подпись. Также она обладает непосредственной привязкой к электронному ключу, хранящемуся у владельца подписи. У этого ключа две части: открытая и закрытая, а также есть защита – наличие специального кода.

Система безопасности, в общем,  является непрерывным процессом идентификации, анализа и контроля.

**Существуют основные принципы, согласно которым обеспечивается информационная безопасность банка:**

1. Проблемы своевременно устанавливаются и обнаруживаются
2. Можно спрогнозировать развитие
3. Предпринятые меры должны быть актуальными и эффективными.

Также стоит отдельно выделить, насколько важна тщательная и регулярная работа с персоналом, так как обеспечение безопасности информации зависит и от того, насколько качественно и аккуратно выполняются требования службы безопасности.

## Угрозы информационной безопасности банка

Человеческий фактор – основная и главная угроза информационной безопасности, напрямую зависящий от человеческих отношений. Утечка информации чаще всего происходит во вине банковского персонала.

Как показывает статистика, примерно 80% правонарушений происходит из-за банковских сотрудников – из-за тех, кто обладает доступом к данным.

При этом обеспечение внутренней информационной безопасности банка, является крайне необходимой мерой как для того, чтобы защитить конфиденциальность данных от обычной халатности, так и для того, чтобы исключить намеренный взлом баз данных.

         Есть не только внутренний фактор – но и наличие технической угрозы информационной безопасности, как банковских организаций, так и компаний. Технические угрозы – это взломы информационных систем, лицами, не имеющими прямого доступа к системе. Это могут быть криминальные или конкурирующие организации.

Снимают и получают информацию в этом случае с помощью особенной аудио или видео аппаратуры. Современная популярная форма взлома – когда применяются электрические и электромагнитные излучения. Злоумышленники за это время получают конфиденциальную информацию, ЭЦП.

Опасность и угроза для программного обеспечения исходит и от различных вредоносных для носителя информации компьютерных вирусов, программных закладок, способных привести к  разрушению введенных кодов.

Самый известный способ решения подобных компьютерных проблем – установка лицензионных антивирусных программ, успешно справляющихся с данной проблемой.

В защите банковской информации от внутренних и внешних утечек может помочь поможет грамотный специалист в этой области и программное обеспечение, которое будет заниматься отслеживанием и блокировкой передачи информации на съемные носители (например — флешки).

Что необходимо, чтобы успешно автоматизировать склад: четко представлять складские процессы, наличие достаточных исходных данных о продукции, наличие интегрируемой информационной корпоративной системы и подготовленного персонала.

Если на складе не будут работать такие высококвалифицированные специалисты, как: заведующий складом, кладовщики, грузчики и уборщицы, то и эффекта ожидать будет довольно сложно.

## Важное защитное направление – своевременное распознавание и ограничение утечек различного вида.

Подводя итоги можно сказать, что поскольку банковские системы очень важны в экономическом смысле – их информационная безопасность обязательно будет обеспечена. Так как информация, находящаяся в базе данных банков – это реальная материальная стоимость, то требования к хранению и обработке этой информации всегда будут повышенными.

Специфика и особенности системы обеспечения безопасности, само собой, индивидуальны для любой банковской организации в отдельности, поэтому комплексное и профессиональное предоставление систем защиты – необходимое условие работы всей банковской системы.