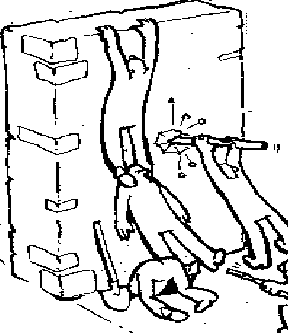
**ИНСТИТУТ СИСТЕМНОГО АНАЛИЗА И УПРАВЛЕНИЯ**

**ЗАДАНИЕ**

на деловую ситуацию

*Математические модели рисков информационной безопасности (на примере банка* «*X-trimBank*»)

****

**2017**

**Содержание**

[Введение 2](#_Toc447679711)

[1.Постановка задачи 2](#_Toc447679712)

[1.1.Описание ситуации 2](#_Toc447679713)

[1.2.Дополнительная информация 2](#_Toc447679714)

[1.3.Основные активы банка 2](#_Toc447679715)

[2.Методика выполнения задания 2](#_Toc447679716)

[2.1.Установление контекста (подготовительный этап) 2](#_Toc447679717)

[2.2.Инвентаризация и классификация информационных активов (этап 1) 2](#_Toc447679718)

[2.3.Моделирование угроз информационной безопасности (этап 2) 2](#_Toc447679719)

[2.5.Обработка рисков, обоснование мер и средств контроля и управления (этап 4) 2](#_Toc447679720)

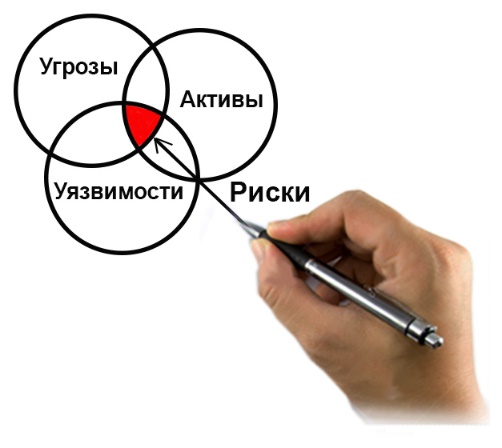
[2.6.Моделирование плана обработки рисков (этап 5) 2](#_Toc447679721)

[Защита результатов деловой игры 2](#_Toc447679722)

[2.6.Варианты заданий 2](#_Toc447679723)

[Литература 2](#_Toc447679724)

# Введение



Защита информационных активов организации сегодня является одним из важных составляющих успешности бизнеса. Главная цель защиты информации направлена на обеспечение эффективности и непрерывности бизнеса. Это достигается введением обоснованных механизмов защиты информации на основе сбалансированных требований по конфиденциальности, целостности, доступности и других показателей.

Сегодня деятельность специалистов в сфере информационной безопасности определяется Федеральными законами, государственными и отраслевыми стандартами, определяющими методологию построения системы защиты информации хозяйствующего субъекта (ХС). Сложность же практической реализации требований этих руководящих документов заключается в том, что не существует единого подхода к организации защиты информации в различных хозяйствующих субъектах даже одной отрасли. Это определяется различными методологическими концепциями построения системы управления информационной безопасностью ХС.

Первая концепция основана на ***создании систем с полной защищённостью информационных активов*** на основе анализа модели угроз, проведения исследований технических каналов утечки информации, проектирования системы защиты информации с использованием технических и криптографических средств защиты и завершается сертификацией системы информационной безопасности объекта информатизации. При организации защиты учитываются все возможные каналы утечки информации, а также используются сертифицированные программные средства, оборудование, вычислительные средства, средства связи и телекоммуникаций, средства криптографической защиты (допускаются только отечественного производства). Доверие к этим системам обеспечивается за счет аттестации рабочих мест после проведения специальных исследований. Дальнейшая эксплуатация предполагает мониторинг состояния системы безопасности и поддержания её в актуальном состоянии. Эта концепция хорошо вписывается в систему защиты конфиденциальной информации. Для защиты не конфиденциальной информации используются другие подходы, основанные на создании системы обеспечения ИБ, включающей правовое, организационное, инженерно-техническое, материальное, криптографическое, кадровое, финансовое и др. Такой подход является субъективным и может быть в условиях, когда информационная система уже существует и не предполагается каких-либо ее радикальных изменений.

Более перспективным подходом к построению системы информационной безопасности можно считать процессный подход (рис.1), изложенный в стандарте по менеджменту информационной безопасности [1] и основанный на цикле Деминга-Шухарта (PDCA):

1. *Plan - планирование*
2. *Do - воплощение, реализация*
3. *( Check ) - измерение, проверка*
4. *Act - улучшение.*

На стадии ***планирования*** устанавливают политики информационной безопасности, цели, задачи, процессы и процедуры, адекватные потребностям в менеджменте риска информационной безопасности для достижения результатов в соответствии с политиками и целями организации.

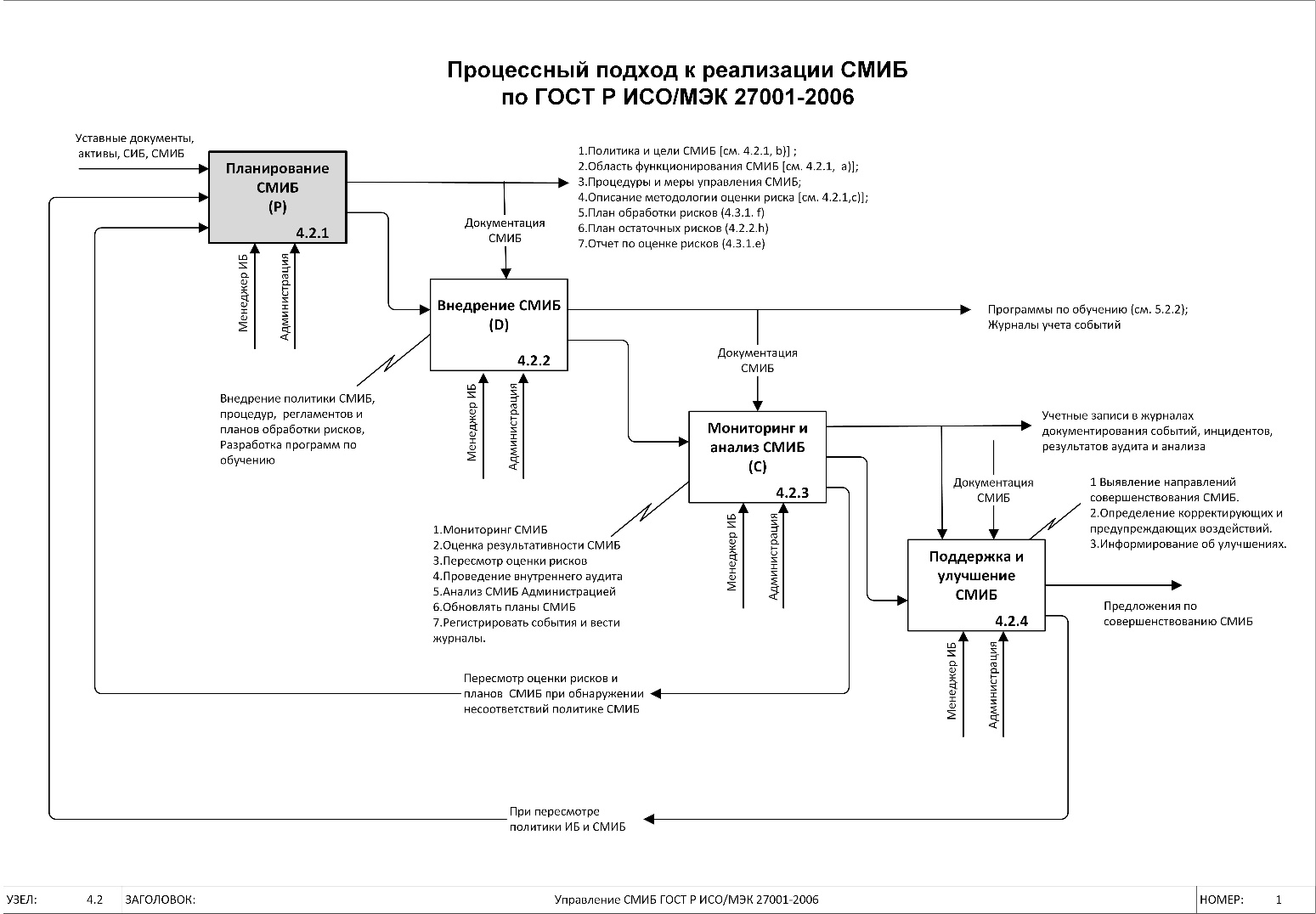


Рис.1. Концепция СМИБ на основе ГОСТ Р ИСО/МЭК 27001-2006 г.

