Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Основы защиты информации

Студент: Валдайцев А. Д.

ФИТ 2 курс 5 группа

Преподаватель: Берников В. О.

Минск 2022

**Практическое занятие №3**

**Тема «Разработка политики информационной безопасности бизнес-компании»**

Цель: Разработать проект политики информационной безопасности бизнес-компании.

**Теоретическое введение**

Жизнь современного общества немыслима без современных информационных технологий. Компьютеры обслуживают банковские системы, контролируют работу атомных реакторов, распределяют энергию, следят за расписанием поездов, управляют самолетами, космическими кораблями. Компьютерные сети и телекоммуникации предопределяют надежность и мощность систем обороны и безопасности страны. Компьютеры обеспечивают хранение информации, ее обработку и предоставление потребителям, реализуя таким образом информационные технологии.

Однако именно высокая степень автоматизации порождает риск снижения безопасности (личной, информационной, государственной, и т.п.). Доступность и широкое распространение информационных технологий, ЭВМ делает их чрезвычайно уязвимыми по отношению к деструктивным воздействиям.

Информационная сфера имеет две составляющие: информационно-техническую (искусственно созданный человеком мир техники, технологий и т. п.) и информационно-психологическую (естественный мир живой природы, включающий и самого человека). Соответственно, в общем случае информационную безопасность общества (государства) можно представить двумя составными частями: информационно-технической безопасностью и информационно-психологической (психофизической) безопасностью.

Сущность информационно-технической безопасности можно определить, как достижение такого состояния развития общественных отношений, при котором обеспечена надежная и всесторонняя защита интересов субъектов этих отношений - человека, общества и государства - от угроз деструктивного информационного воздействия.

Информационно-психологическая безопасность состоит в том, что основным ее содержанием является защита интересов безопасности человека, безопасности общества и безопасности государства, как осознанная социальная потребность субъекта на безопасное удовлетворение своих потребностей.

## **Описание структуры службы банка**

Cтруктуру банка определяют внешние требования к нему и особенности его работы.

К внешним условиям относятся:

* указания владельцев банка;
* цели создания данной конкретной организации;
* ее место в финансово-экономической системе страны или региона.

Среди внутренних аспектов работы банка особенно важными оказываются:

* основные направления деятельности: кредитование, привлечение средств во вклады, расчетные и обменные операции, пр.;
* масштаб деятельности банка: один или несколько близких городов, представительства в регионах страны, международные структуры;
* важнейшие категории клиентов банка: частные лица, производственные или торговые предприятия, отдельные отрасли и др.

Единого подхода, шаблона для банковской структуры в рыночной экономике не встречается, но есть некоторые общие принципы и распространенные варианты.

Упрощенно внутреннюю систему коммерческого банка можно представить так:

* высшее руководство банка – собрание учредителей, другая подобная структура.

Непосредственным управлением операциями этот орган не занимается, но назначает исполнительные органы и контролирует их деятельность.

* правление банка во главе с председателем.

Это уже элемент текущего, оперативного управления. В его подчинении находятся руководители всех прочих подразделений.

Здесь обычно выделяют:

* управление розничного бизнеса. Сюда войдут отделы, обслуживающие частных лиц: кредитование, валютно-обменные операции, прием вкладов, операции с банковскими картами и пр.
* управление корпоративного бизнеса. Тут речь идет о работе с организациями. Это также кредитование, привлечение средств, производство платежей и прочих расчетов, привлечение средств организаций на депозиты.
* управление безопасности и контроля. Отделы с такими задачами могут входить в состав двух приведенных выше управлений или иметь единое руководство. Часто контроль, внутреннюю и внешнюю безопасность разделяют между несколькими отдельными управлениями.
* управление межбанковских коммуникаций. Такое подразделение можно считать необходимым на современном этапе консолидации банковской системы. Для работы с банками-партнерами, конкурентами и всеми прочими кредитными учреждениями создается особое управление, либо эти функции остаются в ведении руководства банка.
* бухгалтерия. Структура обязательная для любого хозяйствующего субъекта, и всегда имеющая единое руководство.
* управление операций на фондовом рынке. В распоряжении банков, на разных условиях, оказываются ценные бумаги многих предприятий и государств. Для обращения с этими активами банки могут формировать специальные службы.
* юридическое управление. Существует во всех банках, имеет в своем названии указание на специализацию и единое руководство.
* управление развития. Сюда относятся элементы системы, связанные с поиском новых рынков, клиентов, направлений и способов дохода. Отделы развития создаются при разных управлениях или объединяются в единую службу при тесном взаимодействии с другими подразделениями.
* пиар (PR) и реклама. Эти направления могут выделяться в отдельные банковские структуры, могут объединяться с управлением развития, или подчиняться подразделениям, ориентированным на определенных клиентов.
* управление информационных технологий. По мере компьютеризации систем обработки информации и развитием удаленного управления, подобные службы стали обязательной частью любой банковской структуры. Они взаимодействуют со всеми отделами, но обычно составляют единую систему.
* региональные подразделения. Такие элементы присущи крупным банкам. Система управления в них варьируется по нескольким критериям. Иногда региональные подразделения дублируют в своем составе все перечисленные выше управления и службы, иногда курируют только некоторые направления, к примеру – работу с физическими лицами.

