|  |  |  |
| --- | --- | --- |
| **УТВЕРЖДЕН** | |  | | --- | |  | |
|  |  |
|  | Общекорпоративная политика информационной безопасности |
|  |  |

**ОАО АКБ "Унивбанк"**

**УТВЕРЖДАЮ**

**Председатель Правления**

**ОАО АКБ «Унивбанк»**

**\_\_\_\_\_\_\_\_\_\_\_\_И.И. Иванов**

**«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_2019 года**

**Общекорпоративная политика информационной безопасности**

**УНВБ. ИБ - 001.1000. ОП**

**ЛИСТ СОГЛАСОВАНИЯ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Согласовано** | Должность | Ф.И.О. | Подпись | Дата |
|  | Вице-президент | Пирогов А.А. | Электронное согласование |  |
|  | Заместитель начальника Департамента информационных технологий | Обижаев А.Л. | Электронное согласование |  |
|  | Начальник Управления делами | Вискова Е.В. | Электронное согласование |  |
|  | Начальник Юридического управления | Мартемьянов К.В. | Электронное согласование |  |
|  | Начальник Департамента банковских технологий и процессов | Костикова Г.А. | Электронное согласование |  |
|  | Главный специалист Отдела технологической документации УБТ | Жанабергенова А.А. | Электронное согласование |  |
|  | Заместитель руководителя Службы внутреннего контроля | Шилова Е.В. | Электронное согласование |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Должность | Ф.И.О. | Подпись | Дата |
| Документ подготовлен | Начальник отдела информационной безопасности | Белясников А.В. |  |  |

**ИНФОРМАЦИЯ О ВЕРСИЯХ ДОКУМЕНТА**

| **№ вер.** | **Дата создания версии** | **Кем создана версия** | **Краткое описание причин и состава изменений документа** | **Наименование файла** |
| --- | --- | --- | --- | --- |
| 1.00 | 39722 |  | Начальная версии документа | Политика ИБ\_Пробизнес.doc |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**СВЯЗАННЫЕ ДОКУМЕНТЫ**

|  |  |  |
| --- | --- | --- |
| **№** | **Наименование документа** | **Наименование файла** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**ПРИНЯТЫЕ СОКРАЩЕНИЯ**

АБС – автоматизированная банковская система.

АКБ – акционерный коммерческий банк.

АРМ – автоматизированное рабочее место.

АС – автоматизированная система.

БД – база данных.

БР – Банк России.

БС РФ – Банковская система Российской Федерации.

ГОСТ – государственный стандарт.

ГОСТ Р – государственный стандарт России.

ЖЩ – жизненный цикл.

ГК РФ – гражданский кодекс Российской Федерации.

ИБ – информационная безопасность.

ИС – информационная система.

ИСО – международная организация по стандартизации.

ИТ – информационная технология.

МЭК – международная электротехническая комиссия.

НСД – несанкционированный доступ.

ОАО – открытое акционерное общество.

ПБоИБ – подразделение Банка, ответственное за информационную безопасность.

ПО – программное обеспечение.

СЗИ – система защиты информации.

СКЗИ – средство криптографической защиты информации.

СПД – сеть передачи данных.

СУБД – система управления базами данных.

СУИБ – система управления информационной безопасностью.

ФЗ – федеральный закон.

ЦБР – Центральный Банк России.

ЭВМ – электронная вычислительная машина.

BCM – Business Continuity Management.

BS – British Standard.

BSI – British Standards Institute.

COBIT – Control Objectives for Information and related Technology.

IDS – Intrusion Detection System.

IS – International Standard.

ISMS-T – Information security management system. Requirements for telecommunications.

ISO – International Organization for Standardization (Международная организация по стандартизации).

ISO TR – International Organization for Standardization (Международная организация по стандартизации).

ITU-T – International Telecommunications Union - Telecommunications sector (Международный союз электросвязи - сектор телекоммуникаций).

OCTAVE – Operationally Critical Threat, Asset, and Vulnerability Evaluation.

PDCA – Plan, Do, Check, Act.

TR - Technical Regulation (технические условия).

**Введение**

В соответствии с положениями Стандарта Банка России (БР) "Обеспечение Информационной Безопасности Банковской Системы Российской Федерации" основными целями деятельности Банка России являются развитие и укрепление Банковской Системы (БС) РФ, а также обеспечение эффективного и бесперебойного функционирования платежной системы РФ и повышение доверия к БС РФ в целом. Важнейшим условием реализации этих целей в Стандарте БР названо обеспечение необходимого уровня информационной безопасности (далее – ИБ) всех организаций БС РФ.

Под информационной безопасностью организации банковской системы РФ понимается состояние защищенности интересов (целей) организации БС РФ в условиях угроз в информационной сфере.

Данное требование является актуальным для ОАО АКБ "Унивбанк" (далее – Банк) – кредитной организации, являющейся частью БС РФ.

Актуальность обеспечения ИБ в целом обуславливается современными условиями ведения бизнеса, характеризующимися возрастающим уровнем конкуренции, глобализацией экономики, растущей зависимостью бизнес-процессов от информационных технологий, большими объемами информационных потоков, сложностью используемых технологий и большим количеством потенциальных угроз ИБ как случайного, так и преднамеренного характера, реализация которых может приводить к негативным последствиям для организации.

Система управления ИБ Банка строится на основе управления рисками ИБ.

# Оглавление

[Оглавление 8](#__RefHeading___Toc222915943)

[1. Назначение документа 9](#__RefHeading___Toc222915944)

[1.1. Область действия 9](#__RefHeading___Toc222915945)

[1.2. Термины и определения 9](#__RefHeading___Toc222915946)

[2. Концепция обеспечения ИБ 15](#__RefHeading___Toc222915947)

[2.1. Цели и задачи обеспечения ИБ 15](#__RefHeading___Toc222915948)

[2.2. Стратегия обеспечения ИБ 15](#__RefHeading___Toc222915949)

[2.3. Законодательная основа обеспечения ИБ 17](#__RefHeading___Toc222915950)

[2.4. Основные понятия 18](#__RefHeading___Toc222915951)

[3. Характеристика объекта защиты 22](#__RefHeading___Toc222915952)

[3.1. Модель угроз безопасности 22](#__RefHeading___Toc222915953)

[3.2. Модель нарушителя 31](#__RefHeading___Toc222915954)

[4. Аспекты обеспечения Информационной Безопасности 37](#__RefHeading___Toc222915955)

[4.1. Политика Информационной Безопасности 37](#__RefHeading___Toc222915956)

[4.2. Организационные аспекты обеспечения ИБ 38](#__RefHeading___Toc222915957)

[4.3. Управление активами 42](#__RefHeading___Toc222915958)

[4.4. Безопасность, связанная с персоналом 45](#__RefHeading___Toc222915959)

[4.5. Физическая безопасность 48](#__RefHeading___Toc222915960)

[4.6. Обеспечение ИБ при эксплуатации 51](#__RefHeading___Toc222915961)

[4.7. Контроль доступа 63](#__RefHeading___Toc222915962)

[4.8. Приобретение, разработка и поддержка систем 73](#__RefHeading___Toc222915963)

[4.9. Управление инцидентами 78](#__RefHeading___Toc222915964)

[4.10. Обеспечение непрерывности бизнеса 81](#__RefHeading___Toc222915965)

[4.11. Соответствие требованиям 83](#__RefHeading___Toc222915966)

[4.12. Обеспечение ИБ банковских платежных технологических процессов 85](#__RefHeading___Toc222915967)

[4.13. Обеспечение ИБ банковских информационных технологических процессов 88](#__RefHeading___Toc222915968)

[4.14. Обеспечение информационной безопасности автоматизированных банковских систем на стадиях жизненного цикла 90](#__RefHeading___Toc222915969)

[5. Порядок организации работ по Информационной Безопасности 94](#__RefHeading___Toc222915970)

[6. Нормативные ссылки 95](#__RefHeading___Toc222915971)

Назначение документа

Документ "Политика информационной безопасности ОАО АКБ "Унивбанк" определяет основные положения внутренней политики организации в области информационной безопасности. Документ определяет цели и задачи Банка в области ИБ, концептуальные подходы и основные принципы построения системы управления информационной безопасностью (СУИБ) Банка и требования к ее реализации.

Область действия

Положения настоящей Политики ИБ распространяются на все офисы ОАО АКБ "Унивбанк".

Термины и определения

***Автоматизированная банковская система*** –система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая банковскую информационную технологию.

***Авторизация*** – предоставление прав, гарантирующих доступ к ресурсам в соответствии с правами на доступ.

***Активы банка*** – все, что имеет ценность для банка: банковские ресурсы (финансовые, вычислительные, телекоммуникационные), виды банковской информации (платежная, финансово-аналитическая, служебная, управляющая), банковские процессы (банковские платежные технологические процессы, процессы жизненного цикла автоматизированных банковских систем), банковские продукты и услуги, предоставляемые клиентам.

***Аудит информационной безопасности организации*** –систематический, независимый от объекта аудита и документированный процесс получения свидетельств аудита и объективной их оценки с целью установления степени выполнения в организации установленных требований по обеспечению информационной безопасности.

***Аутентификация*** – проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

***Аутентичность информации*** – обеспечение полноты и точности информации при ее санкционированных изменениях.

***Банковский* *технологический процесс*** – технологический процесс, содержащий операции по изменению и (или) определению состояния банковской информации, используемой при функционировании или необходимой для реализации банковских услуг.

***Банковский информационный технологический процесс*** –часть банковского технологического процесса, содержащая операции над неплатежной информацией, необходимой для функционирования Банка.

***Банковский платежный технологический процесс*** –часть банковского технологического процесса, содержащая расчетные, учетные, кассовые и иные банковские операции над платежной информацией, связанные с перемещением денежных средств с одного счета на другой, открытием (закрытием) счетов или контролем над данными операциями.

***Допустимый риск*** – риск, который в данной ситуации считается приемлемым для организации.

***Доступность*** – свойство информации, ее носителей и технологий обработки, при котором обеспечивается санкционированный доступ к ней и надежность предоставления требуемой информации, или же свойство сервиса или ресурса, при котором обеспечивается выполнение установленных функций.

***Защита информации*** – деятельность, направленная на обеспечение конфиденциальности, целостности и доступности информации, а также обеспечение таких ее характеристик, как достоверность, идентифицируемость, неотказуемость и надежность.

***Защитная мера*** – мера, используемая для снижения риска.

***Злоумышленник*** - нарушитель, действующий намеренно из корыстных, идейных или иных побуждений.

***Информационная безопасность информационной системы (ИС)*** – характеристика состояния ИС, определяемая защищенностью обрабатываемой информации и способностью ИС к выполнению установленных функций без неприемлемого ущерба.

***Информационная технология*** – приемы, способы и методы применения средств вычислительной техники при выполнении функций хранения, обработки, передачи и использования данных.

***Информационный процесс*** – процесс создания, сбора, обработки, накопления, хранения, поиска, распространения и использования информации.

***Информационная система* (ИС)** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

***Инцидент ИБ*** – событие, которое может нанести ущерб организации.

***Конфиденциальность*** – свойство информации, характеризующее невозможность получения доступа или ознакомления с ней со стороны неуполномоченных на это лиц, субъектов или процессов.

***Модель нарушителя*** – формализованное описание возможного нарушителя с указанием его характеристик.

***Модель угроз*** – формализованное описание способов реализации угроз.

***Модель PDCA*** – модель Plan – Do – Check – Act, определяющая четыре этапа, которые должны циклически выполняться для процессов СУИБ.

***Мониторинг событий ИБ*** – постоянный контроль и действия по наблюдению, получению, хранению, распознаванию и анализу информации, связанной с событиями ИБ, выявлению фактов нарушения установленных требований ИБ и объектов/субъектов, с которыми связаны эти нарушения.

***Нарушитель*** - это лицо, которое предприняло попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

***Неотказуемость при работе с информацией*** - невозможность субъекта отказаться от совершенных в отношении информации действий.

***Обеспечение информационной безопасности ИС*** – деятельность, направленная на достижение требуемого уровня информационной безопасности.

***Обработка информации*** – совокупность операций сбора, накопления, ввода, вывода, приема, передачи, записи, хранения, регистрации, уничтожения, преобразования, отображения, осуществляемых над информацией.

***Обработка риска*** – процесс выбора вариантов модификации риска.

***Остаточный риск*** – риск, оставшийся после обработки риска.

***Отслеживаемость при работе с информацией*** – возможность восстановить сценарий нарушения (или попытки нарушения) информационной безопасности в отношении информационного актива.

***Оценка риска*** – общий процесс анализа и оценивания риска.

***Оценка соответствия информационной безопасности организации, установленным требованиям*** –деятельность, связанная с прямым или косвенным определением того, что выполняются или не выполняются соответствующие требования информационной безопасности в организации.

***Политика информационной безопасности организации*** –одно или несколько правил, процедур, практических приемов и руководящих принципов в области информационной безопасности, которыми руководствуется организация в своей деятельности.

***Процедура безопасной регистрации в системе*** – процедура регистрации, минимизирующая возможность несанкционированного доступа к системе и выдающая минимальное количество информации о ней.

***Риск*** – неопределенность, предполагающая возможность потерь.

***Свидетельство аудита*** –записи, изложение фактов или другой информации, связанной с критериями аудита информационной безопасности, которые могут быть проверены.

***Система управления информационной безопасностью*** (СУИБ) – часть общей системы менеджмента организации банка, основывающаяся на подходе бизнес-риска, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения информационной безопасности банка организации [ISO/IEC IS 27001].

***Система защиты информации ИС*** (СЗИ) – совокупность технических, программных и программно-технических средств защиты информации и средств контроля эффективности защиты информации.

***Средство защиты информации*** – техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации.

***Субъект информационных отношений*** –собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения — субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения указанными объектами; владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения — субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных Законом;   
пользователь (потребитель) информации - субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

***Угроза ИБ*** – потенциальная возможность возникновения инцидента ИБ.

***Управление рисками*** – общий процесс оценки рисков и их обработки.

***Ущерб*** – оценка значимости негативных последствий для организации, которые будут иметь место в результате возникновения инцидентов ИБ.

***Уязвимость*** – фактор, способствующий реализации угрозы.

***Целостность*** – свойство информации, при котором обеспечивается достижение целей ее функционального применения в системе.