На стадии ***реализации*** осуществляются внедрение и поддержка политики информационной безопасности (организации, средств управления (защитных мер), регламентов, процессов и процедур системы защиты информации.

На стадии ***проверки*** осуществляются оценка и, если необходимо, измерение эффективности процессов управления информационной безопасностью организации на соответствие требованиям политики информационной безопасности, целям и установленным практикам, обеспечивается отчетность высшему руководству о результатах для проведения соответствующего анализа.

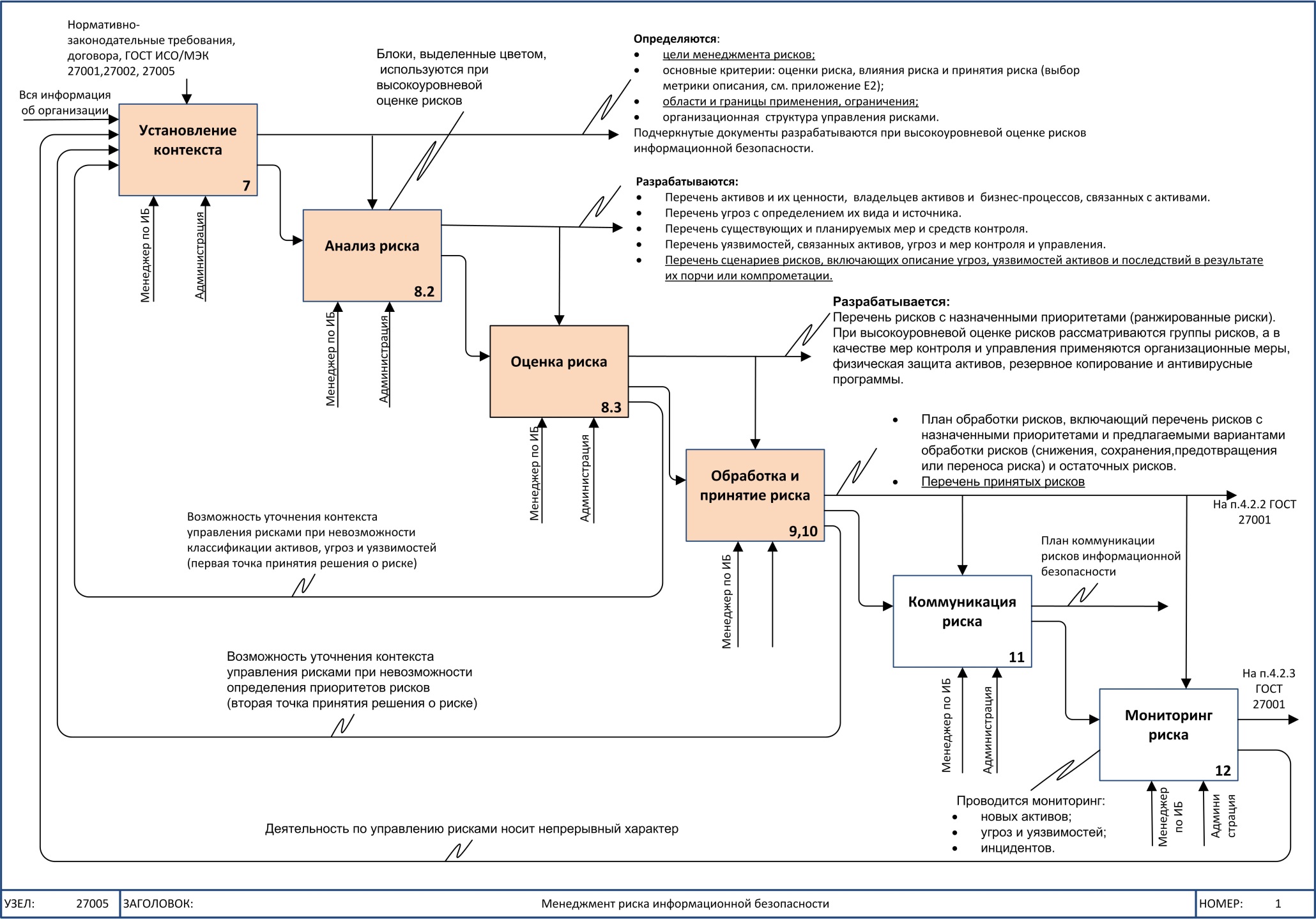
На стадии ***совершенствования*** осуществляются выработка и принятие корректирующих и превентивных действий, основанных на результатах анализа, для достижения непрерывного усовершенствования СМИБ организации.

Особенность того подхода к управлению ИБ заключается в том, что построение СМИБ основано на анализе технологий ведения бизнес-процессов, оценке финансовых возможностей ХС, оценке уровня понимания администрацией ХС необходимости защиты информационных ресурсов организации, рекомендаций стандартов по лучшим мировым практикам организации защиты информации и учете ряда других факторов. Для каждой организации это, безусловно, разные решения. Очень важно, что в организации защиты информации принимают участие все сотрудники ХС и, конечно, его администрация. Этот стандарт даёт большую возможность в определении уровня защищенности ХС от различных факторов. Основным механизмом, определяющим важность угроз влияющих на бизнес-процессы является оценка рисков информационной безопасности, которая выполняется на этапе планирования СМИБ.

Сегодня существуют различные подходы к оценке рисков информационной безопасности, но все они обладают дают субъективные оценки и не учитывают множество других факторов, важных в принятии решений. Это требует от специалистов по информационной безопасности дополнительной работы по определению критериев принятия рисков, влияния и их граничных значений. Так эти процессы слабо формализованы, то каждая организация разрабатывает свои подходы к оценке рисков информационной безопасности, а весь цикл планирования СМИБ может быть представлен на этой диаграмме (рис.2). При оценке рисков используются рекомендации и приложение (Е) стандарта ГОСТ Р ИСО/МЭК 27005-2012 г. [2].

При проведении оценки рисков и разработки план обработки рисков определяются необходимые контрмеры. Для этого применяются практические правила управления информационной безопасностью, которые приведены в стандарте ГОСТ Р ИСО/МЭК 27002-2013г. [3]. Эти правила включают в себя более 800 рекомендаций по следующим направлениям обеспечения информационной безопасности*:*

1. *Разработка политики информационной безопасности.*
2. *Решение организационных вопросов безопасности.*
3. *Классификация и управление активами.*
4. *Вопросы безопасности, связанные с персоналом.*
5. *Физическая защита и защита от воздействий окружающей среды.*
6. *Управление передачей данных и операционной деятельностью.*
7. *Контроль доступа.*
8. *Разработка и обслуживание информационных систем.*
9. *Управление непрерывностью бизнеса.*
10. *Оценка соответствия.*

 Рис.2.Процессы менеджмента рисков информационной безопасности

Стандарт имеет большое значение при организации защиты информации в бизнесе и, по существу, может использоваться при защите любой информации. Особенность концепции защиты в этом стандарте заключается в определении политики безопасности, которая создается совместно с руководством организации и в определении ценности информационных активов, в отношении которых и планируется защита.

К сожалению, более глубокие методологические подходы к построению систем информационной безопасности, основанные на принципах адаптивного управления, эмерджентности и гомеостаза сегодня в теории информационной безопасности не рассматриваются. Есть и другие интересные подходы к организации системы защиты информации, которые высказываются на уровне идей без соответствующей научной и методической их проработки. Наиболее интересной идеей к построению системы информационной безопасности является объектно-ориентированный подход, широко используемый при создании современных информационных систем. Сущность этого подхода основана на создании принципиально любых систем, способных к эволюционному развитию. Этот подход основан на простой идее: любая система должна строиться таким образом, чтобы дальнейшее развитие не отвергало предыдущие формы ее реализации. Автором этого взгляда на новую методологию создания информационных системе является Гради Буч. Элементы этого подхода реализованы в одном из самых перспективных сегодня стандартов [4], содержащий совершенно новую концепцию защиты информационных технологий, но, к сожалению, слабо используемый сегодня в системах защиты информации.

Предлагаемая деловая ситуация имеет цель обучить методам и технологиям организации защиты информации на ХС. Особенность заключается в том, что в информационной системе организации присутствуют различные формы документов (электронные и бумажные) с различной степенью их конфиденциальности. Это требует внимательного и тщательного подхода к изучению исходной информации и руководящих документов по организации защиты информации. Методология организации защиты информации основывалась на концепции учета приоритетов ценностей информационных активов организации, наиболее применимой для бизнеса и изложенной в ГОСТ ИСО/МЭК 27002. Организационные вопросы создания режимов банковской и коммерческой тайны не рассматривались. Политика безопасности разрабатывалась в соответствие с рекомендациями стандарта [3]. Обоснование предложений по защите информации проводилось с использованием требований стандарта [3] по различным моделям рисков [2] и многофакторным моделям.