## **Оценка рисков**

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы, стратегия защиты определена, тогда составляется программа, реализация которой должна обеспечить информационную безопасность. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы

Риск – возможность возникновения у банка финансовых потерь (убытков), незапланированных расходов или снижения планируемых доходов, возникающий в результате недостатков в организации системы безопасности банка, используемых технологиях, функционировании информационных систем, неадекватных действий или ошибок сотрудников, а также в результате внешних событий.

Риск характеризует опасность, которой может подвергаться система и использующая ее организация. Риск зависит от показателей ценности ресурсов, вероятности реализации угроз для ресурсов и степени легкости, с которой уязвимости могут быть использованы при существующих или планируемых средствах обеспечения информационной безопасности.

Цель оценивания рисков состоит в определении характеристик рисков для информационной системы и ее ресурсов. На основе таких данных могут быть выбраны необходимые средства управления информационной безопасности.

При оценивании рисков учитывается:

* ценность ресурсов;
* оценка значимости угроз;
* эффективность существующих и планируемых средств защиты.

Анализ рисков состоит в том, чтобы выявить существующие риски и предложить способ их оценки.

В самом широком смысле мера риска может рассматриваться в дальнейшем как описание видов неблагоприятных действий, воздействию которых может подвергнуться система или организация, и вероятностей того, что эти действия могут произойти. Результат этого процесса должен указать банку степень риска, связанного с определенными ценностями. Этот результат важен, потому что он является основой для дальнейшего выбора средств защиты и решений по минимизации риска.

Показатели ресурсов или потенциальное негативное воздействие на деятельность организации можно определять несколькими способами:

* количественными (например, стоимостные);
* качественными (могут быть построены на использовании таких понятий, как, умеренный или чрезвычайно опасный);
* их комбинацией.

Для того, чтобы конкретизировать определение вероятности в течение которого предполагается защитить ресурс. Вероятность того, что угроза реализуется, определяется следующими факторами:

* привлекательность ресурса как показатель при рассмотрении угрозы от умышленного воздействия со стороны человека;
* возможность использования ресурса для получения дохода как показатель при рассмотрении угрозы от умышленного воздействия со стороны человека;
* технические возможности угрозы, используемые при умышленном воздействии со стороны человека;
* вероятность того, что угроза реализуется;
* степень легкости, с которой уязвимость может быть использована.

К процедурному уровню относятся меры безопасности, реализуемые людьми.

Можно выделить следующие группы процедурных мер:

* управление персоналом;
* физическая защита;
* поддержание работоспособности;
* реагирование на нарушения режима безопасности;
* планирование восстановительных работ.

Основой программно-технического уровня являются следующие механизмы безопасности:

* идентификация и аутентификация пользователей;
* управление доступом;
* протоколирование и аудит;
* криптография;
* экранирование;
* обеспечение высокой доступности.

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.

Любое лицо, имеющее логический или физический доступ к информационным активам и компонентам соответствующих информационных технологий (программному обеспечению и данным, средствам вычислительной техники, коммуникационному оборудованию и каналам связи), может являться потенциальным злоумышленником. При этом предполагается возможность сговора сотрудника банка с внешним злоумышленником, но не сговор двух и более сотрудников банка.

