Об утверждении Правил по обеспечению безопасности информационных систем банков второго уровня и организаций, осуществляющих отдельные виды банковских операций

Утративший силу

Постановление Правления Национального Банка Республики Казахстан от 31 марта 2001 года N 80 Зарегистрирован в Министерстве юстиции Республики Казахстан 18.05.2001 г. за N 1517. Утратило силу постановлением Правления Национального Банка Республики Казахстан от 27 марта 2018 года № 48 (вводится в действие с 01.12.2018)

Сноска. Утратило силу постановлением Правления Национального Банка РК от 27.03.2018 № 48 (вводится в действие с 01.12.2018).

В целях урегулирования порядка проведения работ по обеспечению безопасности информационных систем банков второго уровня и организаций, осуществляющих отдельные виды банковских операций, Правление Национального Банка Республики Казахстан постановляет:

1. Утвердить прилагаемые Правила по обеспечению безопасности информационных систем банков второго уровня и организаций, осуществляющих отдельные виды банковских операций, и ввести их и настоящее постановление в действие по истечении четырнадцатидневного срока со дня государственной регистрации в Министерстве юстиции Республики Казахстан.

2. Департаменту информационных технологий (Молчанов С.Н.):

1) совместно с Юридическим департаментом (Шарипов С.Б.) принять меры к государственной регистрации в Министерстве юстиции Республики Казахстан настоящего постановления и Правил по обеспечению безопасности информационных систем банков второго уровня и организаций, осуществляющих отдельные виды банковских операций (далее - Правила);

2) в десятидневный срок со дня государственной регистрации в Министерстве юстиции Республики Казахстан довести настоящее постановление и утвержденные Правила до сведения всех подразделений центрального аппарата , филиалов, организаций и представительства Национального Банка Республики Казахстан.

3. Руководителям территориальных филиалов Национального Банка Республики Казахстан в четырехдневный срок со дня получения настоящего

постановления и утвержденных Правил довести их до сведения банков второго уровня и организаций, осуществляющих отдельные виды банковских операций, за исключением ломбардов и обменных пунктов.

4. Центральному филиалу Национального Банка Республики Казахстан (г. Астана) (Сейфуллин М.Х.) в четырехдневный срок со дня получения настоящего постановления и утвержденных Правил довести их до сведения Комитета Казначейства Министерства финансов Республики Казахстан.

5. Контроль за исполнением настоящего постановления возложить на заместителей Председателя Национального Банка Республики Казахстан Абдулину Н.К. (по пункту 2) и Таджиякова Б.Ш. (по пунктам 3 и 4).

Председатель
Национального Банка

Утверждены
постановлением Правления
Национального Банка
Республики Казахстан
от 31 марта 2001 года
N 80

Правила по обеспечению безопасности информационных систем банков второго уровня и организаций, осуществляющих отдельные виды банковских операций

Глава 1. Общие положения

1. Правила по обеспечению безопасности информационных систем банков второго уровня и организаций, осуществляющих отдельные виды банковских операций (далее - Правила), определяют цели, стратегию и общую политику безопасности информационных систем банков второго уровня и организаций, осуществляющих отдельные виды банковских операций (далее - банковские организации).

2. Правила разработаны в соответствии с нормативными правовыми актами Республики Казахстан и определяют виды угроз безопасности информационных систем, ресурсы, подлежащие защите, а также основные направления реализации системы безопасности, включая организационные и программно-технические меры защиты.

3. Нормы Правил обязательны для применения банковскими организациями, за исключением ломбардов и обменных пунктов.

Глава 2. Основные понятия, используемые в Правилах

4. В Правилах используются следующие понятия:

1) информационная безопасность - защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, утечки, хищения, утраты, уничтожения, искажения, копирования, подделки, блокирования и других угроз, возникающих в результате несанкционированного доступа;

2) защита информации - комплекс мероприятий, обеспечивающих информационную безопасность;

3) система безопасности - комплекс организационных мер и программно-технических средств защиты информации;

4) зловредное программное обеспечение (компьютерные вирусы) - совокупность выполняемого кода, способная создавать свои копии (частично или полностью совпадающие с оригиналом) и внедрять их в различные объекты/ ресурсы компьютерных систем, сетей без ведома пользователя. При этом копии сохраняют способность дальнейшего распространения, нарушают нормальную работу информационной системы и/или оборудования, зачастую приводят к потере данных информационных систем;