Деловая ситуация проходит в несколько этапов. По каждому этапу студентами представляется соответствующая отчетность на сайте (адрес сайта указывается преподавателем) в доступном для них разделе. Необходимые справочные материалы и нормативная информация: стандарты, положения и другие материалы представлены также на этом же портале.

# 1.Постановка задачи

### 1.1.Описание ситуации

Акционерный коммерческий банк АКБ «***Х-TrimBank***» расположен в одном из городов Московской области и обеспечивает обслуживание юридических и физических лиц города и ближайших населенных пунктов следующими услугами в соответствие со ст.5 ФЗ №395 от 1990 года [1]:

* *привлечение денежных средств физических и юридических лиц во вклады (до востребования и на определенный срок);*
* *открытие и ведение банковских счетов физических и юридических лиц;*
* *осуществление переводов денежных средств по поручению физических и юридических лиц, в том числе банков-корреспондентов, по их банковским счетам;*
* *инкассация денежных средств, векселей, платежных и расчетных документов и кассовое обслуживание физических и юридических лиц;*
* *купля-продажа иностранной валюты в наличной и безналичной формах;*
* *осуществление переводов денежных средств без открытия банковских счетов, в том числе электронных денежных средств.*

Анализ экономической эффективности работы удаленного офиса, проведенный управляющим банка показал, что в текущем году был значительный рост непроизводственных потерь и, в том числе, из-за инцидентов включающих:

1. *Выход из строя оборудования серверной комнаты из-за затопления, что привело к необходимости закупки нового оборудования.*
2. *Заражение локальной вычислительной сети вредоносными программами, что вызвало значительную потерю времени на восстановление системы.*
3. *Превышение входящего трафика по сравнению с прошлым аналогичным периодом, что привело к дополнительным затратам.*
4. *Неумение работы сотрудников с автоматизированными банковскими системами и системами защиты информации, что приводило к частым отказам общего и специального программного обеспечения при обслуживании клиентов банка и, как следствие, потере клиентов и снижение репутации АКБ.*
5. *Существующая система информационной безопасности не обеспечивает требования по непрерывности бизнеса. За прошедший год было зафиксировано 32 инцидента остановки банковского технологического процесса на срок от 1 до 24 часов.*

По оценкам Правления банка общие потери по этим причинам составили до ***х*** руб за прошедший год (*потери задаются вариантом задания*). В результате проведенного внутреннего аудита системы комплексной безопасности, выполненной специалистом центрального офиса банка, было выявлено следующее (табл.1).

Результаты аудита

*Таблица 1*

|  |  |  |
| --- | --- | --- |
| **№№** | **Категория угроз** | **Наименование уязвимостей системы ИБ, выявленных при аудите** |
| 1 | ФБ | Средства управления физическим доступом в служебные помещения не соответствуют требованиям защиты информации и допускают возможность проникновения посторонних лиц. |
| 2 | ФБ | Входы в помещения закрываются с использованием механических замков, что недостаточно для обеспечения безопасности активов. |
| 3 | ФБ | Офис не оборудован комнатой для ведения переговоров с клиентами, а кабинет управляющего не обеспечивает защиту конфиденциальной информации при проведении совещаний и переговоров. |
| 4 | ФБ | Камеры видеонаблюдения записывают информацию в архив в автоматическом режиме со сроком хранения 1 неделя. |
| 5 | ФБ | Датчики на проникновение в помещение в ночное время отсутствуют. |
| 6 | ФБ | Отсутствует сигнализация на сейфе управляющего и сейфе начальника службы ИБ для хранения документации, электронных ключей и криптографических средств. |
| 7 | ФБ | Размещение и оборудование рабочих мест допускает возможность допуска к АРМ посторонних лиц. |
| 8 | ФБ | Отсутствуют датчики пожарной сигнализации. |
| 9 | ФБ | В помещениях отсутствуют кондиционеры, что приводит к повышению температуры в помещении в летнее время до +35 град С. |
| 10 | ФБ | Во всех помещения используются установки автоматического водяного пожаротушения, это может привести к выводу из строя оборудования. |
| 11 | ФБ | Отсутствует средство резервного копирования и хранения БД АСУ |
| 12 | ФБ | Телекоммуникации и связь не имеют резервных каналов. |
| 13 | ФБ | Электрообеспечение на случай аварий не предусмотрено. Блоки бесперебойного питания не контролируются на обеспечение аварийного завершения бизнес-процессов. |
| 14 | ФБ | Входы в помещения не оборудованы электронными замками и не имеют СКУД. |
| 15 | ЭИС | Общее программное обеспечение (операционные системы, офисные приложения, графические программы не являются лицензионными). Система восстановления сбоев операционных систем основана на повторной их инсталляции. |
| 16 | ЭИС | На компьютерах установлено программное обеспечение неизвестного авторства и не сертифицированное. |
| 17 | ЭИС | Антивирусные программы используются не на всех рабочих местах. Обновления баз данных сигнатур делается самостоятельно на каждом рабочем месте. |
| 18 | УД | Портальное решение эксплуатируется без механизма безопасности «неизменяемость контента», что может привести к потере репутации банка. |
| 19 | ОБ | Политика информационной безопасности существует, но является общей и не отражает специфику этого АКБ . |
| 20 | ОБ | Политика системы менеджмента информационной безопасности (СМИБ) отсутствует. |
| 21 | ОБ | Система управления информационной безопасностью находится на невысоком уровне зрелости администрации АКБ. |
| 22 | ОБ | Требования по обеспечению непрерывности бизнес-процессов не выполняются, а раздел политики информационной безопасности по непрерывности бизнеса отсутствует. |
| 23 | УД | Все сотрудники имеют неограниченный доступ в Интернет и могут использовать практически все его ресурсы. |
| 24 | ОБ | Служебная информация может свободно копироваться на внешние носители: DVD, CD, USB. |
| 25 | ОБ | Не организован учет носителей информации, а сами носители не имеют маркировки (коммерческая тайна, банковская тайна). Для передачи информации используются личные носители (FLASH) информации. |
| 26 | ОБ | Основные информационные активы и баз данных регулярно не обновляются. Периодичность их обновления доходила до 3 месяцев. |
| 27 | ОБ | Документация (инструкции, регламенты) по обработке информации и разграничении доступа к ней отсутствуют. В наличие имеется только «Положение о порядке доступа пользователей к локальной банковской сети и программным комплексам АКБ «Хtrim-Bank» |
| 28 | ОБ | Бумажные носители информации с ошибками оформления договоров, копии документов не уничтожались, а выбрасывались в мусорные корзины. |
| 29 | ОБ | Инциденты, связанные с информационной безопасностью документально не фиксируются и оперативно не доводятся до администрации АКБ. |
| 30 | ОБ | Внутренний аудит информационной безопасности не проводится. |
| 31 | ОБ | Внешний аудит системы информационной безопасности не проводился. |
| 32 | ОБ | Архивирование баз данных, размещенных на сервере не производится регулярно. |
| 33 | ОБ | Бумажные копии договоров хранятся в открытом виде в шкафах помещений для работы с клиентами. |
| 34 | ОБ | Отсутствует резервное оборудование, что приводит к остановке бизнес-процессов. |
| 35 | УД | Парольная политика доступа к информационным активам не соответствует требованиям защиты банковской тайны. |
| 36 | ОБ | Сопровождение информационных систем и процессов обеспечения информационной безопасности делегировано одному сотруднику. |
| 37 | ОБ | Политика «двойного управления» не используется при проведении ответственных операций. |
| 38 | ОБ | В помещениях, где проводится обработка конфиденциальной информации (банковской тайны) не обеспечена защита от утечки информации. |
| 39 | ОБ | Режим банковской и коммерческой тайн в АКБ не введен. |
| 40 | ОБ | Обслуживание оборудования на территории офиса проводится без соблюдения требований по обеспечению информационной безопасности при работе с другими организациями. |
| 41 | ОБ | Помещение управляющего не сертифицировано на обеспечение безопасности коммерческой и банковской тайн. |
| 42 | ОБ | Нерегулярное копирование БД. |
| 43 | ОБ | Отсутствует план обеспечения непрерывности бизнеса. |
| 44 | ОБ | Документация по СМИБ не утверждена и имеется в неполном объеме. |
| 45 | ОБ | Журналы событий должностными лицами регулярно не просматриваются. |
| 46 | ОБ | Группа расследования инцидентов информационной безопасности не создана. Часть инцидентов не доводится с рабочих мест. |
| 47 | ОБ | Резервы расходных материалы на принтеры не созданы. |
| 48 | КБ | Обучение сотрудников методам и технологиям защиты информации не производится, а инструктажей не делается. |
| 49 | КБ | Набор персонала проводится без учета требований работы с конфиденциальной информацией. |
| 50 | КБ | Договора с сотрудниками не включают требования к ним по хранению коммерческой и банковской тайны. |

Обозначения: ФБ-физическая защита;

ОБ-организация защиты;

КБ-кадровые вопросы безопасности;

УД-управление доступом;

П-политика безопасности;

ЭИС-эксплуатация информационных систем.