Целью злоумышленника является получение контроля над информационным активом, приводящего к нарушению его доступности, целостности или конфиденциальности. Для достижения целей злоумышленник может использовать все экономически соизмеримые с потенциальным ущербом способы проведения атак на всех уровнях архитектуры информационных систем.

Источниками угроз информационным активам банка являются: внешние и внутренние злоумышленники, ошибочные действия персонала банка, вирусные атаки, отказы и сбои оборудования и программного обеспечения, техногенные и природные катастрофы, террористические угрозы.

В зависимости от сферы возникновения источников угроз в банке существенными являются следующие типы рисков.

1. Внутренние:

* риск бизнес-процессов (технологический риск) – риск неадекватности/неэффективности внутренних процессов и процедур, включая внедренческий риск, бухгалтерский риск, риск неэффективности системы контроля за совершением операций и т.п.;
* риск автоматизации процессов – риск, связанный с использованием информационных технологий, неудовлетворительным состоянием автоматизированных систем банка (риск ошибок и сбоев в программном обеспечении, электронных технологиях и системах коммуникации и т.п.);
* риск персонала – риск ошибок, превышения установленных полномочий, операционных лимитов и ограничений, некорректного исполнения операций (нарушения действующих регламентов и процедур), недобросовестного исполнения сотрудниками своих служебных обязанностей, злоупотреблений и противоправных действий (хищений, несанкционированного доступа, утечки информации и т.п.) со стороны сотрудников, риск недостаточной квалификации персонала.

2. Внешние:

* риск противоправных действий, включая преступные посягательства (риск мошенничества), риск противоправных действий извне (хищения (кражи, ограбления, разбойные нападения, акты вандализма, несанкционированное проникновение в электронные системы банка), риск отрицательной репутации контрагентов;
* риск утраты или повреждения имущества банка вследствие возникновения форсмажорных обстоятельств.

3. Комбинированный:

* правовой риск – риск прямых или косвенных потерь вследствие правовых ошибок при осуществлении банковской деятельности из-за ошибочной интерпретации или нарушения законодательства и иных нормативных правовых актов; несоответствия им внутренних нормативных документов банка; нечеткого формулирования взаимных прав и обязанностей сторон в договорных отношениях; неверно составленной документации, в том числе при решении спорных вопросов в судебных органах; несовершенства законодательства; нарушения нормативных правовых актов и условий заключенных договоров контрагентами.

В результате воздействия угроз на уязвимости могут возникнуть следующие последствия, влияющие на состояние информационной безопасности банка и его нормальное функционирование:

* + финансовые потери, связанные с утратой, утечкой или недоступностью информации;
  + финансовые потери, связанные с уничтожением и последующим восстановлением информации;
  + ущерб от дезорганизации деятельности банка и потери, связанные с невыполнением им своих обязательств;
  + ущерб репутации банка;
  + юридические и финансовые санкции со стороны регуляторов;
  + другие потери.

Анализ и оценка рисков нарушения информационной безопасности основывается на:

* идентификации информационных систем банка;
* идентификации информационных активов банка;
* ценности информационных активов для целей и задач банка;
* моделях угроз и нарушителей информационной безопасности банка.

Угрозы информационной безопасности реализуются их источниками (источниками угроз информационной безопасности), которые могут воздействовать на объекты среды информационных активов банка. В случае успешной реализации угрозы информационной безопасности информационные активы теряют часть или все свойства информационной безопасности.

Возможными вариантами обработки рисков являются:

* применение защитных мер, позволяющих снизить величину риска до допустимого уровня;
* уход от риска (например, путем отказа от деятельности, выполнение которой приводит к появлению риска);
* перенос риска на другие организации (например, путем страхования или передачи деятельности на аутсорсинг);
* осознанное принятие риска.

Имеется большое количество способов измерения и представления риска. Качественные подходы часто связаны с измерением риска в качественных терминах, заданных с помощью шкалы или ранжирования. Одномерные подходы рассматривают только ограниченные компоненты. Многомерные подходы рассматривают дополнительные компоненты в измерении риска, такие как надежность, безопасность, производительность. Одним из наиболее важных аспектов меры риска является то, что представление должно быть понятным и логичным для тех, кто должен выбирать средства защиты и решать вопросы минимизации риска. Формула, используемая при расчете рисков, представляет собой произведение трех параметров.