***Электронная коммерция*** – заключение путем обмена электронными документами следующих сделок, предусмотренных ГК РФ (но не ограничиваясь ими): купля-продажа, поставка, возмездное оказание услуг, перевозка, заем и кредит, финансирование под уступку денежного требования, банковский вклад, банковский счет, расчеты, хранение, страхование, поручение, комиссия, агентирование, доверительное управление имуществом, коммерческая концессия, а также приобретение и осуществление с использованием электронных средств иных прав и обязанностей в сфере предпринимательской деятельности.

***Электронный документ*** – информация, формируемая, отправляемая, получаемая или хранимая с помощью электронных средств связи в связи с совершением сделок в сфере электронной торговли.

Концепция обеспечения ИБ

Цели и задачи обеспечения ИБ

Основными целями Банка в области обеспечения ИБ являются:

1. Защита информации во всех формах ее представления – обеспечение конфиденциальности, целостности и доступности.
2. Обеспечение функционирования ИС в соответствии с установленными требованиями.
3. Соответствие требованиям законодательных и нормативных документов.
4. Отсутствие неприемлемого ущерба.
5. Обеспечение неотказуемости, отслеживаемости, аутентичности при работе с информацией.

Основными задачами Банка в области обеспечения ИБ являются:

1. Предупреждение реализации угроз ИБ.
2. Снижение ущерба для организации при возможной реализации угроз ИБ (возникновении инцидентов ИБ).
3. Обеспечение доверия (предоставление обоснованных гарантий достижения целей обеспечения ИБ).
4. Оптимизация затрат на обеспечение ИБ.

Выполнение этих задач базируется на использовании процесса управления рисками информационной безопасности.

Стратегия обеспечения ИБ

Эффективное решение задач обеспечения ИБ строится на основе подхода, предусматривающего создание системы управления информационной безопасностью (СУИБ).

Организация СУИБ основывается на следующих принципах:

1. Комплексность – одновременное применение административных, физических и технических мер.
2. Системность – создание системы обеспечения ИБ, включающей совокупность защитных мер и персонал, участвующий в обеспечении ИБ.
3. Управление рисками – оценка рисков возможных инцидентов ИБ и принятие решений по их обработке на основании установленных критериев риска.
4. Мониторинг – оперативное обнаружение инцидентов ИБ и реагирование на них.
5. Совершенствование – оценка эффективности функционирования СУИБ с целью принятия корректирующих и предупреждающих действий и определения возможных улучшений.
6. Адекватность защитных мер – эффективность защитных мер и их стоимость должна быть адекватной имеющимся рискам.

Функционирование СУИБ строится на основе применения PDCA-модели и предполагает использование как активного, так и проактивного управления. Основной задачей активного управления является принятие соответствующих корректирующих и предупреждающих мер по результатам инцидентов ИБ и устранение выявленных несоответствий СУИБ установленным требованиям. Проактивное управление строится на основе управления рисками и направлено на устранение неприемлемых рисков, связанных с возможными инцидентами ИБ. Требуемый уровень ИБ определяется критерием приемлемости рисков.

Реализация СУИБ использует принципы, изложенные в стандарте ISO 27001, а именно:

1. Организация при безусловной поддержке руководства должна создать, внедрить, эксплуатировать, постоянно контролировать, анализировать, поддерживать в рабочем состоянии и улучшать СУИБ в контексте целостной деловой деятельности организации и рисков, с которыми она сталкивается. Руководство организации должно выделять необходимые ресурсы для поддержания СУИБ в рабочем состоянии. Данный процесс основан на модели PDCA.
2. Организация через запланированные интервалы времени должна проводить аудит и самооценку СУИБ.
3. Руководство организации через запланированные интервалы времени (по крайней мере, один раз в год) должно анализировать состояние СУИБ. Такой анализ должен включать в себя оценивание возможностей для улучшения и потребности в изменениях СУИБ.
4. Организация должна постоянно улучшать СУИБ.

Законодательная основа обеспечения ИБ

Законодательную основу обеспечения ИБ Банка составляют следующие документы:

1. Федеральный закон "О безопасности" от 05.03.92 №2446-1.
2. Федеральный закон "О государственной тайне" от 21.07.93 №5485-1.
3. Федеральный закон "Об информации, информатизации и защите информации" от 20.02.95 №24-ФЗ.
4. Федеральный закон "О лицензировании отдельных видов деятельности" от 08.08.01 № 128-Ф3.
5. Федеральный закон "Об участии в международном информационном обмене" от 05.06.96 года №85-ФЗ.
6. Федеральный закон "Об электронной цифровой подписи" от 10.01.02 г. № 1-ФЗ.
7. Федеральный закон "Об экспортном контроле" от 18.07.99 г. № 183 ФЗ.
8. Федеральный закон "О банках и банковской деятельности" (в редакции от 03.02.96 г. № 17-ФЗ).
9. Федеральный закон "О Центральном банке Российской Федерации (Банке России)" от 10.07.02 года № 86-ФЗ.
10. Требования и рекомендации ЦБ РФ.

Основные понятия

Основные понятия используемой модели обеспечения ИБ включают активы, угрозы, уязвимости, ущерб, защитные меры и риски.

Активы

К активам относятся:

1. Бизнес-процессы.
2. Информация и сервисы.
3. Компоненты и ресурсы ИС.
4. Персонал.

Активы являются сущностями, важными для организации. Воздействие на активы инцидентов ИБ приводит к негативным последствиям для организации, характеризуемым ущербом.

Обеспечение защиты активов является одной из главных задач обеспечения ИБ организации. Защита активов реализуется путем применения защитных мер, направленных на предотвращение угроз, уменьшение вероятности их реализации или снижение ущерба при их реализации.

Угрозы

Под угрозой ИБ понимается потенциальная возможность возникновения инцидента ИБ. Реализация угрозы означает возникновение нежелательного инцидента, который, воздействуя на активы, может путем нарушения их ценных свойств причинить ущерб организации. Угрозы могут происходить от различных источников и могут быть случайными или намеренно созданными. Источники угроз делятся на внутренние и внешние, естественные и связанные с людьми и т.д. Для своей реализации угроза требует наличия уязвимости.

Рассматриваются следующие категории инцидентов ИБ:

1. Утечка информации.
2. Модификация.
3. Недоступность.
4. Уничтожение.

Каждая из категорий детализируется для более точного определения негативных последствий и ущерба ("Таблица1.").

Таблица1.

Классификация инцидентов ИБ

| **Инцидент** | **Детализация** |
| --- | --- |
| **Утечка информации** | Информация становится доступной сотрудникам, неуполномоченным на получение доступа или ознакомление с ней |
| Информация становится доступной незаинтересованным внешним сторонам, неуполномоченным на получение доступа или ознакомление с ней |
| Информация становится доступной заинтересованным внешним сторонам, неуполномоченным на получение доступа или ознакомление с ней |
| **Модификация** | Случайная незначительная модификация |
| Случайная значительная модификация |
| Предумышленная незначительная модификация |
| Предумышленная значительная модификация |
| **Недоступность** | Время недоступности до нескольких минут |
| Время недоступности от нескольких минут до нескольких часов |
| Время недоступности больше нескольких часов |
| **Уничтожение** | Полное |
| С момента последнего резервного копирования |

При оценке ущерба для организации рассматриваются негативные последствия, к которым может привести инцидент ИБ.

Уязвимости

Под уязвимостью понимается фактор, способствующий реализации угрозы. Уязвимостями могут быть слабые места в компонентах ИС, ее архитектуре, недостатки организационных защитных мер и процессов СУИБ.

Сочетание угрозы и уязвимости может формулироваться в виде сценария реализации угрозы.

Ущерб

Значимость последствий для организации от воздействий инцидентов ИБ на активы выражается через ущерб. Каждое последствие относится к той или иной категории. Выделяются следующие категории:

1. Финансы.
2. Репутация/доверие клиентов.
3. Штрафы/юридические/административные взыскания.
4. Дезорганизация.
5. Другие.

Защитные меры

В качестве защитных мер применяются административные, физические или технические меры, предназначенные для предупреждения реализации угроз, уменьшения уязвимостей, снижения ущерба, обнаружения инцидентов. Требуемый уровень ИБ обеспечивается сочетанием различных защитных мер.

Ограничения являются важным фактором, который нужно учитывать при выборе защитных мер. Основными видами ограничений являются:

1. Финансовые.
2. Персонала.
3. Времени.
4. Правовые.
5. Технические.

Риски

Риском называется функция двух аргументов: вероятности возникновения инцидента ИБ и ущерба от его последствий. Риск является оценкой опасности потенциально возможного инцидента ИБ. Риск является важнейшим понятием методологии управления рисками.

Характеристика объекта защиты

Объектом защиты являются информационные активы Банка.

Информационные активы Банка, подлежащие защите, отражаются в Перечне информационных активов Банка. Критичность информационного актива определяется на основе оценки трех свойств актива: конфиденциальности, целостности и доступности.

Характерными особенностями Банка являются большое количество данных, хранящихся и обрабатывающихся в различных системах, и необходимость поддерживать работу большого количества клиентов и пользователей.

Модель угроз безопасности

Основными источниками угроз ИБ являются:

* неблагоприятные события природного, техногенного и социального характера;
* террористы и криминальные элементы;
* зависимость от поставщиков/провайдеров/партнеров/клиентов;
* сбои, отказы, разрушения/повреждения программных и технических средств;
* работники организации БС РФ, реализующие угрозы ИБ с использованием легально предоставленных им прав и полномочий (внутренние нарушители ИБ);
* работники организации БС РФ, реализующие угрозы ИБ вне легально предоставленных им прав и полномочий, а также субъекты, не являющиеся работниками организации БС РФ, но осуществляющие попытки НСД и НРД (внешние нарушители ИБ);
* несоответствие требованиям надзорных и регулирующих органов, действующему законодательству.

Наиболее актуальные источники угроз на физическом уровне, уровне сетевого оборудования и уровне сетевых приложений:

* внешние нарушители ИБ: лица, разрабатывающие/распространяющие вирусы и другие вредоносные программные коды; лица, организующие DoS, DDoS и иные виды атак; лица, осуществляющие попытки НСД и НРД;
* внутренние нарушители ИБ: персонал, имеющий права доступа к аппаратному оборудованию, в том числе сетевому, администраторы серверов, сетевых приложений и т.п.;
* комбинированные источники угроз: внешние и внутренние нарушители ИБ, действующие совместно и (или) согласованно;
* сбои, отказы, разрушения/повреждения программных и технических средств

Наиболее актуальные источники угроз на уровнях операционных систем, систем управления базами данных, банковских технологических процессов:

* внутренние нарушители ИБ: администраторы ОС, администраторы СУБД, пользователи банковских приложений и технологий, администраторы ИБ и т.д.;
* комбинированные источники угроз: внешние и внутренние нарушители ИБ, действующие в сговоре

Наиболее актуальные источники угроз на уровне бизнес-процессов:

* внутренние нарушители ИБ: авторизованные пользователи и операторы АБС, представители менеджмента организации и пр.;
* комбинированные источники угроз: внешние нарушители ИБ (например, конкуренты) и внутренние, действующие в сговоре;
* несоответствие требованиям надзорных и регулирующих органов, действующему законодательству

Основные сценарии реализации угроз безопасности информации Банка приведены в Таблице 2.

Таблица 2.