5) информационные системы - организационно упорядоченная совокупность документов, систем технических средств и способов обработки информации;

6) политика безопасности - нормы и практические приемы, регулирующие управление, защиту и распределение информации ограниченного распространения;

7) уникальность - единственность в своем роде, свойство неповторяемости в границах конкретной информационной системы;

8) идентификатор - уникальные персональный код или имя, присвоенные субъекту и/или объекту системы, и предназначенные для регламентированного доступа в систему и/или к ресурсам системы;

9) идентификация - присвоение или определение соответствия предъявленного для получения доступа в систему и/или к ресурсу системы идентификатора перечню идентификаторов, имеющихся в системе;

10) аутентификация - подтверждение подлинности субъекта или объекта доступа путем определения соответствия предъявленных реквизитов доступа имеющимся в системе;

11) раскрытие информации (данных, программного обеспечения, информационных сообщений) - действие, происходящее в результате получения несанкционированного доступа к информации и возможного раскрытия полученных сведений случайным или неавторизованным намеренным образом;

12) метка безопасности - степень закрытости информации, состоящая из уровня секретности и категории предметной области, к которой относятся данные.

Глава 3. Основные цели системы безопасности

5. Целью системы безопасности является обеспечение устойчивого функционирования информационных систем банковских организаций, предотвращение возможности совершения финансовых преступлений при помощи вычислительных и телекоммуникационных средств, утраты, утечки, искажения и уничтожения информации ограниченного распространения.

6. Система безопасности информационных систем банковских организаций должна обеспечивать:

1) конфиденциальность информации - защиту от раскрытия в ходе ее хранения, обработки или при передаче по коммуникационным каналам;

2) сохранность информации - защиту от повреждений, целостность и защищенность от несанкционированного изменения, дополнения, копирования или удаления в ходе ее хранения, обработки или при передаче по коммуникационным каналам;

3) доступность - защиту от перехвата информационных сообщений и/или данных с последующей их задержкой, а также от использования одним пользователем данных и иных ресурсов информационной системы, предназначенных для совместного использования.

Глава 4. Политика безопасности

7. В каждой банковской организации должна быть разработана политика безопасности, утверждаемая ее соответствующим органом управления и определяющая наиболее эффективный способ использования вычислительных и коммуникационных ресурсов и информации, а также разработаны процедуры по обеспечению режима безопасности.

8. Политика безопасности определяет:

1) общие направления работы в области информационной безопасности;

2) цель защиты информационной системы;

3) общие требования к защите информационной системы в целом и отдельным ее частям;

4) закрепление должностных лиц банковских организаций, ответственных за разработку необходимых требований, определяющих политику безопасности;

5) закрепление подразделений банковских организаций, ответственных за создание и поддержание работоспособности информационных систем и системы их защиты.

9. Целью политики безопасности является обеспечение устойчивости функционирования информационной системы и сохранности информации.

10. Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы банковской организации и содержит:

1) описание состава информационной системы;

2) список пользователей информационной системы организации, их права и приоритеты (в зависимости от их служебного положения и характера выполняемых функций) на доступ к информации, программным и техническим средствам.

Глава 5. Оценка рисков

11. Ключевым компонентом формирования политики безопасности является оценка рисков, позволяющая определить объекты системы безопасности и оптимальный объем материальных ресурсов, необходимый для защиты информации.

12. Для оценки рисков, являющихся предметом информационной безопасности, должностными лицами и ответственными подразделениями банковских организаций проводится анализ угроз безопасности информационных систем: характер принимаемых во внимание угроз (спектр воздействия угроз). Процесс анализа рисков состоит из двух этапов:

1) идентификация объектов информационных систем;

2) определение угроз.