1. Стоимость ресурса (Asset Value, *AV)*. Указанная величина характеризует ценность ресурса. При качественной оценке рисков стоимость ресурса чаще всего ранжируется в диапазоне от 1 до 3, где 1 – минимальная стоимость ресурса, 2 – средняя стоимость ресурса и 3 –максимальная стоимость ресурса. К примеру, сервер автоматизированной банковской системы имеет *AV* = 3, тогда как отдельный информационный киоск, предназначенный для обслуживания клиента, имеет *AV* = 1 по отношению к информационной банковской системе.
2. Мера уязвимости ресурса к угрозе (Exposure Factor, *EF*). Этот параметр показывает, в какой степени тот или иной ресурс уязвим по отношению к рассматриваемой угрозе.

Например, с точки зрения банка ресурс автоматизированной банковской системы имеет наибольшую доступность. Таким образом, атаки с целью реализации отказа в обслуживании (Denial of Service, DoS) представляют для него максимальную угрозу. При качественной оценке рисков данная величина также ранжируется в диапазоне от 1 до 3, где 1 – минимальная мера уязвимости (слабое воздействие), 2 – средняя (ресурс подлежит восстановлению), 3 – максимальная (ресурс требует полной замены после реализации угрозы).

1. Оценка вероятности реализации угрозы (Annual Rate of Occurrence, *ARO*) демонстрирует, насколько вероятна реализация определенной угрозы за определенный период времени (как правило, в течение года), и также ранжируется по шкале от 1 до 3 (низкая, средняя, высокая).

На основании полученных данных выводится оценка ожидаемых потерь (уровень риска):

1. оценка ожидаемого возможного ущерба от единичной реализации определенной угрозы (Single Loss Exposure, *SLE*) рассчитывается по формуле: *SLE = AV ×EF*;
2. итоговые ожидаемые потери от конкретной угрозы за определенный период времени (Annual Loss Exposure, *ALE*) характеризуют величину риска и рассчитывается по формуле: *ALE = SLE × ARO.*

## **Разработка мер защиты**

Основными объектами защиты системы информационной безопасности в банке являются:

* информационные ресурсы, содержащие конфиденциальную информацию, коммерческую тайну, банковскую тайну, персональные данные физических лиц, сведения ограниченного распространения, а также открыто распространяемая информация, необходимая для работы Банка, независимо от формы и вида ее представления;
* сотрудники банка, являющиеся пользователями информационных систем банка;
* информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

Информационные активы банка – информация с реквизитами, позволяющими ее идентифицировать; имеющая ценность для банка; находящаяся в распоряжении банка и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме.

Основные типы защищаемых информационных активов банка:

* + коммерческая тайна;
  + банковская тайна;
  + инсайдерская информация;
  + персональные данные.

Информационные активы банка рассматриваются относительно информационных систем, в которых происходит обработка данных активов, в совокупности с соответствующими им объектами среды. При этом обеспечение свойств ИБ для информационных активов выражается в создании необходимой защиты соответствующих им объектов среды, в разрезе каждой информационной системы.

В целях защиты информационных активов производится регулярное повышение осведомленности работников в области обеспечения защиты информации. Порядок повышения осведомленности работников описан во внутренних документах банка.

Для создания эффективной политики безопасности предполагается первоначально провести анализ рисков в области информационной безопасности. Затем определить оптимальный уровень риска для предприятия на основе заданного критерия. Политику безопасности и соответствующую корпоративную систему защиты информации предстоит построить таким образом, чтобы достичь заданного уровня риска.

В ходе работ должны быть установлены границы исследования. Для этого необходимо выделить ресурсы информационной системы, для которых в дальнейшем будут получены оценки рисков. При этом предстоит разделить рассматриваемые ресурсы и внешние элементы, с которыми осуществляется взаимодействие. Ресурсами могут быть средства вычислительной техники, программное обеспечение, данные, а также информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (архивах, фондах, банках данных, других информационных системах). Примерами внешних элементов являются сети связи, внешние сервисы и т.п.

При построении модели будут учитываться взаимосвязи между ресурсами. Например, выход из строя какого-либо оборудования может привести к потере данных или выходу из строя другого критически важного элемента системы. Подобные взаимосвязи определяют основу построения модели организации с точки зрения информационной безопасности.