Основные сценарии реализации угроз

|  |  |
| --- | --- |
| **Источник угрозы ИБ** | **Описание** |
| **Класс 1. Источники угроз ИБ, связанные с неблагоприятными событиями природного, техногенного и социального характера** | | |
| Пожар | Неконтролируемый процесс горения, сопровождающийся уничтожением материальных ценностей и создающий опасность для жизни людей. Возможные причины:  поджог, самовозгорание, природное явление |
| Природные катастрофы, чрезвычайные ситуации и стихийные бедствия | Природные явления разрушительного характера (наводнения, землетрясения, извержения вулканов, ураганы, смерчи, тайфуны, цунами и т.д.) |
| Техногенные катастрофы | Разрушительный процесс, развивающийся в результате нарушения нормального взаимодействия технологических объектов между собой или с компонентами окружающей природной среды, приводящий к гибели людей, разрушению и повреждению объектов экономики и компонентов окружающей природной среды |
| Нарушение внутриклиматических условий | Негативное изменение климатических условий в помещениях, где расположены технические средства и/или находится персонал: значительные изменения температуры и  влажности, повышение содержания углекислого газа, пыли и т.п. Возможные последствия: сбои, отказы и аварии технических средств, снижение работоспособности и нанесение  ущерба здоровью персонала, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов) |
| Нарушение электропитания | Нарушение или снижение качества электропитания. Возможные причины: техногенная катастрофа, стихийное бедствие, природное явление, террористический акт, пожар и т.п. Возможные последствия: сбои и отказы технических средств |
| Нарушение функционирования систем жизнеобеспечения | Сбои и аварии в системах водоснабжения, канализации, отопления |
| Угроза здоровью персонала | Угроза здоровью персонала в результате радиационных, биологических, механических, термических, химических и иных воздействий со стороны окружающей среды, объектов  инженерной инфраструктуры, технических средств, пищевые отравления, производственный травматизм. Возможные причины: техногенные или природные катастрофы, аварии объектов инженерной инфраструктуры, неисправность оборудования, несоблюдение правил техники безопасности и охраны труда, санитарных правил и т.д. Возможные последствия: нехватка персонала, денежные выплаты, судебные разбирательства |
| **Kласс 2. Источники угроз ИБ, связанные с деятельностью террористов и лиц, совершающих преступления и правонарушения** | | |
| Нарушения общественного порядка, вандализм, массовые беспорядки, политическая нестабильность | Уничтожение или повреждение имущества организации БС РФ |
| Террористические действия | Совершение взрыва, поджога или иных действий, устрашающих население и создающих опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, в целях воздействия на принятие решения организацией БС РФ, а также угроза совершения указанных действий в тех же целях |
| Промышленный шпионаж | Передача, собирание, похищение или хранение информационных активов организации  БС РФ для использования их в ущерб организации БС РФ |
| Запугивание и шантаж | Принуждение персонала организации БС РФ к осуществлению несанкционированных действий, заключающееся в угрозе разоблачения, физической расправы или расправы с близкими |
| Социальный инжиниринг | Умышленные действия сторонних лиц, преследующих мошеннические цели, реализуемые посредством обмана, введения в заблуждение работников организации БС РФ. Возможные последствия: ошибки работников, нарушение свойств, утрата информационных активов, нарушение непрерывности процессов, снижение качества информационных услуг (сервисов) |
| **Класс 3. Источники угроз ИБ, связанные с деятельностью поставщиков/провайдеров/партнеров** | | |
| Зависимость от партнеров/клиентов | Зависимость от партнеров заставляет организацию полагаться на их информационную безопасность, организация должна быть уверена, что партнер сможет обеспечить  должный уровень безопасности либо учитывать данный источник угроз |
| Ошибки, допущенные при заключении контрактов с провайдерами внешних услуг | Неточности и неопределенности в договоре с провайдером внешних услуг, которые могут создавать проблемы в работе заказчика |
| Нарушения договорных обязательств сторонними  (третьими) лицами | Невыполнение со стороны третьих лиц взятых на себя обязательств по качеству, составу, содержанию и/или порядку оказания услуг, поставки продукции и т.д. Например, невыполнение требований разработчиками, поставщиками программнотехнических средств и услуг или внешними пользователями |
| Ошибки в обеспечении безопасности информационных систем на стадиях  жизненного цикла | Ошибки в обеспечении безопасности при разработке, эксплуатации, сопровождении и выводе из эксплуатации информационных систем |
| Разработка и использование некачественной документации | Некачественное выполнение документированного описания технологических процессов обработки, хранения, передачи данных, руководств для персонала, участвующего в этих технологических процессах, а также описания средств обеспечения ИБ и руководств по их использованию |
| Использование программных средств и информации без гарантии источника | Использование в информационной системе организации непроверенных данных или нелицензионного программного обеспечения |
| **Класс 4. Источники угроз ИБ, связанные со сбоями, отказами, разрушениями/повреждениями программных и технических средств** | | |
| Превышение допустимой нагрузки | Неумышленное превышение допустимой нагрузки на вычислительные, сетевые ресурсы системы. Выполнение работниками объема операций большего, чем это допускается психофизиологическими нормами. Возможные причины: малая вычислительная и/или пропускная мощность, неправильная организация бизнес процессов.  Возможные последствия: сбои и отказы технических средств, нарушение доступности технических средств, ошибки персонала, нанесение вреда здоровью |
| Разрушение/повреждение, аварии технических средств и каналов связи | Физическое разрушение/повреждение технических средств (канала связи) или определенное сочетание отказов его элементов, приводящее к нарушениям функционирования, сопряженным с особо значительными техническими потерями, делающее невозможным функционирование технического средства (канала связи)  в целом в течение значительного периода времени. Возможные причины: действие внешних (физический несанкционированный доступ, террористический акт, техногенная катастрофа, стихийное бедствие, природное явление, массовые беспорядки) и/или внутренних (значительные отказы элементов технических средств) факторов. Возможные последствия: нарушение свойств информационных активов, их утрата, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов) |
| Сбои и отказы программных средств | Нарушение работоспособности программных средств. Возможные причины: недопустимое изменение параметров или свойств программных средств под влиянием внутренних процессов (ошибок) и/или внешних воздействий со стороны вредоносных программ, оператора и технических средств. Возможные последствия: нарушение свойств информационных активов, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов) |
| Сбои и отказы технических средств и каналов связи | Прерывание работоспособности технических средств или невозможность выполнения ими своих функций в заранее установленных границах. Возможные причины: недопустимое изменение характеристик технических средств под влиянием внутренних процессов, сложность технических средств, нехватка персонала, недостаточное техническое обслуживание. Возможные последствия: сбои, отказы программных средств, аварии систем, нарушение доступности информационных активов, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов) |
| Нарушения функциональности криптографической системы | Случайное или намеренное неправильное управление криптографическими ключами, криптографическими протоколами и алгоритмами, программноаппаратными средствами систем криптографической защиты информации, приводящее к потере конфиденциальности, целостности и доступности информации, нарушению неотказуемости приема передачи информации, блокировке функционирования платежных и информационных систем организации БС РФ |
| Нарушения функциональности архивной системы | Нарушение конфиденциальности и целостности архивных данных и/или не предоставление услуг архивной системой (нарушение доступности) вследствие случайных ошибок  пользователей или неправильного управления архивной системой, а также вследствие физических воздействий на компоненты архивной системы |
| **Класс 5. Источники угроз ИБ, связанные с деятельностью внутренних нарушителей ИБ** | | |
| Недобросовестное исполнение обязанностей | Сознательное неисполнение работниками определенных обязанностей или небрежное их исполнение |
| Халатность | Неисполнение или ненадлежащее исполнение должностным лицом своих обязанностей вследствие недобросовестного или небрежного отношения к службе |
| Причинение имущественного ущерба | Умышленное нанесение персоналом вреда информационным активам. В первую очередь вредительство может быть направлено на технические и программные средства, а также на информационные активы. Возможные последствия: ущерб, вызванный нарушением свойств активов, включая их разрушение и уничтожение |
| Ошибка персонала | Любые не соответствующие установленному регламенту или сложившимся практикам действия персонала, совершаемые без злого умысла. Возможные причины: недостаточно четко определенные обязанности, халатность, недостаточное обучение или квалификация персонала. Возникновению ошибок способствуют отсутствие дисциплинарного процесса и документирования процессов, предоставление избыточных полномочий, умышленное использование методов социального инжиниринга по отношению к персоналу. Возможные последствия: нарушение конфиденциальности и целостности информации, утрата информационных активов, нарушение непрерывности выполнения процессов,  снижение качества информационных услуг (сервисов), сбои и отказы технических и программных средств |
| Хищение | Совершенное с корыстной целью противоправное безвозмездное изъятие и/или обращение имущества организации БС РФ, причинившие ущерб собственнику или иному владельцу этого имущества |
| Выполнение вредоносных программ | Внедрение в систему и выполнение вредоносных программ: программных закладок, “троянских коней”, программных “вирусов” и “червей” и т.п. Возможные причины: беспечность, халатность, низкая квалификация персонала (пользователей), наличие  уязвимостей используемых программных средств. Возможные последствия:  несанкционированный доступ к информационным активам, нарушение их свойств, сбои, отказы и уничтожение программных средств, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов) |
| Использование информационных активов не по назначению | Умышленное использование информационных активов организации в целях, отличных от целей организации. Возможные причины: отсутствие контроля персонала. Возможные последствия: нехватка вычислительных, сетевых или людских ресурсов, прямой ущерб организации |
| Нарушения персоналом организационных мер по обеспечению ИБ | Несоблюдение персоналом требований внутренних документов, регламентирующих деятельность по ИБ |
| Ошибки кадровой работы | Ошибки кадровой работы заключаются в приеме на работу неквалифицированных сотрудников, увольнении/перемещении сотрудников без проведения сопутствующих процедур по обеспечению ИБ, не проведении или нерегулярном проведении тренингов и проверок персонала |
| **Класс 6. Источники угроз ИБ, связанные с деятельностью внешних нарушителей ИБ** | | |
| Действия неавторизованного субъекта | Умышленные действия со стороны субъекта из внешней по отношению к области обеспечения ИБ среды. Возможные последствия: разрушение и уничтожение технических и программных средств, внедрение и выполнение вредоносных программ, нарушение свойств, утрата информационных активов и сервисов |
| Ложное сообщение об угрозе | Ложное сообщение об угрозе, такой как: пожар, террористический акт, техногенная катастрофа, гражданские беспорядки и т.д. Возможные последствия: нарушение свойств информационных активов, их утрата, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов) |
| Неконтролируемое уничтожение информационного актива | Неумышленное уничтожение информационных активов. Возможные причины: сбои оборудования, природные факторы и техногенные катастрофы. Возможные последствия:  прямой ущерб организации |
| Неконтролируемая модификация информационного актива | Неумышленное изменение информационных активов. Возможные причины: сбои оборудования, природные факторы и техногенные катастрофы. Возможные последствия:  нарушение непрерывности выполнения процессов, прямой ущерб организации |
| Несанкционированный логический доступ | Несанкционированный логический доступ неавторизованных субъектов к компонентам подразделения и информационным активам. Возможные причины: компрометация пароля, предоставление пользователям/администраторам избыточных прав доступа, недостатки (отсутствие) механизмов аутентификации пользователей и администраторов, ошибки администрирования, оставление без присмотра программнотехнических средств. Одним  из путей получения несанкционированного доступа к системе является умышленное внедрение вредоносных программ с целью хищения пароля для входа в систему или получения прав доступа. Возможные последствия: нарушение свойств информационных активов, сбои, отказы и аварии программных и технических средств, нарушение непрерывности процессов и/или снижение качества информационных услуг (сервисов) |
| Несанкционированный физический доступ | Физический несанкционированный доступ неавторизованных лиц в контролируемую зону расположения технических средств и/или информационных активов. Возможные причины:  может осуществляться путем обхода средств контроля физического доступа или использования утраченных/похищенных средств обеспечения доступа. Возможные последствия: разрушение и уничтожение технических и программных средств, нарушение конфиденциальности, целостности, доступности информационных активов, нарушение непрерывности процессов и/или снижение качества информационных услуг (сервисов) |
| **Класс 7. Источники угроз ИБ, связанные с несоответствием требованиям надзорных и регулирующих органов, действующему законодательству** | | |
| Несоответствие внутренних документов действующему законодательству | Несоответствие деятельности может привести к административным и уголовным санкциям со стороны судебных, надзорных и регулирующих органов в отношении должностных лиц  подразделения, вызвать остановку отдельных видов деятельности |
| Изменчивость и несогласованность требований надзорных  и регулирующих органов, вышестоящих инстанций | Непостоянство, различия и коллизии в содержании требований и/или порядке их выполнения способны дезорганизовать деятельность подразделения или его отдельных служб, снизить ее эффективность и качество, а при определенных обстоятельствах — затруднить ее осуществление. Способствует “размыванию” или пересечению зон ответственности исполнителей и служб, манипуляции со стороны ответственных лиц и служб своими правами и обязанностями в ущерб общей деятельности. Приводит к перераспределению ресурсов в пользу той деятельности (зачастую не основной),  за несоблюдение требований к которой наказание наиболее ощутимо для организации (должностного лица) |

Модель нарушителя

С учетом разделения нарушителей информационной безопасности на внешних, внутренних и комбинированных в качестве возможных потенциальных нарушителей информационной безопасности могут выступать:

Внешние нарушители информационной безопасности:

* клиенты Банка;
* лица, случайно или намеренно, получившие доступ к информационным

активам Банка через внешние телекоммуникационные каналы связи;

* конкурирующие кредитные организации;
* программисты-разработчики программных компонент, не являющиеся

сотрудниками Банка;

* компании, обеспечивающие поставку и ремонт компьютерной техники;
* спецслужбы и представители силовых ведомств, имеющие возможность применять специальные средства и способы атак на информационные активы Банка;

Внутренние нарушители информационной безопасности:

* сотрудники Банка, имеющие легальный доступ к ресурсам автоматизированной банковской системы;
* сотрудники Банка, осуществляющие доступ к информационным активам с использованием технологии удаленного доступа;
* сотрудники Банка, имеющие полномочия системного администратора или администратора информационной безопасности;
* программисты-разработчики программных компонент, являющиеся сотрудниками Банка.

Комбинированные нарушители информационной безопасности – сотрудники Банка, действующие в сговоре с внешними нарушителями информационной безопасности.

В зависимости от цели, квалификации, технического оснащения и прав доступа к информационным системам Банка нарушители информационной безопасности могут реализовывать атаки на уровне сетевого оборудования, операционных систем, систем управления базами данных, сетевых приложений и сервисов, банковских приложений и сервисов, используя следующие способы несанкционированного доступа:

* внедрение вредоносного программного обеспечения;
* кража носителей информационных активов;
* кража технических средств обработки информационных активов;
* несанкционированное повышение привилегий сотрудника Банка в системе;
* несанкционированные действия сотрудников Банка в системе;
* физическое подключение к каналу связи с целью перехвата информации;
* внесение недекларированных возможностей и/или программных закладок;
* внедрение ложных сетевых сервисов;
* подмена доверенного объекта;
* навязывание ложного сетевого маршрута;
* удаленный запуск приложений и т.д.

Все способы несанкционированного доступа к активам могут быть направлены на преднамеренное или случайное копирование, модификацию, удаление, передачу по каналам связи и/или передачу на материальных носителях, с целью нарушения конфиденциальности, целостности и/или доступности актива.

СУИБ Банка должна строиться исходя из предположений о следующих возможных типах нарушителей в системе (с учетом категории лиц, мотивации, квалификации, наличия специальных средств и др.):

1. Некомпетентный (невнимательный) пользователь - сотрудник Банка (или подразделения другой организации, являющийся легальным пользователем информационной системы Банка), который может предпринимать попытки выполнения запрещенных действий, доступа к защищаемым ресурсам информационной системы с превышением своих полномочий, ввода некорректных данных, нарушения правил и регламентов работы с информацией и т.п., действуя по ошибке, некомпетентности или халатности без злого умысла и использующий при этом только штатные (предоставленные) средства.
2. Любитель - сотрудник Банка (или подразделения другого организации, являющийся зарегистрированным пользователем информационной системы Банка), пытающийся нарушить систему защиты без корыстных целей или злого умысла или для самоутверждения. Для преодоления системы защиты и совершения запрещенных действий он может использовать различные методы получения дополнительных полномочий доступа к ресурсам, недостатки в построении системы защиты и доступные ему штатные средства (несанкционированные действия посредством превышения своих полномочий на использование разрешенных средств). Помимо этого он может пытаться использовать дополнительно нештатные инструментальные и технологические программные средства, самостоятельно разработанные программы или стандартные дополнительные технические средства.
3. Внутренний злоумышленник - сотрудник Банка (или подразделения другого ведомства, зарегистрированный как пользователь системы), действующий целенаправленно из корыстных интересов или мести за нанесенную обиду, возможно в сговоре с лицами, не являющимися сотрудниками Банка. Он может использовать весь набор методов и средств взлома системы защиты, включая агентурные методы, пассивные средства (технические средства перехвата), методы и средства активного воздействия (модификация технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ), а также комбинации воздействий, как изнутри, так и извне Банка.
4. Внешний злоумышленник - постороннее лицо, действующее целенаправленно из корыстных интересов, мести или из любопытства, возможно в сговоре с другими лицами. Он может использовать весь набор методов и средств взлома системы защиты, включая агентурные методы, пассивные средства (технические средства перехвата), методы и средства активного воздействия (модификация технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ), а также комбинации воздействий, как изнутри, так и извне Банка.

Пользователи и обслуживающий персонал из числа сотрудников Банка имеют наиболее широкие возможности по осуществлению несанкционированных действий, вследствие наличия у них определенных полномочий по доступу к информационным ресурсам и хорошего знания технологии обработки информации и защитных мер. Действия этой группы лиц напрямую связано с нарушением действующих правил и инструкций.