13. При идентификации объектов информационных систем составляется список объектов, нуждающихся в защите:

1) технические средства - компьютеры (серверы и рабочие станции), периферийные устройства, внешние интерфейсы, кабельная система, активное сетевое оборудование (мосты, маршрутизаторы и экраны);

2) программное обеспечение - операционные системы (сетевые, серверные и клиентские), прикладное программное обеспечение, исходные тексты, объектные модули, служебные программы, средства управления сетью и отдельными системами;

3) информация - обрабатываемая, передаваемая по каналам связи, сохраненная (архив, резервная копия, база данных, регистрационный журнал и прочие данные);

4) документация - на общесистемное и прикладное программное обеспечение, компьютерное и телекоммуникационное оборудование и иные технические средства, на административные процедуры;

5) носители информации - бумажные, магнитные, оптические и другие носители.

В процессе идентификации формируется список, определяющий регламентированный доступ к информационным ресурсам - пользователей, обслуживающего персонала и спектр их прав.

14. Должностными лицами банковских организаций при определении угроз необходимо проведение оценки размера возможного ущерба от:

1) несанкционированного доступа к объектам, нуждающимся в защите, со стороны сторонних организаций и лиц;

2) утечки конфиденциальной информации через технические средства обеспечения производственной деятельности различного характера и исполнения ;

3) потери информации вследствие непреднамеренных ошибок пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы.

15. Угрозы информационным ресурсам могут быть реализованы путем:

1) несанкционированного доступа и съема информации ограниченного распространения;

2) подкупа лиц, работающих в организации или структурах, непосредственно связанных с их деятельностью;

3) перехвата информации, циркулирующей в средствах и системах связи и вычислительной технике, с помощью технических средств обнаружения и съема информации, несанкционированного доступа к информации и преднамеренных воздействий на нее программными и инструментальными средствами в процессе обработки, передачи и хранения;

4) разрушения данных и программного обеспечения зловредным программным обеспечением;

5) неавторизованной передачи и/или получения информации (сведений) ограниченного распространения.

16. После анализа рисков и разработки политики безопасности должностными лицами банковских организаций осуществляется выбор эффективных и экономичных защитных механизмов и составляется план защиты информации.

Глава 6. Реализация плана защиты информации

17. План защиты информации включает следующие меры:

1) организационные;

2) программно-технические.

18. Для построения эффективных систем защиты информационных систем в банковских организациях должны использоваться следующие основные принципы и подходы:

1) идентификация пользователей - каждый пользователь информационной системы должен иметь свой индивидуальный, уникальный идентификатор (в рамках соответствующей подсистемы регистрации), либо единый для нескольких или всех автоматизированных систем;

2) ограничение по доступу - пользователю или группе пользователей предоставляется соответствующий уровень доступа к различным данным, группам данных или ресурсам;

3) подготовка персонала - банковские организации должны обеспечивать обязательное периодическое обучение всех работников, участвующих в управлении, использовании или функционировании системы защиты информации;

4) централизованное администрирование информационной системы - в каждой информационной системе банковских организаций соответствующим распоряжением должен быть назначен администратор безопасности информационной системы;

5) чистота программного обеспечения - используемое прикладное и общесистемное программное обеспечение должно иметь лицензию, приобретаться у сертифицированных поставщиков программного обеспечения или быть сертифицировано в соответствии с нормативными правовыми актами Республики Казахстан;

6) использование качественных услуг - для разработки и установки средств и систем защиты информационных систем должны привлекаться на договорной основе только специализированные организации, имеющие лицензии (сертификаты) на указанные виды деятельности.

Параграф 1. Организационные меры обеспечения информационной безопасности

19. Организационные меры должны обеспечивать соблюдение нормативных правовых актов Республики Казахстан и внутренних требований банковской организации, отслеживание состояния безопасности внутри организации, реагирование на случаи нарушений, развитие защитных мер с учетом изменений в организации.

20. К организационным мерам обеспечения безопасности относятся следующие мероприятия:

1) физическая защита информационных систем;

2) поддержание работоспособности информационных систем, имеющих отношение к информационной безопасности;

3) разделение обязанностей при выполнении действий по изменению данных информационной системы и подтверждения (санкционирования) их необходимости не менее 2 (двумя) сотрудниками;

4) установление каждому пользователю соответствующего права доступа, необходимого для выполнения им возложенных должностных обязанностей и обеспечения взаимозаменяемости;

5) реагирование ответственных лиц на нарушения режима информационной безопасности;

6) планирование восстановительных работ.