Схема размезения активов и рабочих мест приведена на рис.3.

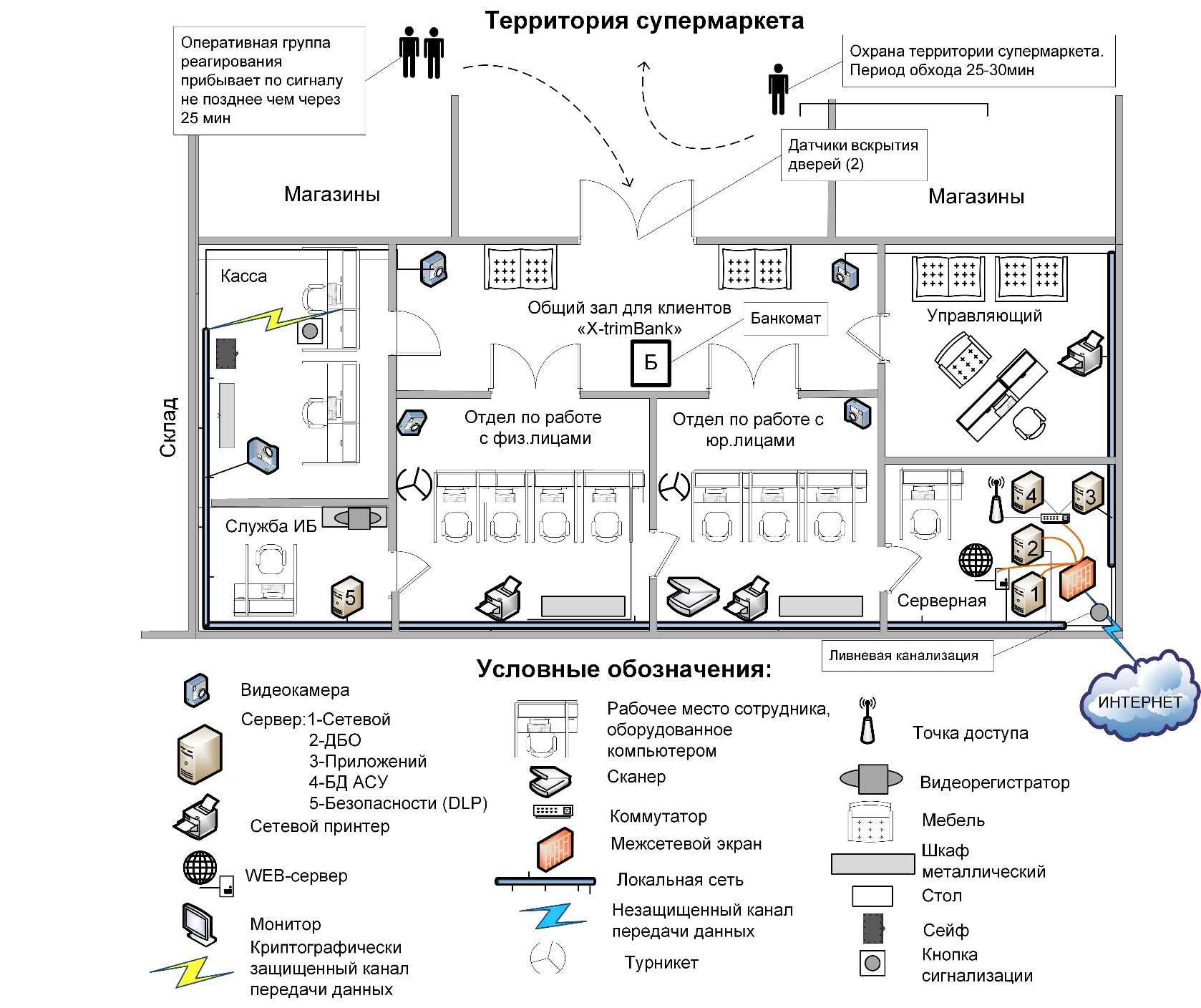


Рис.3.Схема размещения рабочих мест и оборудования АКБ «***Х-TrimBank***»

### 1.2.Дополнительная информация

1. Система технических средств охраны включает 6 видеокамер (рис.1), видеорегистратор и охранную сигнализацию, установленную на входную дверь банка и дверь кассового отделения.
2. На всех рабочих местах установлены источники бесперебойного питания, обеспечивающие работу оборудования при отключенном питании до 10 мин.
3. Работа сотрудников банка осуществляется в 2 смены с 9.00 до 22.00 для специалистов по работе с физическими и юридическими лицами.
4. Дистанционное банковское обслуживание (ДБО) обеспечивается круглосуточно. Контроль процессов обслуживания, подключение клиентов к системе ДБО, генерация ключей и настройку доступа обеспечивает инженер АСУ.
5. Решение вопросов обеспечения доступа в вечернее время и в выходные дни осуществляется инженером АСУ через удаленный рабочий стол.
6. Работу портала обеспечивает персонал компании-провайдера Интернет. Изменения информации на портале и его контроль обеспечивает заместитель управляющего банком.
7. Офис АКБ размещен в крупном торговом центре в цокольном этаже здания и имеет внутреннюю охрану и внешнее наблюдение.
8. Архивы бумажных документов хранятся в металлических шкафах в соответствующих отделах по работе с физическими и юридическими лицами.
9. Организационно-штатная структура банка включает:

* *управляющего банка;*
* *его заместителя;*
* *операторов-кассиров (2 сотрудника, один из них старший оператор-кассир);*
* *ведущего специалиста по работе с физическими лицами (начальник отдела);*
* *специалистов отдела по работе с физическими лицами (2 сотрудника);*
* *ведущего специалиста по работе с юридическими лицами (начальник отдел;*
* *специалиста по работе с юридическими лицами;*
* *специалиста по информационной безопасности;*
* *инженера АСУ (системный администратор);*
* *бухгалтера.*

### 1.3.Основные активы банка

К основным активам банка относятся (таблица 2).