Особую категорию составляют администраторы различных автоматизированных систем, имеющих практически неограниченный доступ к информационным ресурсам компонентов корпоративной информационной системы. Численность данной категории пользователей должна быть минимальной, а их действия должны находиться под обязательным контролем со стороны ПБоИБ.

Уволенные сотрудники могут использовать для достижения целей свои знания о технологии работы, защитных мерах и правах доступа. Полученные во время работы в Банке знания и опыт выделяют их среди других источников внешних угроз.

Криминальные структуры являются наиболее агрессивным источником внешних угроз. Для осуществления своих замыслов эти структуры могут идти на открытое нарушение закона и вовлекать в свою деятельность сотрудников Банка всеми доступными им силами и средствами.

Профессиональные хакеры имеют наиболее высокую техническую квалификацию и знания о слабостях программных средств, используемых в автоматизированных системах обработки информации. Они представляют наибольшую угрозу при взаимодействии с работающими или уволенными сотрудниками Банка и криминальными структурами.

Организации, занимающиеся разработкой, поставкой, ремонтом и обслуживанием оборудования или информационных систем, представляют внешнюю угрозу в силу того, что эпизодически имеют непосредственный доступ к информационным ресурсам. Конкурирующие организации, криминальные структуры и спецслужбы могут использовать эти организации для временного устройства на работу своих членов с целью доступа к ресурсам информационной системы Банка.

Принимаются следующие ограничения и предположения о характере действий возможных нарушителей:

1. Нарушитель скрывает свои несанкционированные действия от других сотрудников Банка.
2. Несанкционированные действия могут быть следствием ошибок пользователей, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, хранения и передачи информации.
3. В своей деятельности вероятный нарушитель может использовать любое имеющееся средство перехвата информации, воздействия на информацию и информационные системы, адекватные финансовые средства для подкупа персонала, шантаж и другие средства и методы для достижения стоящих перед ним целей.

Аспекты обеспечения Информационной Безопасности

Политика Информационной Безопасности

Разработка Политики Информационной Безопасности

Политика ИБ служит для описания целей и задач обеспечения ИБ Банка, стратегии и подходов к ее реализации, основных аспектов организации общего процесса обеспечения ИБ, а также определения совокупности требований в области ИБ, которыми руководствуется Банк в своей деятельности. Политика должна быть утверждена руководством и доведена до сведения всех сотрудников.

Помимо общекорпоративной политики ИБ должны быть разработаны следующие частные политики и документы:

1. Политика использования сети Интернет.
2. Политика использования средств антивирусной защиты.
3. Политика использования электронной почты.
4. Политика стандартизации рабочих мест.
5. Политика использования средств криптографической защиты информации.
6. План по непрерывности бизнеса.
7. План по восстановлению бизнеса.

Кроме того, должен быть документально определен перечень информации, относимой к коммерческой и служебной тайне, а также определена ответственность за разглашение этой информации.

Поддержка актуальности политики ИБ

Политика ИБ должна пересматриваться один раз в год или при необходимости. Изменения должны утверждаться руководством. Необходимо информировать сотрудников обо всех изменениях и обеспечить их доступ к наиболее актуальной версии документа.

Организационные аспекты обеспечения ИБ

Общие вопросы

Обязанности руководства в области обеспечения ИБ

Руководство Банка осознает важность обеспечения ИБ для Банка. Руководство обеспечивает создание необходимой организационной структуры, назначение обязанностей по обеспечению ИБ и выделение необходимых ресурсов.

Координация работ по обеспечению ИБ

Должна осуществляться координация работ в области обеспечения ИБ проводимых различными подразделениями Банка.

Для этого в Банке следует создать совет по информационной безопасности, возглавляемый Ответственным по ИБ Банка из числа руководителей высшего звена. Кроме того, в состав совета должны входить специалисты в области юриспруденции, управления персоналом, ИТ и ИБ.

Кроме того, создано подразделение Банка, ответственное за вопросы информационной безопасности (ПБоИБ), подотчетное высшему руководству Банка.

Распределение обязанностей

Все обязанности по обеспечению ИБ должны быть назначены исполнителям внутри существующей организационной структуры Банка.

Следует однозначно определить ответственность за отдельные активы и выполнение конкретных процессов в соответствии с требованиями ИБ.

Для распределения персональной ответственности в каждой конкретной области необходимо выполнить следующее:

1. Четко определить и описать активы и процессы, относящиеся к конкретным системам.
2. Назначить ответственных за каждый актив или процесс, и документировать их обязанности.
3. Четко определить и документировать процесс санкционирования предоставления доступа к активам и процессам.

Порядок введения новых средств обработки информации

Должна быть определена и внедрена процедура утверждения использования новых средств ИТ.

Для того, чтобы избежать возможных временных и финансовых затрат на внедрение средств защиты информации после приобретения новых средств обработки информации, не удовлетворяющих требованиям безопасности, введение новых средств обработки информации должно происходить в соответствии со следующими правилами:

1. Руководство Банка должно утвердить новые средства обработки информации для однозначного определения их назначения и способа применения.
2. Руководитель, ответственный за поддержку безопасности конкретной автоматизированной системы, должен одобрить эти средства и подтвердить соблюдение всех необходимых условий и требований безопасности.
3. Оборудование и программное обеспечение следует проверить на совместимость с другими компонентами системы.
4. В случае применения личных средств обработки информации необходимо произвести их проверку и получить санкцию руководства на их применение.

Соглашение о конфиденциальности

Следует разработать и регулярно пересматривать соглашение о конфиденциальности, устанавливающее требования по обеспечению конфиденциальности информации и включающее обязательства по ее неразглашению. Данное соглашение должно быть подписано всеми сотрудниками Банка.

Соглашение о конфиденциальности должно учитывать существующие нормативно-правовые требования.

Временные работники и сторонние пользователи также должны подписывать соглашение о неразглашении конфиденциальной информации перед тем, как они получат доступ к средствам обработки информации.

Соглашение о конфиденциальности следует пересматривать через определенные интервалы и в случае изменений, влияющих на требования к его разработке.

Контакты с уполномоченными организациями

Должен быть определен порядок обращения к представителям других организаций в случае необходимости (правоохранительные органы, пожарная охрана, аварийные службы и т.д.).

Контакты с другими организациями и тематическими форумами

Должны быть налажены каналы получения актуальной информации по вопросам ИБ через контакты с другими организациями, тематическими форумами, участие в конференциях и т.д.

Независимая оценка информационной безопасности

СУИБ Банка должна регулярно проверяться на предмет эффективности и адекватности, а также при существенных изменениях. Проверка должна проводиться независимой внешней стороной или внутренними аудиторами, не имеющими обязанностей по реализации СУИБ.

Результаты проведения независимой оценки, включая выводы о необходимости улучшений и/или изменений в политике и обеспечении ИБ, должны документироваться и представляться на рассмотрение руководству Банка.

Безопасность, связанная с доступом внешних пользователей

Выявление рисков, связанных с участием внешних сторон

Для принятия адекватных мер безопасности следует провести идентификацию, оценку и обработку рисков, связанных с предоставлением доступа внешним пользователям.

Доступ к информации и средствам ее обработки должен предоставляться сторонним организациям только после внедрения необходимых средств защиты и подписания договора, определяющего условия подключения или доступа.

Обеспечение ИБ при работе с клиентами

В зависимости от типа и объема предоставляемого доступа следует определить требования по обеспечению ИБ при работе с клиентами и при необходимости включить их в соответствующие договоры.

Соглашения со сторонними организациями

Аспекты обеспечения ИБ должны быть рассмотрены и соответствующие требования учтены в соглашениях со сторонними организациями во всех случаях, когда это необходимо.

Должны быть сформулированы требования к предоставлению доступа, обработке, управлению информацией Банка и процессами обработки информации сторонним организациям.

Управление активами

Ответственность за активы

Перечень активов

Все важные с точки зрения ИБ активы Банка должны быть идентифицированы. Перечни активов следует составить и пересматривать не реже одного раза в год, а также при изменении технологий, при выявлении новых рисков, изменении законодательства и т.д.

Следует четко описать каждый актив, согласовать и обозначить его владельца и категорию конфиденциальности, а также указать его местоположение.

Перечни всех активов должны разрабатываться при участии сотрудников структурных подразделений Банка.

Определение владельцев активов

Все идентифицированные активы Банка должны иметь определенного владельца, ответственного за их классификацию и определение прав доступа для всех субъектов.

Назначение ответственности за активы необходимо также для обеспечения и поддержки защиты активов, степень которой будет соразмерна их ценности и важности.

Обязанности по реализации средств защиты могут передаваться другим сотрудникам, но ответственность за обеспечение должной защиты остается за назначенным владельцем актива.

Обращение с активами

Должен быть определен, документирован и внедрен необходимый набор правил, регламентирующих обращение с активами.

Сотрудники Банка и сторонние пользователи должны быть ознакомлены с этими правилами.

Категорирование активов

Порядок категорирования активов

Для определения необходимости, приоритетов и степени защиты активов должен быть определен порядок их категорирования.

Активы следует категорировать с учетом их ценности, требований законодательства и важности для Банка. Следует разработать систему категорирования активов, которая поможет создать необходимый перечень уровней защиты и пояснить пользователям необходимость в особом обращении. Ценность актива определяется требованиями к нему по конфиденциальности, целостности и доступности.

За определение категории актива и периодическую ее переоценку ответственность несет его владелец.

В рамках выбранной области действия политики для каждого информационного актива должны указываться:

1. Дивизион, использующий в работе данный информационный актив.
2. Бизнес-услуга/процесс дивизиона, использующий данный информационный актив.
3. Подпроцесс дивизиона, использующий данный информационный актив.
4. Имя владельца бизнес-услуги (процесса).
5. Название подразделения, оказывающего бизнес-услугу.
6. Название информационной системы, используемой при работе с данным информационным активом.
7. Показатели конфиденциальности, целостности и доступности как требования к данному информационному активу.
8. Совокупная ценность (стоимость) информационного актива.

Когда программное обеспечение имеет собственную ценность, заключающуюся, например, в необходимости обеспечения конфиденциальности и целостности исходных текстов программ, представлении собой объекта интеллектуальной собственности или отнесении к категории коммерческой тайны ОАО АКБ "Унивбанк", его ценность (стоимость) должна оцениваться так же, как и для информационных активов.

**Таблица 3.**

**Классификация и категорирование активов**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№** | **Дивизион** | **Бизнес-услуга/процесс дивизиона** | **Подпроцесс дивизиона** | **Владелец бизнес -услуги** | **Подразделение, оказывающее бизнес-услугу** | **Поддерживается информационными системами** | **Владелец информационной системы** | **Используемый информационный актив** | **Требования к информационному активу** | | | **Совокупная ценность информационного актива** |
| **Конфиденциальность** | **Целостность** | **Доступность** |
|  |  | **Бизнес-процесс 1** | **Подпроцесс 1** |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| **Подпроцесс 2** |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| **Бизнес-процесс N** | **Подпроцесс 1** |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| **Подпроцесс 2** |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| **Подпроцесс 3** |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

Маркировка информации и правила обращения с ней

Следует разработать правила маркировки информации в зависимости от установленной категории конфиденциальности. Должны быть разработаны правила обращения с информацией регламентирующие операции по ее обработке, хранению, передаче, изменению категории и уничтожению для каждой категории.

Все сотрудники Банка, работающие с информацией, должны быть ознакомлены с правилами маркировки и обращения с информацией.

При использовании информации совместно с другими организациями в договора должны быть включены правила определения ее категорий.

Безопасность, связанная с персоналом

Требования к безопасности до найма сотрудников

Роли и обязанности

Все роли, участвующие в процессе обеспечения ИБ, должны быть определены. Обязанности по их выполнению должны быть назначены всем сотрудникам, а также представителям сторонних организаций, участвующим в обеспечении ИБ.

Роли по управлению и обеспечению ИБ определяются с учетом организационной структуры Банка, имеющихся ресурсов, функциональных и процедурных требований.

Роли по обеспечению ИБ и ответственность за их исполнение должны быть зафиксированы в должностных инструкциях сотрудников Банка.

Отбор персонала и политика приема на работу

Должен быть определен порядок проверки кандидатов при рассмотрении вопроса о приеме их на работу. Проверка должна также распространяться на временных сотрудников и представителей сторонних организаций, если они будут иметь доступ к активам Банка.

Процедуру проверки следует регламентировать в должностных инструкциях сотрудников управления персоналом, службы безопасности и сотрудников отделов, принимающих участие в проверке квалификации кандидатов. Результаты выполнения проверок необходимо фиксировать.

Контрольные проверки сотрудников, имеющих доступ к информации ограниченного распространения, следует выполнять регулярно, а также проводить внеплановые проверки при выявлении фактов нештатного поведения сотрудников, их участия в инцидентах ИБ, или подозрений в таком поведении или участии.

Условия найма

Все кандидаты должны быть ознакомлены с условиями контракта или трудового договора и должны его подписать. Условия контрактов или трудовых договоров должны включать обязательства по обеспечению ИБ.

При необходимости эти обязательства должны распространяться и на определенный период по окончании срока работы. В договоре должны быть описаны меры, которые будут приняты в случае несоблюдения сотрудником требований к безопасности.

Требования к безопасности в процессе работы

Во время действия трудовых отношений все сотрудники должны быть осведомлены об угрозах ИБ, а также о своей ответственности и обязанностях по обеспечению ИБ. Это поможет снизить риск ошибок персонала.

Ответственность руководства

Руководство должно требовать от сотрудников применения защитных мер в соответствии с политикой и процедурами, принятыми в Банке.

Информирование и обучение

Все сотрудники Банка, а также временные работники и представители сторонних фирм должны проходить соответствующее обучение процедурам безопасности и иметь доступ к актуальным версиям политик и процедур безопасности, существенных для выполнения ими своих функций.

Периодически следует проводить переподготовку пользователей. Для этого необходимо разработать программу периодического обучения пользователей. К обучению персонала по мере надобности следует привлекать компетентных специалистов. Выполнение программы обучения следует документировать.

В случае внесения изменений в политики, процедуры, инструкции необходимо информировать пользователей об этом посредством издания приказов и распоряжений, рассылки уведомлений по электронной почте, проведения совещаний.

Дисциплинарный процесс

Следует формализовать процедуру дисциплинарных взысканий для сотрудников, нарушивших правила и процедуры безопасной работы.

Дисциплинарные взыскания должны оказывать сдерживающий эффект на сотрудников, которые могут пренебречь правилами безопасности.

Требования к безопасности при увольнении

Прекращение или изменение трудовых отношений должно выполняться в установленном порядке.