Эта модель, в соответствии с предлагаемой методикой, строится следующим образом: для выделенных ресурсов определяется их ценность, как с точки зрения ассоциированных с ними возможных финансовых потерь, так и с точки зрения ущерба репутации организации, дезорганизации ее деятельности, нематериального ущерба от разглашения конфиденциальной информации и т.д. Затем описываются взаимосвязи ресурсов, определяются угрозы безопасности и оцениваются вероятности их реализации.

На основе построенной модели можно обоснованно выбрать систему контрмер, снижающих риски до допустимых уровней и обладающих наибольшей ценовой эффективностью. Частью системы контрмер будут рекомендации по проведению регулярных проверок эффективности системы защиты.

Обеспечение повышенных требований к информационной безопасности предполагает соответствующие мероприятия на всех этапах жизненного цикла информационных технологий. Планирование этих мероприятий производится по завершении этапа анализа рисков и выбора контрмер. Обязательной составной частью этих планов является периодическая проверка соответствия существующего режима информационной безопасности политике безопасности, сертификация информационной системы (технологии) на соответствие требованиям определенного стандарта безопасности.

По завершении работ, можно будет определить меру гарантии безопасности информационной среды, основанную на оценке, с которой можно доверять информационной среде объекта. Данный подход предполагает, что большая гарантия следует из применения больших усилий при проведении оценки безопасности.

Таблица 3.1 – Специфические угрозы и предлагаемые контрмеры

|  |  |
| --- | --- |
| Специфические угрозы | Предлагаемые контрмеры |
| Возможность отключения электричества, что приведет к сбою незавершенных операций и потере данных. | Оснащенность каждого отдела, во-первых, фильтрами бесперебойного питания, а также собственным генератором. |
| Угроза проникновения на рабочие места сотрудников людей, не являющихся работниками отделов, которые имеют туда доступ. | Ужесточить пропускной режим на склад, ввести проход в конкретный отдел по пропускам и индивидуальным паролям. |
| Угроза доступа в эксплуатационный отдел, могут быть нарушены эксплуатационные планы. | Допуск в отдел только инженеров, по предъявлению пропуска с индивидуальным номером. |
| Угроза изменения базы данных об объектах. | Резервная копия БД, хранящаяся не только в данном здании банковской компании. |
| Угроза доступа в ИТ-отделе. | Может быть решена, наличием качественных: дверей, окон. Также сигнализации и камер видеонаблюдения. |

Опираясь на риски, собранные в предыдущем пункте, можно описать следующие меры защиты информации банка:

* защита помещений и объектов от несанкционированного доступа;
* защита информации в бумажном документообороте банка;
* защита информации от утечки по техническим каналам, возможные угрозы при проведении мероприятий и эксплуатации технических средств, когда возможны утечки или нарушения целостности информации, нарушения работоспособности технических средств:
  + побочные электромагнитные излучения информативного сигнала от технических средств;
  + радиоизлучения или электрические сигналы от внедренных специальных электронных устройств перехвата информации;
  + акустическое излучение информативного речевого сигнала;
  + просмотр информации с экранов дисплеев и других средств ее отображения визуально и с помощью оптических средств;
  + воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации;
  + непреднамеренное попадание защищаемой информации к лицам, не допущенным к ней, но находящимся в пределах контролируемой зоны;
  + непреднамеренное прослушивание без использования технических средств разговоров, ведущихся в выделенном помещении, из-за недостаточной звукоизоляции его ограждающих конструкций, систем вентиляции и кондиционирования воздуха;
* обеспечение безопасности информации, передаваемой по каналам связи и в системе внутреннего электронного документооборота между подразделениями банка;
* обеспечение информационной безопасности в компьютерных сетях;
* обеспечение информационной безопасности в платежных системах;
* обеспечение информационной безопасности в платежных системах с использованием банковских пластиковых карточек:
  + меры технологического характера, имеющие целью повысить надежность процедуры передачи информации платежной системы и идентификации владельца карточки,
  + меры безопасности при проведении операций с пластиковыми картами непосредственно в подразделениях, осуществляющих их выпуск, выдачу и обслуживание,
  + меры безопасности при обслуживании терминального оборудования (банкоматы, инфокиоски, терминалы), включая меры по предупреждению и/или обнаружению противоправных действий с терминальным оборудованием, совершаемых третьими лицами в процессе его функционирования,
  + организация распределения и закрепления за персоналом реквизитов доступа (ключей, служебных карточек операторов и администраторов, паролей, прав доступа);
* обеспечение информационной безопасности при использовании ресурсов Internet:
  + использование сети Internet сотрудниками банка,
  + доступ к сервисам банка клиентов через Internet (Internet-banking)
* обеспечение безопасности информации в автоматизированных системах;
* архивы электронной информации;
* размещение компьютерного и телекоммуникационного оборудования;
* регистрация пользователей и использование паролей на уровне операционных систем, прикладного программного обеспечения и компьютерной сети;
* средства предотвращения несанкционированного доступа для операционных систем, прикладного программного обеспечения и компьютерной сети;
* защита от вирусов и других вредоносных программ;
* системы мониторинга безопасности операционных систем, прикладного программного обеспечения и компьютерной сети;
* системы сканирования безопасности операционных систем, прикладного программного обеспечения и компьютерной сети;
* порядок приемки-сдачи общесистемного и прикладного программного обеспечения;
* установка обновлений на общесистемное и прикладное программное обеспечение;
* резервное копирование данных.
* обеспечение непрерывной работы и восстановления программно-технических комплексов;
* рекомендации о службах информационной безопасности и их составу на всех уровнях (головной банк, филиал, отделение, РКЦ).
* план аварийного восстановления данных.
* анти-DDoS. Грамотная защита от DDoS-атак собственными силами невозможна. Многие разработчики программного обеспечения предлагают услугу анти-DDoS, которая способна защитить от подобных нападений. Как только в системе обнаруживается трафик необычного типа или качества, активируется система защиты, выявляющая и блокирующая вредный трафик. При этом бизнес-трафик поступает беспрепятственно. Система способна срабатывать неограниченное количество раз, до тех пор, пока угроза не будет полностью устранена.
* антивирусные программы – программа для обнаружения компьютерных вирусов и лечения инфицированных файлов, а также для профилактики – предотвращения заражения файлов или операционной системы вредоносным кодом.
* организацию охраны помещений, в которых содержатся носители конфиденциальной информации;
* установление пропускного режима в помещения, содержащие носители конфиденциальной информации;
* закрепление технических средств обработки конфиденциальной информации за сотрудниками, определение персональной ответственности за их сохранность;
* установление порядка пользования носителями конфиденциальной информации (учет, хранение, передача другим должностным лицам, уничтожение, отчетность);
* организацию ремонта технических средств обработки конфиденциальной информации;
* организацию контроля за установленным порядком.

Основными мерами по обеспечению информационной безопасности банка являются:

* административно-правовые и организационные меры;
* технические, основанные на использовании аппаратно-программных и специальных средств;
* режимные;
* комбинированные – на основе первых трёх типов.

Для обеспечения актуальности модели угроз должен осуществляться ее плановый (регулярный) и внеплановый пересмотр. Плановый пересмотр проводится с периодичностью не реже чем один раз в два года.

Внеплановый пересмотр должен осуществляться в случаях:

* по решению начальника отдела автоматизации и информационного сопровождения банка на основе периодически проводимых им анализа и оценки угроз безопасности с учетом особенностей и (или) изменений конкретной информационной системы;
* по результатам мероприятий по контролю за выполнением требований по обеспечению безопасности информационных активов при их обработке в информационных системах.

Внесение изменений в модель угроз (корректировка) осуществляется по решении руководства банка или отдела автоматизации и информационного сопровождения банка.

## **Вывод**

В ходе этой работы были проанализированы риски, связанные с информационной безопасностью банковской компании. Были предусмотрены явления, которые могут оказать влияние на целостность системы и вывести ее из строя. Разработанная политика безопасности не способна обеспечить полную защиту всей информации компании, но она необходима для обеспечения некоторых гарантий.

Политика безопасности определяет стратегию организации в области информационной безопасности, а также ту меру внимания и количество ресурсов, которую руководство считает целесообразным выделить.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы, стратегия защиты определена, тогда составляется программа, реализация которой должна обеспечить информационную безопасность. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т.п.