*Таблица 2.*

Основные активы АКБ

|  |  |  |
| --- | --- | --- |
| **№№** | **Наименование активов** | **Примечание** |
| 1 | Банковский платежный технологический процесс, включающий все виды платежей в бумажной и электронной формах. Выполняется в расчетно-кассовом отделении (относится к банковской тайне). |  |
| 2 | Банковский технологический процесс по обслуживанию физических лиц (депозиты, кредиты). |  |
| 3 | Банковский технологический процесс по обслуживанию юридических лиц (счета, кредиты). |  |
| 4 | Банковский процесс дистанционного обслуживания клиентов (ДБО). |  |
| 5 | Банковский технологический процесс «мобильный банкинг». |  |
| 6 | Банковский технологический процесс межбанковских переводов (выполняется в расчетно-кассовом отделении). |  |
| 7 | Банковский технологический процесс генерации отчетов для ЦБ РФ (выполняется в отделении по работе с юридическими лицами). |  |
| 8 | Банковский процесс обменных валютных операций (выполняется в расчетно-кассовом отделении). |  |
| 9 | Банковское делопроизводство (внешнее и внутреннее) включает обычную почту, внутреннюю и внешнюю электронную почту для сотрудников в соответствии с их должностными полномочиями. Ответственный – заместитель управляющего банка. |  |
| 10 | Системная документация по АСУ, программному обеспечению, операционным системам. |  |
| 11 | Руководства и инструкции должностных лиц по работе с информационными системами. |  |
| 12 | Инструкции по обеспечению информационной безопасности сотрудниками банка. |  |
| 13 | Учебные материалы по функциональным процедурам, выполняемым сотрудниками АКБ (Ответственный – заместитель управляющего банком). |  |
| 14 | Планы по обеспечению непрерывности функционирования информационного обеспечения (Ответственный – заместитель управляющего банком). |  |
| 15 | Документированная политика информационной безопасности АКБ (Начальник службы ИБ). |  |
| 16 | Документация по процедурам действий должностных лиц при сбоях информационных систем, нарушении режимов работы и архивирования информации. |  |
| 17 | Активы программного обеспечения (инсталляции и установленное ПО): операционные системы прикладное программное обеспечение, АСУ банковскими процессами, системное программное обеспечение, инструментальные средства разработки и утилиты. |  |
| 18 | Учебные базы данных АСУ АКБ. Используются для предварительной проверки обновлений и нового программного обеспечения. |  |
| 19 | Периодически обновляемые образы системных разделов дисков АРМ и серверов. |  |
| 20 | Антивирусное ПО (инсталляции и установленное). |  |
| 21 | Средства криптографической защиты информации (СКЗИ): электронные системы аутентификации пользователей; системы шифрования дисковых данных; системы шифрования данных, передаваемых по сетям; средства управления ключевой информацией. |  |
| 22 | Компьютерное оборудование (процессоры, мониторы, переносные компьютеры, модемы), оборудование связи (маршрутизаторы, автоматические телефонные станции с выходом в сеть общего пользования, факсы, автоответчики), магнитные носители (ленты и диски). |  |
| 23 | Другое техническое оборудование (источники бесперебойного питания, кондиционеры). |  |
| 24 | Система видеонаблюдения (видеокамеры и регистраторы). |  |
| 25 | Системное программное обеспечение, включающее: операционные системы, сетевые приложения и сервисы, необходимые для обеспе­чения надежного функционирования информационно - вычислительной техники банка. Ответственный – инженер АСУ. |  |
| 26 | Банковская локально-вычислительная сеть и оборудование (маршрутизаторы, сервер, рабочие станции, сетевые устройства печати, сканер). Ответственные за оборудование - начальники соответствующих отделов банка. Ответственный за поддержание в исправном состоянии и администрирование – инженер АСУ. |  |
| 27 | Представительство банка в глобальной информационной сети ИНТЕРНЕТ (портал Х-TrimBank.ru). Ответственный – провайдер Интернет. |  |
| 28 | Автоматизированная банковская система (АБС), обеспечивающая реализацию основных функций банковских технологических процессов по работе с клиентами при выполнении различных банковских услуг (кредиты, депозиты, ценные бумаги и др. операции). Клиентская база данных относится к банковской тайне. Ответственность за информацию – персональная для сотрудников, имеющих доступ к АБС. Ответственность за работу АСУ – инженер АСУ. |  |
| 29 | Персональные данные сотрудников и клиентов банка (электронная и бумажная форма) хранятся в кабинете управляющего. В электронном виде эта информация доступна только для управляющего банка и его заместителю. |  |
| 30 | Прикладное программное обеспечение, необходимое для обеспечения  жизнедеятельности основных и вспомогательных банковских процессов (реклама, видеоролики и т.д.). Ответственный за программное обеспечение – инженер АСУ. Ответственные за материалы – заместитель управляющего и исполнители. |  |
| 31 | Отчетные материалы бухгалтерской отчетности и другие сведения о деятельности банка, доступные для всех. Ответственный – бухгалтер. |  |
| 32 | Информационные базы и информационные архивы, являющиеся результатом финансовой, экономической и управленческой деятельности банка (в бумажном и электронном формах). Имеют статус «банковская тайна», размещаются в кабинете управляющего банком. |  |
| 33 | Системы международных платежей и переводов. Технология переводов с использо-ванием крипто ключей осуществляется операторами-кассирами. Генерация крипто ключей проводится сотрудником службы безопасности АКБ. |  |
| 34 | Сертификаты, лицензии и другие документы, сгенерированные банком самостоятельно и полученные им для использования от других организаций ( например ЦБ и пр.). Размещаются в кабинете управляющего банка в сейфе. |  |
| 35 | Отчетные материалы бухгалтерской отчетности и другие сведения о деятельности банка, доступные для всех. Ответственный – бухгалтер. |  |
| 36 | Информационные каналы, арендуемые и используемые для перемещения информационных потоков: системы связи служебной (внутренней), городской и мобильной, сети и др. Ответственный за эксплуатацию –инженер АСУ. |  |
| 37 | Системы международных платежей и переводов. Технология переводов с использованием крипто ключей осуществляется операторами-кассирами. Генерация крипто ключей проводится сотрудником службы безопасности АКБ. |  |
| 38 | Персональные данные сотрудников и клиентов банка (электронная и бумажная форма) хранятся в кабинете управляющего. В электронном виде эта информация доступна только для управляющего банка и его заместителю. |  |
| 39 | В кабинете управляющего банка проводятся совещания, которые могут содержать конфиденциальную информацию – банковскую и коммерческую тайну. |  |
| 40 | Банкомат в общем зале (Б). |  |

# 2.Методика выполнения задания

Деловая ситуация выполняется в форме отдельных функционально завершенных работ, выполняемых в определенной последовательности (рис.4). Содержание этих работ определяется концепцией создаваемой системой защиты информации для АКБ. В нашем случае для АКБ *«X-trimBank»* была использована модель защиты на основе требований стандарта ГОСТ ИСО/МЭК 27002-2012 г. По каждому этапу результаты работы представляются в форме таблиц, графиков и диаграмм. В результате их анализа делаются выводы, позволяющие обратить внимание на основные и наиболее важные для последующих работ значения анализируемых показателей.

### 

Рис.4. Последовательность оценки рисков

### 2.1.Установление контекста (подготовительный этап)

При выполнении этого этапа определить сначала цель (цели) управления рисками, а затем исходя из этого, определить основные критерии, области и границы применения и методики обработки рисков.

2.1.1.Определение основных целей управления рисками

Возможные цели по возрастанию сложности решения задач:

1. Провести высокоуровневую оценку рисков информационной безопасности и предложить адекватные рискам меры и средства управления и контроля системой информационной безопасности.
2. Повысить эффективность системы управления информационной безопасностью организации за счет обоснования адекватных рискам мер контроля и управления.
3. Повысить эффективность бизнеса за счёт совершенствования системы управления СМИБ и снижения ущерба от реализации возможных угроз информационной безопасности.

2.1.2.Определение основных критериев

***Критерии\_оценки\_риска***

Возможны следующие варианты мер риска (метрик):

1. В виде обобщенного значения показателя величины риска ***Kr=F(Kt, Ky, Ka),***

где ***Kt –*** шкала классификации угроз [0,1,2];

***Ky –*** шкала классификации уязвимостей [0,1,2];

***Ka*** – шкала классификации активов по ценности [0,1,2,3,4].

Пример такого показателя приведен в приложении Е (табл.Е.1а) [1]. Конечные значения величины риска могут быть заданы в форме лингвистической переменной «малый» [0-2], средний [3-4], высокий [5-6], критичный [7-8]. Значения в квадратных скобках определяют границы интервалов метрики рисков заданных табл. E.1a [1].

1. В виде экспертных оценок влияния на бизнес-процессы, заданных в форме лингвистической переменной «малое», «среднее», «высокое», «критичное». Эта форма критерия оценки риска используется при высокоуровневой оценке рисков (приложение Е [1]).
2. В виде меры риска, основанной на соотношении величины возможного ущерба и затрат на принятие контрмер по снижению риска в одной из следующих форм:

***R=Uat – Zat*** или ***R=Uat / Zat,***

где ***Uat*** – оценка величины возможного ущерба;

***Zat*** – оценка величины затрат на принятие контрмер по угрозе ***t.***

Эта форма критерия используется при многофакторной оценке рисков и отличается от предыдущих оценок тем, что метрика рисков универсальна и имеет экономический смысл. Это позволяет одновременно учесть критерий влияния.

Для каждого из рассмотренных критериев используется различная методика оценки рисков.

Критерии\_оценки влияния риска на бизнес-процессы (Kv)

1. В виде обобщенного значения показателя влияния на бизнес-процессы, как функции от ***вероятности сценария инцидента (в шкале степени влияния на бизнес)***. Пример в приложении Е (табл.Е.1b) [1]. Конечные значения величины влияния угрозы могут быть заданы в форме лингвистической переменной «малое» [0-2], «среднее» [3-4], «высокое» [5-6], «критичное» [7-8]. Значения в квадратных скобках определяют границы интервалов метрики рисков заданных табл. E.1b [1].
2. В форме экспертных оценок влияния на бизнес-процессы, заданных в форме лингвистической переменной «малое», «среднее», «высокое», «критичное».

***Критерии\_принятия риска (Kp)***

Представляют собой определённые значения критериев оценки рисков и влияние, которые являются пороговыми при принятии решения. Так как эти критерии трудно определить в начальном цикле оценки рисков, процесс оценки рисков повторяется начиная с первого этапа «Установления контекста» организации (раздел 6) [1].

### 2.2.Инвентаризация и классификация информационных активов (этап 1)

Основная цель этапа - изучение бизнес-процессов организации, инвентаризация и классификация информационных активов АКБ *«X-trimBank»*.

В результате выполнения этого этапа определяются приоритеты активов по их ценности. Модель классификации информационных активов необходимо представить в форме кортежа

***<A, F, H, V >*** (1)

где

*А (active)* – информационный актив АКБ *«X-trimBank» (по варианту задания).*

*F (form)*– форма представления актива (процесс, база данных, бумажный документ, программное обеспечение, оборудование, архив и т.д.).

*H (holder)* –владелец актива.

*V (value)–* оценка ценности активов в форме терм-переменной, принимающей значения «критичная», «высокая», «средняя», «низкая». Возможна и количественная оценка ценности актива при его утрате, выходе из строя или компрометации.