Процесс увольнения сотрудников должен контролироваться для того, чтобы все используемые ими средства были возвращены в Банк и все права доступа к активам были аннулированы.

Изменение условий трудового договора внутри Банка должно происходить так же, как при прекращении трудового договора и приеме нового сотрудника.

Порядок увольнения

Следует четко определить ответственность при прекращении или изменении трудового соглашения.

В случае необходимости, должен быть определен период соблюдения соглашения о конфиденциальности после окончания действия трудового договора.

Возврат активов

Все сотрудники и пользователи сторонних организаций должны возвратить все принадлежащие Банку активы при расторжении трудового соглашения – программное обеспечение, оборудование, документацию и пр.

Аннулирование прав доступа

При расторжении трудового договора права доступа к информации и средствам ее обработки должны быть аннулированы.

При изменении трудового договора права доступа должны быть изменены в соответствии с новыми обязанностями. Права доступа должны быть ограничены или аннулированы до прекращения действия договора, если существует риск злоупотребления.

Физическая безопасность

Зоны безопасности

Для предотвращения несанкционированного доступа к территории и помещениям Банка и принадлежащей ему информации, ее повреждения и вмешательства в работу Банка должны применяться средства физической защиты.

Периметр безопасности

Информация и средства ее обработки должны находиться в помещениях, защищенных периметрами безопасности с соответствующими преградами и ограничением доступа.

В состав периметра могут входить стены, автоматизированные проходные и контрольно-пропускные пункты. Расположение и степень защиты периметров выбираются на основе результатов оценки рисков.

Средства контроля доступа

Физический доступ в здание Банка должен быть защищен соответствующими средствами контроля доступа.

Доступ в здание должен предоставляться только тем сотрудникам, которые имеют необходимое разрешение.

Безопасность офисов, помещений и оборудования

Необходимо разработать меры по защите офисов, помещения и оборудования и применять их.

Защита от внешних угроз и воздействий окружающей среды

Для защиты от разрушающих воздействий окружающей среды и внешних угроз, таких как пожары, землетрясения, наводнения, гражданские беспорядки и пр. следует разработать меры по защите и применять их.

Работа в зонах безопасности

Для работы на защищенных территориях следует разработать и применять защитные меры и инструкции.

Места общего доступа, площадки для погрузоразгрузочных работ

Операционные залы, помещения, куда имеют доступ клиенты, площадки для погрузоразгрузочных работ должны находиться под контролем и по возможности должны быть отделены от средств обработки информации, чтобы избежать доступа посторонних.

Требования к безопасности для таких территорий необходимо определить путем оценки рисков.

Безопасность оборудования

Расположение и защита оборудования

Оборудование должно быть расположено и защищено таким образом, чтобы снизить риски и опасности, связанные с окружающей средой и возможностью несанкционированного доступа.

Защита от сбоев электропитания

Следует применять меры для защиты оборудования от сбоев и других аномалий в системе электропитания.

Защита кабельной системы

Силовые и телекоммуникационные кабели, передающие данные или поддерживающие информационные сервисы, должны быть защищены от перехвата или повреждения.

Поддержка работоспособности оборудования

Для обеспечения постоянной доступности и целостности оборудования следует проводить его регулярное профилактическое обслуживание.

Безопасность оборудования за пределами Банка

Должны быть разработаны меры для защиты оборудования, находящегося за пределами Банка. Эти меры должны разрабатываться с учетом рисков удаленной работы.

Безопасность при высвобождении или повторном использовании оборудования

Все оборудование, содержащее устройства хранения информации, должно проверяться на отсутствие конфиденциальной информации и лицензионного ПО перед высвобождением или повторным использованием оборудования.

Необходимо разработать процедуры, позволяющие надежно уничтожать информацию при высвобождении или перед повторным использованием оборудования.

Удаленное использование

Для использования оборудования, информации или ПО за пределами Банка должна требоваться санкция руководства.

Обеспечение ИБ при эксплуатации

Процедуры эксплуатации и ответственность

Должны быть разработаны процедуры управления и эксплуатации средств обработки информации для обеспечения правильной и безопасной эксплуатации.

Документированные правила работы

Необходимо разработать инструкции по эксплуатации, документировать и поддерживать их в актуальном состоянии. Пользователи, которым необходимы эти инструкции, должны иметь к ним доступ.

Инструкции по эксплуатации являются официальными документами, утверждаемыми руководством Банка, изменения в них должны вноситься с санкции руководства.

Контроль внесения изменений в эксплуатацию

Изменения в системах и средствах обработки информации необходимо контролировать.

Необходимо разработать процедуру, обеспечивающую контроль внесения всех изменений в оборудование, программное обеспечение и процедуры. Внесение изменений следует регистрировать.

Разделение полномочий

Полномочия по управлению или выполнению определенных действий, либо области ответственности должны быть разделены, чтобы ограничить возможности для несанкционированного изменения или неправомерного использования информации или сервисов.

В случае невозможности разделения полномочий следует применять другие меры, например, мониторинг деятельности, ведение аудиторских записей, наблюдение со стороны руководящего органа по ИБ.

Аудит безопасности должен быть независимым.

Для уменьшения вероятности возможного сговора следует применять защитные меры, обеспечивающие участие в действиях нескольких человек.

Разделение областей разработки, тестирования и эксплуатации

Области разработки, тестирования и эксплуатации должны быть разделены для снижения риска несанкционированного доступа или изменений в системах эксплуатации.

Необходимо определить степень разделения областей разработки, тестирования и эксплуатации для предотвращения возможных проблем в эксплуатации и обеспечить ее принятием соответствующих мер.

Управление сервисами, предоставляемыми сторонними организациями

Необходимо контролировать выполнение соглашений на предоставление услуг сторонними организациями для обеспечения уверенности в том, что качество и уровень безопасности предоставляемых сервисов соответствуют требованиям Банка.

Контроль предоставления сервисов

Необходимо контролировать внедрение, выполнение и поддержку сторонними организациями средств защиты и уровней предоставляемых сервисов, включенных в соглашения о предоставлении услуг.

Кроме того, необходимо контролировать поддержку сторонними организациями объема сервисов, достаточного для обеспечения непрерывности в соответствии с аварийными планами.

Мониторинг и оценка сервисов, предоставляемых сторонними организациями

Необходимо регулярно проводить мониторинг и анализ сервисов, отчетов и регистрационных записей, предоставляемых сторонними организациями.

Контроль изменений в предоставляемых сторонними организациями сервисах

Изменения в предоставлении сторонними организациями сервисов, включая поддержку и усовершенствование существующей СУИБ, необходимо контролировать. В случае существенных изменений, затрагивающих критичные системы и процессы, может потребоваться проведение оценки рисков.

Планирование и приемка систем

Для минимизации системных ошибок и обеспечения вычислительной мощности необходимо заранее планировать и формулировать требования по обеспечению необходимого объема и вычислительной мощности систем.

Прогнозирование требуемой вычислительной мощности необходимо для уменьшения риска перегрузки систем.

Управление мощностью

Для обеспечения требуемой производительности проектируемых систем необходимо контролировать использование ресурсов.

Приемка систем

Необходимо установить критерии приемки и разработать процедуру приемки для новых информационных систем, обновлений и новых версий. Перед приемкой система должна проходить соответствующее тестирование.

Защита от вредоносного программного обеспечения

Необходимо предпринимать меры для защиты целостности информации и ПО от злонамеренного и несанкционированного изменения ПО.

Пользователи должны быть осведомлены об угрозах вредоносного ПО. Должны быть внедрены защитные меры для предотвращения, обнаружения и удаления вредоносного ПО.

Защита от вредоносного ПО

Должны быть внедрены меры предотвращения, обнаружения и восстановления для защиты от вредоносного ПО.

Кроме того, необходимо разработать процедуры информирования пользователей об угрозах вредоносного ПО.

В Банке должны применяться только официально приобретенные средства защиты от вредоносного ПО. Установка и регулярное обновление средств защиты от вредоносного ПО на автоматизированных рабочих местах и серверах АБС должны осуществляться администраторами АБС.

Установку обновлений программного обеспечения, используемого для защиты от вредоносного ПО, рекомендуется осуществлять в автоматическом режиме.

Должны быть разработаны и введены в действие политика и инструкции по антивирусной защите, учитывающие особенности банковских технологических процессов. Особое внимание должно быть уделено антивирусной фильтрации трафика электронного почтового обмена.

Рекомендуется осуществлять построение эшелонированной централизованной системы защиты от вредоносного ПО, предусматривающей использование средств защиты различных производителей и их раздельную установку на рабочих станциях, почтовых серверах и межсетевых экранах.

В ЭВМ и АБС не допускается присутствие и использование программного обеспечения и данных, не связанных с выполнением конкретных функций в банковских технологических процессах организации.

Устанавливаемое или изменяемое программное обеспечение должно быть предварительно проверено на отсутствие вредоносного ПО. После установки или изменения программного обеспечения должна быть выполнена проверка на наличие вредоносного ПО.

При обнаружении вредоносного ПО необходимо принять меры по устранению последствий от его воздействия, проинформировать руководство и приостановить при необходимости работу (на период устранения последствий).

Отключение или необновление средств защиты от вредоносного ПО не допускается. Установка и обновление средств защиты от вредоносного ПО в Банке должны контролироваться представителями ПБоИБ.

Ответственность за выполнение требований политики и инструкций антивирусной защиты должна быть возложена на руководителя функционального подразделения организации, а обязанности по выполнению мер защиты должны быть возложены на каждого сотрудника организации, имеющего доступ к ЭВМ и/или АБС.

Защита при изменении ПО

Изменение ПО должно быть санкционировано. Перед изменением ПО необходимо убедиться в том, что оно не содержит вредоносного кода.

Резервное копирование

Для обеспечения целостности и доступности информации и средств ее обработки необходимо разработать политику резервного копирования данных.

Резервное копирование информации

Резервные копии информации и ПО должны выполняться регулярно и тестироваться в соответствии с разработанной политикой резервного копирования.

Управление сетевой безопасностью

Для обеспечения безопасности передаваемой информации по вычислительным сетям необходимо разработать и внедрить соответствующие меры защиты.

Средства обеспечения сетевой безопасности

Вычислительные сети должны адекватно управляться и контролироваться для обеспечения защиты от угроз и поддержания защиты систем и приложений, использующих сети, а также защиты передаваемой по сети информации.

Администраторы вычислительных сетей должны внедрить средства защиты сетей, гарантирующие безопасность информации в сетях и защиту сервисов от несанкционированного доступа.

Безопасность сетевых сервисов

Мероприятия по защите, уровень сервисов и требования к управлению сетевыми сервисами должны быть определены и включены в соглашения, в зависимости от того, обеспечиваются ли эти сервисы соответствующими подразделениями Банка или предоставляются по договорам сторонними организациями.

Обращение с носителями информации

Для предотвращения несанкционированного разглашения, модификации или уничтожения активов и нарушения деятельности Банка необходимо контролировать и физически защищать носители информации.

Должны быть разработаны соответствующие правила для защиты документов, компьютерных носителей, входных и выходных данных и системной документации от несанкционированного разглашения, модификации или уничтожения.

Обращение со съемными компьютерными носителями

Должны быть разработаны и документированы правила обращения со съемными компьютерными носителями.

Все пользователи, имеющие доступ к съемным компьютерным носителям, должны быть ознакомлены с этими правилами.

Уничтожение носителей

Носители, ставшие ненужными, следует утилизировать с соблюдением требований безопасности. Для этого необходимо разработать правила безопасной утилизации носителей.

Правила обращения с информацией

Для защиты информации от несанкционированного раскрытия или неправомерного использования необходимо разработать правила хранения информации и обращения с ней.

Все сотрудники, имеющие доступ к информации, должны быть ознакомлены с правилами хранения и обращения с информацией при приеме на работу.

Безопасность системной документации

Системная документация должна быть защищена от несанкционированного доступа.

Следует разработать и соблюдать правила безопасного хранения системной документации.

Следует ограничить круг лиц, имеющих доступ к системной документации. Для доступа к ней должно требоваться разрешение владельца (ответственного лица) программы.

Обмен информацией

Обмен информацией и программным обеспечением между Банком и сторонними организациями должен контролироваться и соответствовать действующему законодательству.

Должны быть разработаны правила и стандарты для защиты информации и физических носителей, содержащих передаваемую информацию.

Правила обмена информацией

Необходимо разработать правила и защитные меры для защиты обмена информацией, учитывающие использование всех способов передачи.

Сотрудники, имеющие отношение к процессам обмена информацией, должны быть ознакомлены с этими правилами.

Соглашения об обмене

Для обмена информацией и программным обеспечением между Банком и сторонними организациями (в физическом и электронном виде) должны быть разработаны соглашения.

Соглашения об обмене информацией должны содержать ссылки на правила и стандарты, разработанные для защиты процесса обмена информацией.

Обеспечение безопасности носителей при передаче

Носители, содержащие информацию, должны быть защищены при передаче от несанкционированного доступа, неправомерного использования или повреждения во время транспортировки.

Безопасность при обмене электронными сообщениями

Информация, передаваемая в электронных сообщениях, должна быть защищена соответствующим образом. Средства и методы защиты должны быть описаны в частных политиках использования соответствующих подсистем обмена электронными сообщениями.

Меры по защите информации, передаваемой в электронных сообщениях, должны разрабатываться с учетом рисков.

Безопасность электронных офисных систем

К электронным офисным системам относят системы электронного документооборота и автоматизации делопроизводства, системы автоматизации бумажных и электронных архивов, системы автоматизации кадрового учета и документооборота и другие.

Должны быть разработаны и внедрены правила и процедуры для обеспечения защиты информации, используемой в электронных офисных системах.

При разработке защитных мер необходимо учитывать известные угрозы и уязвимости, связанные с использованием таких систем.

Безопасность систем электронной коммерции

Для обеспечения безопасности систем электронной коммерции и безопасного их использования следует выработать решения по их защите. Также необходимо принять решения по обеспечению целостности и доступности информации, опубликованной в общедоступных системах.

Безопасность систем электронной коммерции

Информация, используемая в системах электронной коммерции и передаваемая через общедоступные сети, должна быть защищена от мошеннической деятельности, раскрытия или модификации.

Онлайновые транзакции

Информацию, используемую в онлайновых транзакциях, необходимо защищать для предотвращения незавершенных передач, ошибочной передачи, несанкционированной модификации сообщений, несанкционированного разглашения и несанкционированного дублирования.

Безопасность общедоступных систем

Необходимо предпринимать меры для защиты целостности информации, опубликованной в общедоступных системах, чтобы предотвратить несанкционированные изменения, которые могут повредить репутации Банка.

Обеспечение информационной безопасности при использовании ресурсов сети Интернет

Ресурсы сети Интернет в Банке могут использоваться для ведения дистанционного банковского обслуживания, получения и распространения информации, связанной с банковской деятельностью (путем создания web сайтов), информационно-аналитической работы в интересах организации, обмена почтовыми сообщениями исключительно с внешними организациями, а также ведения собственной хозяйственной деятельности.

Иное использование ресурсов сети Интернет, решение о котором не принято руководством организации в установленном порядке, должно рассматриваться как нарушение ИБ.

При осуществлении дистанционного банковского обслуживания клиентов, в связи с повышенными рисками информационной безопасности при взаимодействии с сетью Интернет обязательно должны применяться соответствующие средства защиты информации (межсетевые экраны, антивирусные средства, средства криптографической защиты информации (СКЗИ) и пр.), обеспечивающие прием и передачу информации только в установленном формате и только для конкретной технологии. Не рекомендуется подключать к внутренним сетям ЭВМ, с помощью которых осуществляется взаимодействие с сетью Интернет. Почтовый обмен через сеть Интернет должен осуществляться с использованием защитных мер.

Требования к обеспечению информационной безопасности при использовании ресурсов Интернет должны детализироваться в частной политике использования ресурсов сети Интернет.

Мониторинг

Для обнаружения несанкционированной деятельности по обработке информации необходимо осуществлять мониторинг работы систем и регистрировать инциденты ИБ.

Чтобы убедиться в том, что проблемы в ИС были выявлены, следует вести рабочие журналы систем и регистрировать ошибки.

Деятельность по мониторингу и регистрации событий должна осуществляться в соответствии с действующим законодательством.

Журналы аудита

Необходимо вести и сохранять в течение определенного периода журналы аудита деятельности пользователей, нештатных ситуаций и инцидентов информационной безопасности для использования в расследованиях и мониторинге контроля доступа.

Журналы аудита могут содержать конфиденциальные персональные данные, поэтому должны быть предприняты меры для сохранения их конфиденциальности.

Администраторы не должны иметь возможности удалять или редактировать журналы собственной деятельности.

Мониторинг использования систем

Должны быть разработаны процедуры мониторинга использования средств обработки информации. Результаты выполнения процедур мониторинга следует регулярно анализировать.

Для определения параметров систем, подлежащих мониторингу, следует выполнить оценку рисков.

Процедуры мониторинга следует использовать с гарантией для выполнения пользователями только санкционированных действий в системах.

Защита регистрационной информации

Средства журналирования и регистрационная информация должны быть защищены от неправомерных действий и несанкционированного доступа.

Для выявления инцидентов ИБ следует использовать средства, позволяющие выбирать из журналов большого объема только события, имеющие отношение к ИБ.

Журналы действий пользователей и администраторов

Деятельность администраторов и пользователей систем должна регистрироваться.

Журналы действий пользователей и администраторов систем должны регулярно анализироваться.

Регистрация ошибок

Информация об ошибках должна регистрироваться, анализироваться, и по результатам анализа должны предприниматься соответствующие действия.

Регистрация информации об ошибках и сбоях в работе систем может ухудшать производительность систем, поэтому следует по результатам оценки рисков принять решение о степени детализации этих данных.

Синхронизация системных часов

Для обеспечения точности записей в контрольных журналах, которые могут потребоваться для расследований или в качестве улик при уголовном или административном преследовании, необходимо синхронизировать системные часы с согласованным источником точного времени.

Контроль доступа

Требования к контролю доступа

Доступ к информации и средствам ее обработки должен контролироваться в соответствии с бизнес-требованиями и требованиями безопасности.

Правила контроля доступа должны учитывать правила распространения информации в Банке.

Политика контроля доступа

Политика контроля доступа должна быть разработана и документирована на основе бизнес -требований и требований безопасности доступа.

Следует четко определить правила контроля доступа и права каждого пользователя или группы пользователей.

Для поддержки правил контроля доступа должны быть разработаны соответствующие процедуры и назначена персональная ответственность.

Управление доступом пользователей

Для обеспечения санкционированного доступа пользователей и предотвращения несанкционированного должны быть разработаны процедуры контроля распределения прав пользователей к автоматизированным системам и сервисам.

Процедуры должны охватывать все стадии жизненного цикла прав доступа пользователя, начиная от регистрации новых пользователей и заканчивая удалением прав доступа пользователей, которым больше не требуется доступ к ИС или сервисам.

Пользователи, имеющие привилегии в системах, должны находиться под особым контролем.

Регистрация пользователей

Необходимо разработать официальную процедуру регистрации и удаления регистрационных данных пользователей, которая будет использоваться для предоставления и доступа ко всем автоматизированным системам и сервисам.

Для упрощения предоставления прав пользователям следует разработать профили, включающие в себя набор прав доступа для выполнения каждой роли, основанной на бизнес-требованиях.

В трудовые договоры следует включить описание мер, которые последуют в случае попытки сотрудника получить несанкционированный доступ к ИС или сервисам.

Управление привилегиями

Предоставление и использование привилегированных прав доступа должно ограничиваться и контролироваться.

Для предотвращения несанкционированного доступа к системам следует разработать процедуру предоставления привилегированных прав доступа.

Управление паролями пользователей

Должен быть разработан процесс предоставления и управления паролями пользователей.

Следует разработать правила выбора, изменения и хранения паролей пользователями и ознакомить с ними пользователей перед предоставлением им доступа к системам или сервисам.

Проверка прав доступа пользователей

Для обеспечения эффективного контроля доступа к системам и сервисам следует разработать процесс проверки прав доступа пользователей и выполнять его через определенные интервалы времени.

Обязанности пользователей

Для эффективной поддержки безопасности и предотвращения несанкционированного доступа, компрометации и хищения информации и средств ее обработки необходимо сотрудничество авторизованных пользователей.

Пользователи должны быть поставлены в известность о своих обязанностях по поддержке эффективных мер контроля доступа, в частности, о правилах использования паролей и защите пользовательского оборудования.

Для уменьшения риска несанкционированного доступа или повреждения информации на любых носителях или средств ее обработки следует применять правила "чистого стола" и "чистого экрана" (раздел 4.7.3.3).

Использование паролей

При выборе и использовании паролей пользователи должны применять надежные методы.

В случае необходимости предоставления пользователю доступа к нескольким сервисам или системам, он может использовать один и тот же надежный пароль для всех сервисов, обеспечивающих необходимый уровень защиты при хранении пароля.

Правила обеспечения безопасности при выборе и использовании паролей должны быть сформулированы в виде парольной политики.

Оборудование, остающееся без присмотра

Пользователи должны обеспечивать необходимую защиту оборудования, остающегося без присмотра.

Все пользователи должны быть осведомлены о требованиях безопасности и правилах защиты остающегося без присмотра оборудования, а также о своих обязанностях по обеспечению этой защиты.

Оборудование, установленное на пользовательских территориях, например, рабочие станции и файловые серверы, могут потребовать особой защиты от несанкционированного доступа в том случае, если они останутся без присмотра на длительный срок.

Политика "чистого стола" и "чистого экрана"

Должна применяться политика очистки стола от бумажных и компьютерных носителей и политика очистки экрана для средств обработки информации.

Политика "чистого стола" и "чистого экрана" должна применяться с учетом категории информации в соответствии с требованиями законодательства и договорных обязательств. Требования политики формулируются в правилах внутреннего трудового распорядка, с которыми должен ознакомиться каждый новый сотрудник, принимаемый на работу, а также в частной политике по стандартизации рабочих мест.

Контроль доступа к вычислительной сети

Для предотвращения несанкционированного доступа к сетевым сервисам доступ к внутренним и внешним сетевым сервисам должен контролироваться.

Для предотвращения нарушения пользователями безопасности использования сетей и сетевых сервисов следует применять следующие меры:

1. Использовать соответствующие интерфейсы между сетями Банка, сетями сторонних организаций и общедоступными сетями.
2. Использовать соответствующие механизмы аутентификации для пользователей и оборудования.
3. Осуществлять контроль доступа пользователей к сетевым сервисам.

Политика использования сетевых сервисов

Пользователям должен предоставляться доступ только к тем сервисам, на использование которых они получили специальное разрешение.

Следует разработать правила использования сетей и сетевых сервисов. Пользователи должны быть ознакомлены с этими правилами перед предоставлением им доступа к сетям и сетевым сервисам.

Правила использования сетей и сетевых сервисов должны учитывать правила контроля доступа, принятые в Банке.

Аутентификация пользователей при внешних подключениях

Для контроля доступа удаленных пользователей должны использоваться соответствующие методы аутентификации.

Для контроля доступа к беспроводным сетям следует использовать дополнительные средства защиты.

Уровни необходимой защиты и методы аутентификации при внешних подключениях должны определяться на основе оценки рисков.

Идентификация оборудования в сети

Автоматические подключения к удаленным системам должны применяться с использованием средств аутентификации. Это особенно важно в том случае, если для подключения используется сеть, находящаяся за пределами контроля организации.

Средства аутентификации оборудования могут применяться в сочетании с аутентификацией пользователей.

Защита удаленных диагностических портов

Необходимо контролировать физический и логический доступ к диагностическим портам.

Порты, сервисы и подобные средства, установленные на компьютерном или сетевом оборудовании, и не требуемые для бизнес-деятельности, должны быть закрыты или удалены для предотвращения несанкционированного доступа.

Разделение сетей

Группы информационных сервисов, пользователей и информационных систем должны быть разделены в вычислительных сетях.

Критерии разделения сетей должны быть основаны на правилах контроля доступа, применяемых в Банке, и требованиях к доступу.

Кроме того, решения о разделении сетей должны приниматься с учетом ценности и категории информации, хранящейся и обрабатываемой в сети.

При использовании беспроводных сетей в силу неопределенности их периметра для адекватного выбора средств защиты необходимо выполнить оценку рисков.

Контроль сетевых подключений

Для совместно используемых сетей, особенно выходящих за пределы Банка, количество подключающихся пользователей должно быть ограничено в соответствии с правилами контроля доступа и требованиями к бизнес-приложениям.

Права пользователей на доступ к сети должны контролироваться в соответствии с правилами контроля доступа, действующими в Банке.

Контроль сетевой маршрутизации

Для обеспечения уверенности в том, что компьютерные подключения и информационные потоки не нарушают правила контроля доступа, должны использоваться средства маршрутизации.

Средства маршрутизации должны использовать механизмы проверки адресов источника и назначения.

Требования к сетевой маршрутизации должны быть разработаны с учетом правил контроля доступа.

Контроль доступа к операционным системам

Для предоставления доступа к операционным системам только авторизованным пользователям, должны использоваться средства защиты, обеспечивающие следующее:

1. Аутентификацию авторизованных пользователей в соответствии с правилами контроля доступа.
2. Регистрацию успешных и неуспешных попыток аутентификации в системе.
3. Регистрацию использования системных привилегий.
4. Выдачу сигнала при нарушении политики безопасности системы.
5. Обеспечение соответствующих средств аутентификации.
6. Ограничение времени подключения пользователя.

Безопасная процедура входа в систему

Доступ к операционной системе должен осуществляться с использованием процедуры безопасной регистрации в системе.

Процедура безопасной регистрации в операционной системе должна минимизировать возможность несанкционированного доступа к системе и выдавать минимум сведений об операционной системе.

Идентификация и аутентификация пользователей

Все пользователи должны иметь уникальные идентификаторы для персональной аутентификации. Кроме того, должны быть выбраны соответствующие средства аутентификации для подтверждения заявленных персональных данных пользователей.

Эти средства должны применяться для проверки всех типов пользователей (персонала технической поддержки, пользователей, операторов).

Система управления паролями

Для проверки качества паролей следует использовать системы управления паролями.

Должны быть разработаны правила выбора и смены паролей. Все пользователи должны быть ознакомлены с этими правилами.

Использование системных утилит

Использование утилит и служебных программ, которые могут иметь возможность обходить средства защиты, реализованные в системе и приложениях, необходимо ограничить и тщательно контролировать.

Отключение по тайм-ауту

Неактивные сессии должны завершаться по истечении определенного периода бездействия.

Время бездействия до отключения по тайм-ауту должно выбираться в зависимости от рисков безопасности для территорий, категории информации, обрабатываемой в приложениях и пользователей, имеющих доступ к оборудованию.

Ограничение времени подключения

В приложениях с высоким уровнем риска следует использовать ограничение времени подключения для обеспечения дополнительной безопасности.

Для уменьшения возможности несанкционированного доступа во время подключения следует ограничивать период времени, в течение которого разрешены терминальные подключения к компьютерным сервисам, если используемые для работы с ними терминалы установлены в общедоступных или внешних помещениях, на которые не распространяются реализованные в Банке меры по обеспечению безопасности.

Контроль доступа к приложениям

Для предотвращения несанкционированного доступа к информации, хранящейся в ИС, должны использоваться средства защиты.

Логический доступ к прикладному ПО и информации должен предоставляться только авторизованным пользователям.

Прикладные системы должны:

1. Контролировать доступ пользователей к информации и функциям прикладных программ в соответствии с принятой в организации политикой контроля доступа
2. Обеспечивать защиту от несанкционированного доступа для любых утилит и системных программ, которые способны обходить средства защиты, реализованные в операционной системе и приложениях
3. Не нарушать безопасность других систем, совместно с которыми используются информационные ресурсы

Ограничение доступа к информации

Доступ к информации и функциям прикладных систем для пользователей и специалистов технической поддержки должен быть ограничен в соответствии в применяемыми в Банке правилами контроля доступа.

Кроме того, ограничения должны быть основаны на требованиях безопасности конкретных прикладных систем.

Изоляция систем, содержащих конфиденциальную информацию

Системы, обрабатывающие конфиденциальную информацию, должны работать в изолированной вычислительной среде.

Изолированная вычислительная среда может обеспечиваться физическими и логическими средствами.

Мобильные компьютеры и средства удаленной работы

Для обеспечения безопасности информации при использовании мобильных компьютеров и средств удаленной работы должны быть разработаны меры безопасности, соответствующие рискам, связанным с этими методами работы.

При использовании мобильных компьютеров необходимо учесть риск, связанный с работой в незащищенной среде, и предпринять соответствующие защитные меры. При использовании средств удаленной работы в Банке необходимо обеспечить защиту места удаленной работы и обеспечить наличие соответствующих защитных мер для данного вида работы.

Мобильные вычислительные средства и средства связи

Необходимо разработать политику и предпринять соответствующие меры для защиты от рисков использования мобильных вычислительных средств и средств связи в незащищенной среде.