Результаты представляются в форме таблицы, ранжированной по уровню ценности активов. По результатам анализа таблицы делаются выводы о ценности информационных активов и ответственных за их безопасность. Результаты анализа представляются в форме гистограмм «распределение активов по ценности» и «распределение активов по ответственным». По результатам анализа делаются выводы.

**Пример по инвентаризации и классификации актива**

Пример моделирования и классификации активов в следующей табл.

*Таблица 3*.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***№№*** | ***A (номер актива)*** | ***(БП-бизнес-процесс; Об-оборудование; По-программное обеспечение; Ос - операционная система; Ас-автоматизированная банковская система; Тк - телекоммуникационный канал связи ... )*** | ***H (владелец: У-управляющий, З-заместитель, И-инж.-адм., Ф-отдел ФЛ, Ю-отдел Юрл)*** | ***V (ценность: высокая (В), средняя (С), низкая (Н) )*** | ***Примечание*** |
| 1 | 1 | БП | У | С | Техн. процесс |
| 2 | 4 | Об | З | Н | АРМ |
| 3 | 5 | Об | Ф | Н | Принтер |

Результаты анализа представляются в следующей форме (рис.4).

Рис.5

В конце анализа делаются выводы:

* Как распределяется ответственность персонала по активам ?
* Как распределяются активы по ценности ?
* Как распределяются активы по ценности и персоналу ?

### 2.3.Моделирование угроз и оценка рисков информационной безопасности (этап 2)

В таблице 4 приведены угрозы, актуальные для АКБ *«X-trimBank* [2, прил.1-С]

*Таблица 4*

Актуальные угрозы АКБ *«X-trimBank*

|  |  |  |
| --- | --- | --- |
|  | |  |
| **N (актив)** | **Вид угрозы** | **Содержание угрозы** |
| 1.1 | Физический ущерб | Пожар |
| 1.2 | Ущерб, причиненный водой |
| 2.1 | Природные явления | Климатическое явление |
| 3.1 | Утрата важных сервисов | Авария системы кондиционирования воздуха или водоснабжения |
| 3.2 |  | Нарушение энергоснабжения |
| 3.3 |  | Отказ телекоммуникационного оборудования |
| 4.1 | Помехи вследствие излучения | Электромагнитное излучение |
| 4.2 |  | Электромагнитные импульсы |
| 5.1 | Компрометация информации | Перехват компрометирующих сигналов помех |
| 5.2 |  | Дистанционный шпионаж |
| 5.3 |  | Прослушивание |
| 5.4 |  | Кража носителей или документов |
| 5.5 |  | Кража оборудования |
| 5.6 |  | Поиск повторно используемых или забракованных носителей |
| 5.7 |  | Данные из ненадежных источников |
| 5.8 |  | Преступное использование аппаратных средств |
| 5.9 |  | Преступное использование программного обеспечения |
| 6.1 | Технические неисправности | Отказ оборудования |
| 6.2 |  | Неисправная работа оборудования |
| 6.3 |  | Нарушение функционирования программного обеспечения |
| 6.4 |  | Нарушение сопровождения информационной системы |
| 7.1 | Несанкционированные действия | Несанкционированное использование оборудования |
| 7.2 | Мошенническое копирование программного обеспечения |
| 7.3 |  | Использование контрафактного или скопированного программного обеспечения |
| 7.4 |  | Искажение данных |
| 7.5 |  | Незаконная обработка данных |
| 8.1 | Компрометация функций | Ошибка при использовании |
| 8.2 |  | Злоупотребление правами |
| 8.3 |  | Фальсификация прав |
| 8.4 |  | Отказ в осуществлении действий |
| 8.5 |  | Нарушение работоспособности персонала |

Моделирование угроз для информационных активов банка проводится по результатам аудита. Модель угроз представляются в форме кортежа [3]

***<Nt, T, A, Ny, YTA ,* [*PTY,*] *UTA, M,* [*Ktv*]*>,***(2)

где

***N*** *–*угроза (наименование) или код (табл.4).

***T*** –классификация угрозы по шкале [0, 1, 2].

***A***– наименование актива (объекта) или его код (табл.2), в отношении которого реализуется угроза.

***Ny*** – наименование уязвимости или её код (табл.1).

***YTA*** – уязвимости актива по этой угрозе, заданные по шкале [0, 1, 2].

***PTY*** *–* вероятность реализации угрозы по этой уязвимости (в том случае, если угроза оценивается по шкале вероятности ).

***UTA*** – оценка возможных результатов реализации угрозы, оценивается как ценность актива по шкале [ 0, 1, 2, 3, 4 ].

***Ktv –*** показатель влияния на бизнес-процессы (при необходимости).

***M*** – метрика комплексной оценки угроз с учетом уязвимостей и ценности актив [2, прил.Е.1.а] , рассчитываемая как сумма ***M=T+Yta+Uta*** . Вариант моделирования угроз по одному активу представлен в табл.5.

*Таблица 5*

Результаты моделирования угроз (фрагмент)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ***Nt*** | ***T*** | ***A*** | ***Ny*** | ***Yta*** | ***Pty*** | ***Uta*** | ***M*** |
| 1.1 | 0 | 2 | 8 | 0 | 0 | 2 | 2 |
| 1.2 | 1 | 2 | 9 | 0 | 0 | 2 | 3 |
| 3.1 | 1 | 2 | 12 | 1 | 1 | 1 | 3 |
| 3.2 | 1 | 2 | 13 | 1 | 1 | 1 | 3 |

Анализ проводится по диаграммам и графикам (рис.5).

В результате анализа делаются выводы:

1. Как распределяются угрозы по вероятности и возможному ущербу ?
2. Как распределяются угрозы по степени опасности и ценности активов ?
3. Как распределяются угрозы по уязвимости активов и их ценности ?

Таблица 6

Сводная таблица для анализа результатов моделирования угроз

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **A** | (Все) |  |  |  |
|  |  |  |  |  |
|  | Данные |  |  |  |
| **Nt** | **Количество по полю Ny** | **Сумма по полю М** | **Среднее по полю Uta** | **Среднее по полю Yta** |
| 7,3 | 6 | 9 | 5 | 2 |
| 8,1 | 5 | 8 | 5 | 2 |
| 8,2 | 5 | 9 | 5 | 2 |
| 7,5 | 4 | 9 | 5 | 2 |
| 1,1 | 4 | 6 | 5 | 2 |
| 1,2 | 4 | 6 | 5 | 2 |
| 8,5 | 4 | 9 | 5 | 2 |
| 6,2 | 3 | 8 | 5 | 1 |
| 6,3 | 3 | 9 | 5 | 2 |
| 6,1 | 3 | 8 | 5 | 2 |
| 3,2 | 2 | 9 | 5 | 2 |
| 5,9 | 2 | 7 | 4 | 1 |
| 5,4 | 2 | 7 | 5 | 1 |
| 5,3 | 2 | 7 | 3 | 2 |
| 7,4 | 1 | 9 | 5 | 2 |
| 8,4 | 1 | 9 | 5 | 2 |
| 3,3 | 1 | 8 | 5 | 2 |
| 5,7 | 1 | 7 | 5 | 1 |
| Общий итог | 53 | 9 | 5 | 2 |
|  |  |  |  |  |

Рис.7.Диаграмма анализа результатов моделирования угроз

**2.4.Обработка рисков (этап 3)**

При находятся показатели рисков, необходимые для принятия плана обработки рисков, включающие:

* *вариант обработки риска (снижение, сохранение, предотвращение или перенос риска) (****Var****),* ***Var={снижение, перенос, отказ, сохранение }***
* *предлагаемые меры контроля и управления (****Мс****);*
* *затраты на меры контроля и управления (****Zat****).*

Модель обработки рисков может быть представлена в виде:

***<Nt, T, A, Ny, YTA ,* [*PTY,*] *UTA, M, Var, Mc, Zat,* [*Ktv*]*>***(3)

В том случае, если оценка ущерба определялась в форме значения шкалы ценности актива [0-4], для перехода к денежному эквиваленту оценки ущерба определяют предельные значения ущерба для каждой шкалы, а затем применяя процедуру рандомизации, вычисляют случайное значение ущерба для каждой угрозы. Например, «малозначимый» ущерб возможен до 30 000 руб, «средний» до 200 000 руб, «высокий» до 1000000 руб, «критичный» [3] до 5000000 руб и свыше 5000000 руб «недопустимый» [4]. Тогда процедура вычисления ущерба для категории «высокий» будет ***Uta=200000+RND(200000, 1000000***), где ***RND*** –датчик случайных чисел в заданном интервале.

Если критерий вероятности угрозы ( ***Т***) необходимо выразить в численных значениях возможности, тогда используется аналогичная процедура рандомизации значения ***Р***.

Анализ проводится по диаграммам и графикам.

В результате анализа делаются выводы:

1. Как распределяются риски по вариантам обработки и ценности активов ?
2. Как распределяются риски по мерам контроля ?
3. Какие риски взаимосвязаны по мерам контроля и управления ?
4. Как распределяются затраты по мерам контроля и управления в зависимости от мер опасности угроз (***М***) ?
5. Как распределяются риски по степени влияния на бизнес процессы ?

### 2.5.Моделирование плана обработки рисков (этап 4)

Моделирование плана обработки рисков предполагает анализ модели плана по различным стратегиям управления рисками. Модель плана имеет следующий вид:

***<Nt, T, A, Ny, YTA ,* [*PTY,*] *Uat, M, Var, Mc, Zat,* [*Ktv*], *Sz, Su, Uat-Zat>*** (4)

где ***Sz*** - накопленная сумма затрат на меры контроля ранжированных рисков;

***Su*** - накопленная сумма возможных последствий от реализации угроз;

***Uat-Zat –*** разница между двумя суммами.

Основными стратегиями обработки рисков являются:

1. Принятие рисков для которых выполняется условие: ***(М≤Mz)∩ (Ktv≤Kv)*** .
2. Принятие рисков при условии … (разработать самостоятельно).
3. Принятие рисков при условии … (разработать самостоятельно).
4. Принятие рисков при условии … (разработать самостоятельно).
5. Принятие рисков при условии … (разработать самостоятельно).
6. Принятие рисков при условии … (разработать самостоятельно).
7. Принятие рисков при условии … (разработать самостоятельно).

Анализ рисков информационной безопасности и разработка предложений по реорганизации системы защиты информации с учетом требований по обеспечению непрерывности бизнеса. Кроме того, на этом этапе разрабатывается, при необходимости, новая рациональная схема размещения информационных активов. По результатам анализа плана обработки рисков делаются выводы и оцениваются остаточные риски. При высокоуровневой оценке рисков предлагаемые меры включают организационные мероприятия, физическую защиту активов, резервное копирование и антивирусное ПО.

### 2.6.Защита результатов деловой игры

Для защиты необходимо выполнить все этапы по настоящему заданию и подготовить презентацию.

### 2.7.Варианты заданий

Приведены в таблице 7. Например, для 1 варианта предусматривается 6 активов, название их выбираются из таблицы №2 (2, 9,20, 24, 32 и 40). При этом допустимые затраты не должны превышать сумму 1700 000 руб. Угрозы для этих активов берутся из таблицы №1.