Политика безопасной работы с использованием мобильных вычислительных средств должны включать требования к физической защите, контролю доступа, резервному копированию, применению средств криптографической защиты и антивирусной защите. Кроме того, политика должна содержать правила подключения мобильных средств к сетям и руководства по использованию мобильных средств в общественных местах.

Сотрудники, которым разрешено использовать мобильные вычислительные средства, должны знать и выполнять требования безопасности такой работы.

Удаленная работа

Необходимо разработать политику, правила и стандарты для обеспечения безопасности удаленной работы.

Использование средств удаленной работы должно разрешаться только в том случае, если эти средства обладают необходимыми функциями для обеспечения безопасности и соответствуют принятой в организации политике безопасности.

Меры безопасности при удаленной работе должны обеспечивать защиту от кражи оборудования и информации, несанкционированного раскрытия информации, несанкционированного удаленного доступа к автоматизированным системам Банка и неправомерного использования технических средств.

Сотрудники, которым разрешено использовать средства удаленной работы, должны знать и выполнять требования безопасности такой работы.

Приобретение, разработка и поддержка систем

Требования безопасности к системам

Требования к безопасности должны быть определены и согласованы до разработки и внедрения автоматизированной системы.

Все требования к безопасности должны быть учтены в проекте на этапе определения требований и оценены, согласованы и зафиксированы в составе общего процесса создания информационной системы.

Анализ и определение требований к безопасности

Бизнес-требования к разработке новых систем и усовершенствованию старых должны учитывать требования безопасности.

Требования к безопасности и средства защиты должны соответствовать ценности активов и потенциальному ущербу для Банка в случае сбоя или нарушения безопасности. Основой для анализа требований к безопасности и выбору мер для поддержки безопасности является оценка рисков.

В случае приобретения систем в договор с поставщиком должны быть включены требования к безопасности. Если уровень безопасности в предлагаемых системах не удовлетворяет требованиям, решения по обеспечению безопасности должны быть пересмотрены до приобретения систем.

Безопасность в прикладных системах

Для предотвращения утраты, несанкционированной модификации и неправомерного использования информации в прикладных системах, в них должны быть встроены средства проверки корректности обработки. Эти средства должны обеспечивать проверку вводимых данных, внутренней обработки и результатов работы.

Для систем, обрабатывающих конфиденциальную и/или ценную информацию или оказывающих определенное воздействие на такую информацию, могут потребоваться дополнительные средства защиты.

Перечень необходимых средств следует определить на основе требований к безопасности и результатов оценки рисков.

Проверка вводимых данных

В целях обеспечения правильности и соответствия поставленной задаче, необходимо проверять данные, вводимые в прикладные системы.

Должны быть разработаны правила реакции на ошибки при проверке. Обязанности всех сотрудников, участвующих в процессе ввода данных, следует включить в инструкции по эксплуатации.

Персонал, участвующий во вводе данных в прикладные системы, должен быть ознакомлен с актуальными версиями инструкций по эксплуатации.

Контроль обработки информации

Для обнаружения повреждения правильно введенных данных в результате ошибок при обработке или умышленного ввода в систему должны быть встроены функции проверки.

Целостность информации

Должны быть определены требования к проверке достоверности и защите целостности информации, а также определены и внедрены соответствующие средства защиты.

Проверка выходных данных

Результаты работы, выдаваемые прикладной системой, необходимо проверять для того, чтобы убедиться, что информация была обработана правильно и соответствует всем условиям.

Средства криптографической защиты информации

Для защиты конфиденциальности, достоверности и целостности информации средствами криптографической защиты следует разработать политику использования таких средств.

Необходимо осуществлять управление ключами для поддержки использования криптографических методов.

Политика использования СКЗИ

Должна быть разработана и внедрена политика использования СКЗИ для защиты информации.

Средства криптографической защиты информации следует использовать, если другие средства не обеспечивают необходимого уровня защиты, для защиты конфиденциальности особо важной информации, для защиты подлинности и целостности электронной информации, обеспечения неотказуемости (как средства обеспечения неоспоримости отправления или получения при разрешении споров относительно того, имели ли место события или действия).

СКЗИ должны быть реализованы на основе алгоритмов, соответствующих национальным стандартам РФ, условиям договора с контрагентами и (или) стандартам Банка.

Сотрудники, использующие СКЗИ, должны быть ознакомлены с данной политикой.

Управление ключами

Для поддержки использования криптографических методов необходимо создать систему управления ключами.

Все криптографические ключи должны быть защищены от утраты, модификации и несанкционированного использования.

Оборудование, используемое для генерации и хранения ключей, должно быть физически защищено.

Безопасность системных файлов

Для обеспечения безопасности выполнения проектов в области информационных технологий и сопутствующих операций необходимо контролировать доступ к системным файлам.

Контроль используемого программного обеспечения

Необходимо разработать правила контроля установки программного обеспечения на рабочих системах.

Уровень поддержки используемого программного обеспечения, предоставленного другими поставщиками, должен соответствовать требованиям поставщиков. Решение о переходе на новую версию должно приниматься с учетом безопасности этой версии.

Программные обновления необходимо устанавливать в том случае, если они помогут устранить уязвимости или уменьшить их серьезность.

Защита данных, используемых для тестирования

Тестовые данные необходимо защищать и контролировать.

При тестировании систем используемые для этого данные необходимо защищать так же, как и рабочие.

Контроль доступа к исходным программным кодам

Доступ к исходным кодам программ должен быть ограничен.

Для предотвращения введения в программные коды несанкционированной функциональности, доступ к библиотекам исходных кодов программ следует строго ограничить и контролировать.

Безопасность при разработке и поддержке

Среды, в которых происходит проектирование и поддержка, должны находиться под строгим контролем.

Руководители, ответственные за прикладные системы, должны также нести ответственность за среды проектирования или поддержки. Они должны обеспечить контроль всех предлагаемых изменений в системе, чтобы гарантировать, что эти изменения не нарушат безопасность системы или среды эксплуатации.

Правила контроля изменений

Должны быть разработаны правила внесения изменений, которыми следует руководствоваться при внесении изменений.

Эти правила должны обеспечивать минимальную вероятность повреждения автоматизированных систем.

Техническая проверка после внесения изменений в системы

После внесения изменений в системы их необходимо проверять и тестировать, чтобы убедиться в отсутствии нарушения безопасности или эффективности работы.

Ограничения на изменения в программных пакетах

Модификация программных пакетов должна применяться только при необходимости и строго контролироваться.

В случае внесения изменений должны использоваться только официально приобретенные версии программных пакетов.

Утечка информации

Возможности утечки информации должны предотвращаться.

Следует разработать меры для выявления возможных каналов утечки информации.

Разработка программного обеспечения сторонними организациями

Разработка программ внешним разработчиком должна происходить под наблюдением и контролем соответствующих сотрудников Банка.

Необходимо разработать меры для предотвращения внесения внешним разработчиком недекларированных возможностей и вредоносного программного обеспечения.

Управление уязвимостями

Для уменьшения рисков, проистекающих от эксплуатации опубликованных уязвимостей, необходимо осуществлять управление такими уязвимостями, предусматривающее оценку результатов от предпринятых действий.

Такие решения должны приниматься в отношении операционных систем и других приложений.

Контроль уязвимостей

Информация об уязвимостях должна использоваться для анализа подверженности автоматизированных систем Банка этой уязвимости и принятия соответствующих мер по снижению соответствующего риска.

Управление инцидентами

Регистрация инцидентов информационной безопасности и недостатков в работе систем

Для своевременного принятия мер по устранению инцидентов ИБ и недостатков в работе ИС необходимо разработать правила регистрации событий и уведомления о них. Все сотрудники и пользователи сторонних организаций должны быть осведомлены о правилах регистрации всех типов событий и сбоев в работе систем, которые могут оказать влияние на безопасность активов Банка.

В их обязанности должна входить максимально быстрая передача информации об инцидентах безопасности или сбоях в работе соответствующим лицам.

Уведомление о событиях информационной безопасности

Информация о событиях информационной безопасности должна быть максимально быстро передана соответствующим лицам.

Необходимо разработать процедуру уведомления, а также процедуру реакции на инциденты, включающую в себя действия, которые должны выполняться при поступлении сообщения об инциденте.

Все сотрудники и пользователи сторонних организаций должны быть ознакомлены с процедурой уведомления об инцидентах, а в их обязанности должна входить максимально быстрая передача информации о таких инцидентах.

Уведомление о недостатках в работе систем

В обязанности пользователей ИС и информационных сервисов должно быть включено уведомление о выявленных или подозреваемых уязвимостях или угрозах для систем и сервисов.

Пользователи должны максимально быстро сообщать об этом либо своему руководителю, либо непосредственно поставщику услуг.

Управление инцидентами информационной безопасности и усовершенствование

Должна быть назначена ответственность за обработку событий информационной безопасности. Процесс управления инцидентами информационной безопасности необходимо постоянно усовершенствовать, чтобы обеспечить его эффективность.

Если требуется предоставить доказательства участия в инцидентах, то процесс сбора улик должен соответствовать требованиям законодательства.

Обязанности и правила

Должны быть определены обязанности руководства и правила, позволяющие быстро, эффективно и организованно реагировать на инциденты информационной безопасности.

Кроме регистрации событий информационной безопасности и сбоев в работе систем, необходимо использовать мониторинг работы систем, появления уязвимостей и предупреждений о проблемах для обнаружения инцидентов ИБ.

Изучение инцидентов ИБ

Должны быть механизмы, позволяющие оценивать и отслеживать тип инцидентов, их масштаб и связанные с ними затраты.

Полученная информация должна использоваться для сокращения частоты, уменьшения масштаба и ущерба от возникновения подобных инцидентов в будущем.

Сбор улик

Для привлечения человека или организации к ответственности в связи с происшедшими инцидентами ИБ, должны быть обеспечены сбор, хранение и предоставление доказательств его вины.

Если обвинение связано с внутренним дисциплинарным взысканием, необходимые улики определяются внутренними процедурами.

Если обвинение относится к области права (гражданского или уголовного), предъявленные улики должны соответствовать правилам предъявления улик, сформулированным в соответствующем законе, или правилам, принятым в суде, в котором будет слушаться дело.

Обеспечение непрерывности бизнеса

Аспекты информационной безопасности для управления непрерывностью бизнеса

Необходимо разработать процесс обеспечения и поддержки непрерывности бизнеса для того, чтобы уменьшить негативное влияние бедствий и нарушений безопасности (которые могут быть, например, результатами стихийных бедствий, случайностей, отказа оборудования и преднамеренных действий) с помощью сочетания профилактических и восстановительных мер. Для разработки контролируемого процесса обеспечения и поддержки непрерывности бизнеса следует выявить события, способные нарушить деятельность Банка.

Включение информационной безопасности в процесс обеспечения непрерывности бизнеса

Необходимо разработать и поддерживать процесс обеспечения непрерывности бизнеса Банка, включающий требования информационной безопасности, необходимые для обеспечения непрерывности бизнеса.

Непрерывность бизнеса и оценка риска

Необходимо определить события, которые могут нарушить деятельность Банка, оценить возможность их возникновения, влияния таких нарушений и их последствий для ИБ.

Оценка рисков должна проводиться при непосредственном участии владельцев активов, используемых в деятельности Банка.

Оценка должна включать в себя все области деятельности Банка.

Разработка и внедрение планов обеспечения непрерывности бизнеса

Должны быть разработаны и внедрены планы по поддержке и восстановлению деятельности Банка за определенный отрезок времени после сбоев и нарушений важных процессов.

Планы должны учитывать приоритетность бизнес-процессов, в частности, возобновление предоставления определенных услуг клиентам за приемлемый отрезок времени.

Необходимо учитывать сервисы и ресурсы, которые потребуются для этого, в том числе кадровое обеспечение, ресурсы, не связанные с обработкой информации, а также варианты аварийного восстановления для средств обработки информации.

Структура планирования обеспечения непрерывности бизнеса

Должна быть создана единая структура планов поддержки непрерывности бизнеса, чтобы гарантировать согласованность всех планов и определить приоритеты в области тестирования и поддержки.

В каждом плане поддержки непрерывности бизнеса должны быть четко указаны условия начала его исполнения и сотрудники, ответственные за выполнение каждого пункта плана.

При появлении новых требований необходимо внести поправки в принятые планы действия в нештатных ситуациях.

Тестирование, поддержка и повторная оценка планов обеспечения непрерывности бизнеса

Планы непрерывности бизнеса должны непрерывно тестироваться и обновляться, чтобы гарантировать их эффективность и соответствие текущим условиям.

Все члены группы реагирования и другие задействованные сотрудники должны быть ознакомлены с соответствующими планами, знать свои обязанности и роли.

Соответствие требованиям

Соответствие требованиям законодательства

Для того чтобы избежать нарушений, связанных с гражданским и уголовным правом, требованиями законов и нормативных актов, обязательствами по контрактам и требованиями к безопасности, при разработке, эксплуатации и управлении ИС необходимо обратиться к имеющим необходимую квалификацию юристам, чтобы получить консультации по вопросам, связанным с законодательством. Также следует учитывать возможные различия требований законодательства в различных странах.

Определение применяемых законодательных актов

Для каждой автоматизированной системы необходимо четко определить и зафиксировать все имеющие к ней отношение требования законов, нормативных актов и контрактов.

Подобным образом необходимо определить и зафиксировать конкретные меры и обязанности отдельных сотрудников по соблюдению этих требований.

Права интеллектуальной собственности

Необходимо реализовать процедуры, обеспечивающие соответствие законодательным ограничениям на использование материалов, на которые могут распространяться права интеллектуальной собственности.

Защита документов Банка

Важные документы, принадлежащие Банку, должны быть защищены от утраты, повреждения и фальсификации в соответствии с требованиями законов и нормативных актов.

Документы необходимо классифицировать по типу. Для каждого документа необходимо указать период хранения и тип носителя. Процедуры хранения и обращения с носителями должны разрабатываться в соответствии с рекомендациями производителя.

Защита данных и сохранение конфиденциальности персональных данных

Защита данных и сохранение конфиденциальности персональных данных должны быть обеспечены в соответствии с требованиями действующего законодательства, нормативных актов и договорных обязательств.

Должна быть разработана и реализована политика защиты и сохранения конфиденциальности. Персонал, осуществляющий обработку персональных данных, должен быть ознакомлен с этой политикой.

Предотвращение неправомерного использования средств обработки информации

Пользователи должны препятствовать несанкционированному использованию средств обработки информации.

Ограничение на использование криптографических средств защиты

Средства криптографической защиты должны использоваться в соответствии со всеми действующими соглашениями, а также требованиями законодательства и нормативных актов.

Соответствие требованиям политики безопасности, стандартам и техническим требованиям

Для проверки соответствия систем требованиям политики безопасности и стандартам необходимо регулярно проверять безопасность ИС.

Такие проверки должны осуществляться в соответствии с действующими политиками безопасности. Технические платформы и информационные системы необходимо проверять на соответствие стандартам реализации безопасности.

Соответствие политике безопасности и стандартам

Руководство должно обеспечить правильное выполнение всех связанных с безопасностью процедур, которые находятся в их ведении.

Кроме того, все области деятельности Банка должны проходить регулярную проверку на предмет соответствия политике безопасности и стандартам.

Проверка соответствия техническим требованиям

Информационные системы необходимо регулярно проверять на предмет соответствия стандартам реализации безопасности.

Обеспечение ИБ банковских платежных технологических процессов

Банковские платежные системы

Объекты защиты

Объектами защиты являются:

1. Банковский платежный технологический процесс.
2. Платежная информация.
3. Технологический процесс по управлению ролями и полномочиями сотрудников Банка, задействованных в обеспечении банковского платежного технологического процесса.

Порядок обмена платежной информацией

Порядок обмена платежной информацией должен быть зафиксирован в договорах между Банком и юридическими или физическими лицами, осуществляющими обмен платежной информацией.

Защита банковских платежных систем

Разделение полномочий

Полномочия в автоматизированных системах должны быть разделены для предотвращения бесконтрольного создания, авторизации, уничтожения и изменения платежной информации, а также проведения операций по изменению состояния банковских счетов.

Для исключения злоупотреблений со стороны администраторов ИС, следует обеспечить контроль и регистрацию их действий в системах.

Проверка результатов обработки информации

Результаты технологических операций по обработке платежной информации должны контролироваться и удостоверяться лицами или автоматизированными процессами.

Лица или автоматизированные процессы, осуществляющие обработку платежной информации и контроль результатов обработки, должны быть независимы друг от друга.

Авторизация и контроль целостности при работе с платежной информацией

При работе с платежной информацией необходимо проводить авторизацию и контроль целостности данной информации.

Для осуществления авторизации и контроля целостности следует применять сертифицированные или разрешенные руководством Банка средства защиты от НСД и СКЗИ.

Администрирование средств защиты платежной информации

Обязанности по администрированию средств защиты платежной информации должны возлагаться приказом по Банку на администраторов информационной безопасности с отражением этих функций в его должностных обязанностях.

Обеспечение комплексной защиты платежной информации

Комплекс мер по обеспечению информационной безопасности банковского платежного технологического процесса предусматривает:

1. Защиту платежной информации от искажения, фальсификации, переадресации, несанкционированного уничтожения, ложной авторизации платежных документов.
2. Минимально необходимый, гарантированный доступ сотрудника Банка только к тем ресурсам банковского платежного технологического процесса, которые необходимы ему для исполнения служебных обязанностей или реализации прав, предусмотренных технологией обработки платежной информации.
3. Контроль (мониторинг) исполнения установленной технологии подготовки, обработки, передачи и хранения платежной информации.
4. Аутентификацию обрабатываемой платежной информации.
5. Двустороннюю аутентификацию автоматизированных рабочих мест, участников обмена платежной информацией.
6. Восстановление платежной информации в случае ее умышленного или случайного разрушения или искажения или выхода из строя средств вычислительной техники.
7. Авторизованный ввод платежной информации в автоматизированные банковские системы двумя сотрудниками с последующей программной сверкой результатов ввода на совпадение.
8. Сверку выходных платежных сообщений с соответствующими поступившими платежными сообщениями.
9. Гарантированную доставку платежных сообщений участникам обмена.

Обеспечение ИБ банковских информационных технологических процессов

Банковские информационные технологические процессы

Неплатежная информация

К неплатежной информации в Банке относятся следующие виды информации:

1. Открытая информация, предназначенная для официальной передачи во внешние организации и средства массовой информации
2. Внутренняя банковская информация, предназначенная для использования исключительно сотрудниками Банка при выполнении ими служебных обязанностей.
3. Информация, содержащая сведения ограниченного распространения в соответствии с утвержденным Банком перечнем, подлежащая защите в соответствии с законодательством РФ, например, банковская тайна, персональные данные.
4. Информация, полученная из федеральных органов исполнительной власти и содержащая сведения ограниченного распространения.
5. Информация, содержащая сведения, составляющие государственную тайну.

Каждому виду информации должен соответствовать свой необходимый уровень защиты.

Объекты защиты

Объектами защиты являются:

1. Информационные ресурсы.
2. Управляющая информация АБС.
3. Банковский информационный технологический процесс.

Обеспечение достоверности информации

Должна быть назначена ответственность и разработаны меры по обеспечению достоверности информации, обрабатываемой в банковских информационных системах.

Должен обеспечиваться уровень защиты как собственной информации, так и информации, официально полученной из внешних организаций и от граждан в соответствии с требованиями законодательства Российской Федерации.

Обеспечение ИБ в банковских информационных технологических процессах

Требования к обеспечению ИБ в АБС

Для обеспечения ИБ в АБС должны быть реализованы следующие меры:

1. Устанавливаемые права доступа к информации в АБС должны назначаться подразделением Банка, ответственным за эту информацию (владельцем информационного актива) на основании заявки, заверенной руководителем структурного подразделения.
2. Для АБС должен быть определен порядок контроля ее функционирования со стороны лиц, отвечающих за ИБ.
3. Процессы подготовки, ввода, обработки и хранения информации, а также порядок установки, настройки, эксплуатации и восстановления необходимых технических и программных средств должны быть регламентированы и обеспечены инструктивными и методическими материалами, согласованными с ПБоИБ.
4. Должна осуществляться и быть регламентирована процедура периодического тестирования всех реализованных программно-техническими средствами функций (требований) по обеспечению ИБ. Регламентирующие документы должны быть согласованы с ПБоИБ.
5. Должна осуществляться и быть регламентирована процедура восстановления системы обеспечения ИБ.

Требования к администратору ИБ АБС

Приказом руководства должен быть назначен администратор ИБ АБС, имеющий служебные полномочия и технические возможности по контролю действий администраторов АБС (без вмешательства в их действия) и пользователей, а также полномочия и технические средства по настройке для каждого пользователя параметров системы, определяющих права доступа к информации.

Не допускается совмещение в одном лице функций администратора АБС и администратора информационной безопасности АБС.

Обеспечение информационной безопасности автоматизированных банковских систем на стадиях жизненного цикла

ИБ АБС должна обеспечиваться на всех стадиях жизненного цикла (ЖЦ) АБС, автоматизирующих банковские технологические процессы, с учетом всех сторон, вовлеченных в процессы ЖЦ (разработчиков, заказчиков, поставщиков продуктов и услуг, эксплуатирующих и надзорных подразделений организации).

Разработка технических заданий, проектирование, создание и тестирование и приемка средств и систем защиты АБС должны осуществляться по согласованию с ПБоИБ.

Ввод в действие, эксплуатация, снятие с эксплуатации АБС в части вопросов ИБ должны осуществляться при участии ПБоИБ.

На стадиях, связанных с разработкой АБС (определение требований заинтересованных сторон, анализ требований, архитектурное проектирование, реализация, интеграция и верификация, поставка, ввод в действие), разработчиком должна быть обеспечена защита от угроз:

1. Неверной формулировки требований к АБС.
2. Выбора неадекватной модели ЖЦ АБС, в том числе неадекватного выбора процессов ЖЦ и вовлеченных в них участников.
3. Принятия неверных проектных решений.
4. Внесения разработчиком дефектов на уровне архитектурных решений.
5. Внесения разработчиком недокументированных возможностей в АБС.
6. Неадекватной (неполной, противоречивой, некорректной и пр.) реализации требований к АБС.
7. Разработки некачественной документации.
8. Сборки АБС разработчиком/производителем с нарушением требований, что приводит к появлению недокументированных возможностей в АБС либо к неадекватной реализации требований.
9. Неверного конфигурирования АБС.
10. Приемки АБС, не отвечающей требованиям Заказчика.
11. Внесения недокументированных возможностей в АБС в процессе проведения приемочных испытаний посредством недокументированных возможностей функциональных тестов и тестов ИБ.

Привлекаемые для разработки и производства средств и систем защиты АБС на договорной основе специализированные организации должны иметь лицензии на данный вид деятельности в соответствии с законодательством РФ.

При приобретении Банком готовых АБС и их компонентов разработчиком должна быть предоставлена документация, содержащая, в том числе описание защитных мер, предпринятых разработчиком в отношении угроз.

Также разработчиком должна быть представлена документация, содержащая описание защитных мер, предпринятых разработчиком АБС, и их компонентов относительно безопасности разработки, безопасности поставки и эксплуатации, поддержки жизненного цикла, включая описание модели жизненного цикла, оценки уязвимости. Данная документация может быть представлена в рамках декларации о соответствии или быть результатом оценки соответствия изделия, проведенной в рамках соответствующей системы оценки.

В договор о поставке АБС и их компонентов Банку рекомендуется включать положения по сопровождению поставляемых изделий на весь срок их службы. В случае невозможности включения в договор (контракт) указанных требований к разработчику должна быть рассмотрена возможность приобретения полного комплекта рабочей конструкторской документации на изделие, обеспечивающего возможность сопровождения АБС и их компонентов без участия разработчика. Если оба указанных варианта неприемлемы, например, вследствие высокой стоимости, руководство Банка должно обеспечить анализ влияния угрозы невозможности сопровождения АБС и их компонентов на обеспечение непрерывности бизнеса.

На стадии эксплуатации в соответствии с документом ISO TR 13569 должна быть обеспечена защита от следующих угроз:

1. Умышленное несанкционированное раскрытие, модификация или уничтожение информации.
2. Неумышленная модификация или уничтожение информации.
3. Недоставка или ошибочная доставка информации.
4. Отказ в обслуживании или ухудшение обслуживания.
5. Отказ от авторства сообщения или выполненной операции.

На стадии сопровождения должна быть обеспечена защита от угроз:

1. Внесения изменений в АБС, приводящих к нарушению ее функциональности либо к появлению недокументированных возможностей.
2. Невнесения разработчиком/поставщиком изменений, необходимых для поддержки правильного функционирования и правильного состояния АБС.

На стадии снятия с эксплуатации должно быть обеспечено удаление информации, несанкционированное использование которой может нанести ущерб деятельности организации, и информации, используемой средствами обеспечения ИБ, из постоянной памяти АБС или с внешних носителей.

Требования ИБ должны включаться во все договоры и контракты на проведение работ или оказание услуг на всех стадиях ЖЦ АБС.

Порядок организации работ по Информационной Безопасности

Для всех подразделений, входящих в область действия СУИБ Банка, должен быть разработан Порядок организации работ – документы, регламентирующие организацию процессов обеспечения ИБ.

Для разработки Порядка организации работ следует:

1. На основе общей политики ИБ Банка разработать необходимые локальные политики ИБ уровня подразделения, а также частные политики. Должна быть проведена детализация требований политики ИБ Банка с учетом специфики организации.
2. Разработать схему реализации организационной структуры СУИБ. Все роли, используемые в модели, должны быть назначены внутри существующей организационной структуры. В случае ее недостаточности, должен быть рассмотрен вопрос о внесении необходимых изменений.
3. Адаптировать процессно-ролевую модель с учетом специфики организации и разработать детальную реализацию процессов и входящих в них процедур. Должен быть определен перечень процессов, реализуемых в организации, и перечень процессов, отдаваемых на аутсорсинг. Должен быть определен перечень документируемых процедур.
4. Определить перечень обязанностей для каждой роли.

Нормативные ссылки

* 1. Стандарт Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения" СТО БР ИББС-1.0-2006 (принят распоряжением ЦБР от 26 января 2006 года № Р-27).
  2. Pекомендации в области стандартизации Банка России РС БР ИББС-2.0-2007 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0".
  3. Стандарт Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Руководство по самооценке соответствия ИБ организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0".
  4. ГОСТ Р 1.0-2004 "Стандартизация в Российской Федерации. Основные положения".
  5. ГОСТ Р 1.4-2004 "Стандартизация в Российской Федерации. Стандарты организаций. Общие положения".
  6. ГОСТ 34.601-90 "Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания".
  7. ГОСТ Р 51898-2002 "Аспекты безопасности. Правила включения в стандарты".
  8. ГОСТ Р ИСО 9001-2001 "Система менеджмента качества. Требования".
  9. ГОСТ Р ИСО 14001-98 "Система управления окружающей средой. Требования и руководство по применению".
  10. ГОСТ Р ИСО/МЭК 15408-1ч3-2002 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий".
  11. ГОСТ Р ИСО/МЭК 12207-99 "Информационная технология. Процессы жизненного цикла программных средств".
  12. ГОСТ Р ИСО/МЭК ТО 15271-2002 "Информационная технология. Руководство по применению ГОСТ Р ИСО/МЭК 12207 (Процессы жизненного цикла программных средств)".
  13. ISO/IEC IS 13335-1÷2 "Information Technology. Security techniques. Management of information and communications technology security".
  14. ISO TR 13569 "Banking and related financial services. Information security guidelines".
  15. ISO/IEC IS 15288-2002 "Systems engineering. System Life Cycle Processes".
  16. ISO/IEC TR 15504-1÷5 "Information technology. Process assessment".
  17. ISO/IEC TR 18028-1÷5 "Information technology. Security techniques. IT network security".
  18. ISO/IEC TR 18043 "Information technology. Selection, deployment and operations of intrusion detection systems (IDS)".
  19. ISO/IEC TR 18044-2004 "Information Technology. Security techniques. Information security incident management".
  20. ISO/IEC IS 17799-2005 (second edition) (с 2007 года — ISO/IEC IS 27002) "Information Technology. Code of practice for information security management".
  21. BS 7799-2-2002 "Information security management systems. Specification with guidance for use".
  22. ISO/IEC IS 27001-2005 "Information technology. Security techniques. Information security management systems. Requirements".
  23. ITU-T Recommendation X.1051 "Information security management system. Requirements for telecommunications (ISMS-T)".
  24. BSI PAS-56 "Guide to Business Continuity Management (BCM)".
  25. COBIT "Control Objectives for Information and related Technology", 3rd Edition, July 2000.
  26. OCTAVE "Operationally Critical Threat, Asset, and Vulnerability Evaluation".
  27. CRAMM UK "Government’s Risk Analysis and Management Method".