Таблица 7

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | **Активы** | | | | | |  |
| **Номер группы** | **Номер варианта задания** | **1** | **2** | **3** | **4** | **5** | **6** | **Затраты (Zo), тыс.руб** |
|  | 1 | 2 | 9 | 20 | 24 | 32 | 40 | 1700 |
|  | 2 | 4 | 12 | 16 | 28 | 31 | 37 | 2500 |
|  | 3 | 7 | 10 | 17 | 28 | 31 | 38 | 2300 |
|  | 4 | 7 | 12 | 17 | 26 | 33 | 39 | 1100 |
|  | 5 | 5 | 9 | 17 | 22 | 34 | 39 | 2500 |
|  | 6 | 6 | 9 | 21 | 27 | 35 | 38 | 2200 |
|  | 7 | 7 | 12 | 18 | 25 | 33 | 39 | 1300 |
|  | 8 | 7 | 14 | 15 | 23 | 31 | 36 | 2000 |
| 6011 | 9 | 2 | 8 | 16 | 29 | 34 | 37 | 1000 |
|  | 10 | 4 | 11 | 19 | 23 | 35 | 37 | 2300 |
|  | 11 | 3 | 8 | 20 | 27 | 32 | 39 | 1700 |
|  | 12 | 7 | 10 | 21 | 29 | 32 | 37 | 900 |
|  | 13 | 1 | 10 | 17 | 22 | 32 | 39 | 900 |
|  | 14 | 6 | 14 | 19 | 29 | 34 | 38 | 2400 |
|  | 15 | 3 | 8 | 19 | 29 | 35 | 39 | 1800 |
|  | 16 | 5 | 13 | 17 | 27 | 32 | 38 | 900 |
|  | 1 | 7 | 13 | 19 | 26 | 31 | 39 | 1400 |
|  | 2 | 1 | 14 | 21 | 27 | 32 | 37 | 600 |
|  | 3 | 1 | 13 | 19 | 22 | 33 | 40 | 1200 |
|  | 4 | 4 | 13 | 16 | 24 | 30 | 36 | 1000 |
|  | 5 | 4 | 9 | 18 | 28 | 32 | 38 | 700 |
|  | 6 | 4 | 14 | 16 | 27 | 32 | 39 | 800 |
|  | 7 | 2 | 8 | 15 | 29 | 32 | 38 | 1300 |
| 6012 | 8 | 4 | 13 | 15 | 25 | 32 | 39 | 1300 |
|  | 9 | 7 | 8 | 16 | 22 | 31 | 38 | 1500 |
|  | 10 | 6 | 8 | 16 | 25 | 31 | 36 | 1600 |
|  | 11 | 5 | 10 | 16 | 26 | 32 | 37 | 2000 |
|  | 12 | 6 | 8 | 15 | 26 | 34 | 37 | 1700 |
|  | 13 | 3 | 13 | 15 | 24 | 33 | 36 | 1600 |
|  | 14 | 4 | 10 | 19 | 29 | 32 | 40 | 1900 |
|  | 15 | 4 | 14 | 18 | 24 | 31 | 40 | 1900 |
|  | 1 | 2 | 9 | 20 | 24 | 32 | 40 | 2000 |
|  | 2 | 4 | 12 | 16 | 28 | 31 | 37 | 1100 |
|  | 3 | 7 | 10 | 17 | 28 | 31 | 38 | 1700 |
|  | 4 | 7 | 12 | 17 | 26 | 33 | 39 | 1500 |
|  | 5 | 5 | 9 | 17 | 22 | 34 | 39 | 1600 |
|  | 6 | 6 | 9 | 21 | 27 | 35 | 38 | 2000 |
|  | 7 | 7 | 12 | 18 | 25 | 33 | 39 | 1700 |
|  | 8 | 7 | 14 | 15 | 23 | 31 | 36 | 1600 |
| 6015 | 9 | 2 | 8 | 16 | 29 | 34 | 37 | 1900 |
|  | 10 | 4 | 11 | 19 | 23 | 35 | 37 | 1500 |
|  | 11 | 3 | 8 | 20 | 27 | 32 | 39 | 1600 |
|  | 12 | 7 | 10 | 21 | 29 | 32 | 37 | 2000 |
|  | 13 | 1 | 10 | 17 | 22 | 32 | 39 | 1700 |
|  | 14 | 6 | 14 | 19 | 29 | 34 | 38 | 1600 |
|  | 15 | 3 | 8 | 19 | 29 | 35 | 39 | 1900 |
|  | 1 | 2 | 9 | 20 | 24 | 32 | 40 | 1700 |
|  | 2 | 4 | 12 | 16 | 28 | 31 | 37 | 2500 |
|  | 3 | 7 | 10 | 17 | 28 | 31 | 38 | 2300 |
|  | 4 | 7 | 12 | 17 | 26 | 33 | 39 | 1100 |
|  | 5 | 5 | 9 | 17 | 22 | 34 | 39 | 2500 |
| 6014 | 6 | 6 | 9 | 21 | 27 | 35 | 38 | 2200 |
|  | 7 | 7 | 12 | 18 | 25 | 33 | 39 | 1300 |
|  | 8 | 7 | 14 | 15 | 23 | 31 | 36 | 2000 |
|  | 9 | 2 | 8 | 16 | 29 | 34 | 37 | 1000 |
|  | 10 | 4 | 11 | 19 | 23 | 35 | 37 | 2300 |
|  | 11 | 3 | 8 | 20 | 27 | 32 | 39 | 1700 |
|  | 1 | 2 | 9 | 20 | 24 | 32 | 40 | 1700 |
|  | 2 | 4 | 12 | 16 | 28 | 31 | 37 | 2500 |
|  | 3 | 7 | 10 | 17 | 28 | 31 | 38 | 2300 |
|  | 4 | 7 | 12 | 17 | 26 | 33 | 39 | 1100 |
|  | 5 | 5 | 9 | 17 | 22 | 34 | 39 | 2500 |
|  | 6 | 6 | 9 | 21 | 27 | 35 | 38 | 2200 |
|  | 7 | 7 | 12 | 18 | 25 | 33 | 39 | 1300 |
|  | 8 | 7 | 14 | 15 | 23 | 31 | 36 | 2000 |
| 6016 | 9 | 2 | 8 | 16 | 29 | 34 | 37 | 1000 |
|  | 10 | 4 | 11 | 19 | 23 | 35 | 37 | 2300 |
|  | 11 | 3 | 8 | 20 | 27 | 32 | 39 | 1700 |
|  | 12 | 7 | 10 | 21 | 29 | 32 | 37 | 900 |
|  | 13 | 1 | 10 | 17 | 22 | 32 | 39 | 900 |
|  | 14 | 6 | 14 | 19 | 29 | 34 | 38 | 2400 |
|  | 15 | 3 | 8 | 19 | 29 | 35 | 39 | 1800 |
|  | 1 | 7 | 13 | 19 | 26 | 31 | 39 | 1400 |
|  | 2 | 1 | 14 | 21 | 27 | 32 | 37 | 600 |
|  | 3 | 1 | 13 | 19 | 22 | 33 | 40 | 1200 |
|  | 4 | 4 | 13 | 16 | 24 | 30 | 36 | 1000 |
|  | 5 | 4 | 9 | 18 | 28 | 32 | 38 | 700 |
|  | 6 | 4 | 14 | 16 | 27 | 32 | 39 | 800 |
|  | 7 | 2 | 8 | 15 | 29 | 32 | 38 | 1300 |
| 6071 | 8 | 4 | 13 | 15 | 25 | 32 | 39 | 1300 |
|  | 9 | 7 | 8 | 16 | 22 | 31 | 38 | 1500 |
|  | 10 | 6 | 8 | 16 | 25 | 31 | 36 | 1600 |
|  | 11 | 5 | 10 | 16 | 26 | 32 | 37 | 2000 |
|  | 12 | 6 | 8 | 15 | 26 | 34 | 37 | 1700 |
|  | 13 | 3 | 13 | 15 | 24 | 33 | 36 | 1600 |
|  | 14 | 4 | 10 | 19 | 29 | 32 | 40 | 1900 |
|  | 15 | 4 | 14 | 18 | 24 | 31 | 40 | 1900 |
|  | 1 | 2 | 9 | 20 | 24 | 32 | 40 | 1700 |
|  | 2 | 4 | 12 | 16 | 28 | 31 | 37 | 2500 |
|  | 3 | 7 | 10 | 17 | 28 | 31 | 38 | 2300 |
|  | 4 | 7 | 12 | 17 | 26 | 33 | 39 | 1100 |
|  | 5 | 5 | 9 | 17 | 22 | 34 | 39 | 2500 |
|  | 6 | 6 | 9 | 21 | 27 | 35 | 38 | 2200 |
|  | 7 | 7 | 12 | 18 | 25 | 33 | 39 | 1300 |
|  | 8 | 7 | 14 | 15 | 23 | 31 | 36 | 2000 |
| 6072 | 9 | 2 | 8 | 16 | 29 | 34 | 37 | 1000 |
|  | 10 | 4 | 11 | 19 | 23 | 35 | 37 | 2300 |
|  | 11 | 3 | 8 | 20 | 27 | 32 | 39 | 1700 |
|  | 12 | 7 | 10 | 21 | 29 | 32 | 37 | 900 |
|  | 13 | 1 | 10 | 17 | 22 | 32 | 39 | 900 |
|  | 14 | 6 | 14 | 19 | 29 | 34 | 38 | 2400 |
|  | 1 | 7 | 13 | 19 | 26 | 31 | 39 | 1400 |
|  | 2 | 1 | 14 | 21 | 27 | 32 | 37 | 600 |
|  | 3 | 1 | 13 | 19 | 22 | 33 | 40 | 1200 |
| 6073 | 4 | 4 | 13 | 16 | 24 | 30 | 36 | 1000 |
|  | 5 | 4 | 9 | 18 | 28 | 32 | 38 | 700 |
|  | 6 | 4 | 14 | 16 | 27 | 32 | 39 | 800 |
|  | 7 | 2 | 8 | 15 | 29 | 32 | 38 | 1300 |
|  | 8 | 4 | 13 | 15 | 25 | 32 | 39 | 1300 |
|  | 9 | 7 | 8 | 16 | 22 | 31 | 38 | 1500 |
|  | 10 | 6 | 8 | 16 | 25 | 31 | 36 | 1600 |
|  | 1 | 7 | 13 | 19 | 26 | 31 | 39 | 1400 |
|  | 2 | 1 | 14 | 21 | 27 | 32 | 37 | 600 |
|  | 3 | 1 | 13 | 19 | 22 | 33 | 40 | 1200 |
|  | 4 | 4 | 13 | 16 | 24 | 30 | 36 | 1000 |
|  | 5 | 4 | 9 | 18 | 28 | 32 | 38 | 700 |
|  | 6 | 4 | 14 | 16 | 27 | 32 | 39 | 800 |
|  | 7 | 2 | 8 | 15 | 29 | 32 | 38 | 1300 |
| 6074 | 8 | 4 | 13 | 15 | 25 | 32 | 39 | 1300 |
|  | 9 | 7 | 8 | 16 | 22 | 31 | 38 | 1500 |
|  | 10 | 6 | 8 | 16 | 25 | 31 | 36 | 1600 |
|  | 11 | 5 | 10 | 16 | 26 | 32 | 37 | 2000 |
|  | 1 | 7 | 13 | 19 | 26 | 31 | 39 | 1400 |
|  | 2 | 1 | 14 | 21 | 27 | 32 | 37 | 600 |
|  | 3 | 1 | 13 | 19 | 22 | 33 | 40 | 1200 |
|  | 4 | 4 | 13 | 16 | 24 | 30 | 36 | 1000 |
|  | 5 | 4 | 9 | 18 | 28 | 32 | 38 | 700 |
|  | 6 | 4 | 14 | 16 | 27 | 32 | 39 | 800 |
|  | 7 | 2 | 8 | 15 | 29 | 32 | 38 | 1300 |
| 6075 | 8 | 4 | 13 | 15 | 25 | 32 | 39 | 1300 |
|  | 9 | 7 | 8 | 16 | 22 | 31 | 38 | 1500 |
|  | 10 | 6 | 8 | 16 | 25 | 31 | 36 | 1600 |
|  | 11 | 5 | 10 | 16 | 26 | 32 | 37 | 2000 |
|  | 12 | 6 | 8 | 15 | 26 | 34 | 37 | 1700 |
|  | 1 | 7 | 13 | 19 | 26 | 31 | 39 | 1400 |
|  | 2 | 1 | 14 | 21 | 27 | 32 | 37 | 600 |
|  | 3 | 1 | 13 | 19 | 22 | 33 | 40 | 1200 |
|  | 4 | 4 | 13 | 16 | 24 | 30 | 36 | 1000 |
|  | 5 | 4 | 9 | 18 | 28 | 32 | 38 | 700 |
|  | 6 | 4 | 14 | 16 | 27 | 32 | 39 | 800 |
|  | 7 | 2 | 8 | 15 | 29 | 32 | 38 | 1300 |
| 6181 | 8 | 4 | 13 | 15 | 25 | 32 | 39 | 1300 |
|  | 9 | 7 | 8 | 16 | 22 | 31 | 38 | 1500 |
|  | 10 | 6 | 8 | 16 | 25 | 31 | 36 | 1600 |
|  | 611 | 5 | 10 | 16 | 26 | 32 | 37 | 2000 |
|  | 612 | 6 | 8 | 15 | 26 | 34 | 37 | 1700 |
| Доп. | 613 | 3 | 13 | 15 | 24 | 33 | 36 | 1600 |
| варианты | 614 | 4 | 10 | 19 | 29 | 32 | 40 | 1900 |
|  | 773 | 1 | 13 | 19 | 22 | 33 | 40 | 1200 |
|  | 774 | 4 | 13 | 16 | 24 | 30 | 36 | 1000 |
|  | 775 | 4 | 9 | 18 | 28 | 32 | 38 | 700 |
|  | 776 | 4 | 14 | 16 | 27 | 32 | 39 | 800 |
|  | 777 | 2 | 8 | 15 | 29 | 32 | 38 | 1300 |
|  | 778 | 4 | 13 | 15 | 25 | 32 | 39 | 1300 |

# Литература

1. Менеджмент рисков информационной безопасности. ГОСТ Р ИСO/МЭК 27005-20012.
2. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. ГОСТ Р ИСO/МЭК 27001-2006.
3. Практические правила управления информационной безопасностью. ГОСТ Р ИСО/МЭК 27002-2012.
4. Обеспечение информационной безопасности организаций банковской системы РФ. Стандарт банка России СТО БР ИББС-1.0-2010. ) [Электронный ресурс] <http://www.cbr.ru/credit/Gubzi_docs/main.asp?Prtid=Stnd>
5. Стандарт Банка России: "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0 - 2010" (СТО БР ИББС-1.2-2010) [Электронный ресурс] <http://www.cbr.ru/credit/Gubzi_docs/main.asp?Prtid=Stnd>
6. Минзов А.С. Методология применения терминов и определений в сфере информационной, экономической и комплексной безопасности бизнеса. Уч-мет. пособие.-М.:ВНИИ геосистем, 2011.-84 с.