21. Физическая защита подразделяется на:

1) физическое управление доступом;

2) меры противопожарной безопасности;

3) защита поддерживающей инфраструктуры;

4) защита от перехвата данных, защита мобильных систем.

22. Мероприятия по поддержанию работоспособности информационных систем подразделяются на:

1) поддержку пользователей - организация консультаций по вопросам информационной безопасности, выявление их типичных ошибок и обеспечение памятками с рекомендациями для распространенных ситуаций;

2) поддержку программного обеспечения - контроль лицензионной (сертифицированной) чистоты программного обеспечения;

3) конфигурационное управление - контроль и фиксирование изменений, вносимых в программную и техническую конфигурацию;

4) резервное копирование для восстановления информационной системы и данных в случае аварии и других обстоятельств непреодолимой силы;

5) управление носителями данных - правила учета, обращения и хранения;

6) документирование - актуальное отражение текущего состояния дел.

23. В случае нарушения режима безопасности информационных систем ответственные лица банковских организаций обязаны осуществлять:

1) выполнение оперативных мероприятий с целью уменьшения наносимого вреда - выявление лица, совершившего несанкционированный доступ и его блокирование;

2) обзор накопленной статистики нарушений - анализ инцидента,выявление повторных нарушений, разработка мер по усовершенствованию системы защиты.

24. Резервное копирование и восстановление после потери работоспособности информационной системы определяются требованиями, установленными в банковской организации.

Параграф 2. Программно-технические меры обеспечения информационной безопасности

25. Программно-технические меры по обеспечению информационной безопасности банковской организации должны включать в себя систему:

1) управления доступом;

2) протоколирования и проверки технического состояния;

3) криптографической защиты данных.

26. Система управления доступом должна обеспечивать выполнение следующих мероприятий:

1) определение перечня групп данных, задач и установления им уровня секретности;

2) установление способов и процедур защиты каждой группы данных;

3) определение групп пользователей информационных систем и разбиение их на категории по выполняемым функциям и установление им уровней доступа к информации;

4) установление порядка идентификации категории пользователей;

5) определение категории доступа для каждой пары "категория пользователей - тип данных";

6) идентификация и аутентификация пользователей при входе в систему по специальным устройствам (жетонам, картам, электронным ключам) и паролю временного действия длиной не менее восьми буквенно-цифровых символов;

7) аппаратная идентификация и аутентификация терминалов, персональных компьютеров, узлов компьютерной сети, каналов связи, внешних устройств вычислительных машин по уникальным встроенным устройствам;

8) идентификация и аутентификация программ, именованных дисковых пространств (томов логических дисков, каталогов, файлов), записей, полей записей по именам и контрольным суммам (паролям, ключам);

9) управление потоками информации с помощью меток безопасности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на него информации.

27. С момента установления пользователям, группе пользователей, обслуживающему персоналу прав доступа к ресурсам информационной системы программно-техническими средствами системы ведется протоколирование, сбор и накопление информации о происходящих в системе событий.

28. В процессе протоколирования событий системы записывается следующая информация:

1) дата и время события;

2) идентификатор инициатора события;

3) тип события;

4) результат действия (успех или неудача);

5) источник запроса (имя терминала);

6) имена затронутых объектов (открываемых, копируемых или удаляемых файлов);

7) описание изменений, внесенных в базы данных защиты (новая метка безопасности объекта);

8) метки безопасности субъектов и объектов события.

29. Результаты протоколирования используются для последующих проверок технического состояния системы.

30. Проверка технического состояния накопленной информации с целью контроля, проводится должностными лицами банковских организаций ежедневно для облегчения обнаружения нарушения безопасности, выявления причин возникновения.

31. К числу событий, затрагивающих безопасность информационной системы и требующих проверки, относятся:

1) вход в систему (успешный или нет);

2) выход из системы;

3) обращение к удаленной системе;

4) операции с файлами (открыть, закрыть, переименовать, удалить, копировать);

5) изменение уровня доступа или иных атрибутов безопасности (режима доступа, права доступа пользователя к информационным ресурсам).

32. В целях обеспечения конфиденциальности информации необходимо выполнять криптографическими средствами и/или системами шифрование данной информации при осуществлении:

1) записи на разделяемые носители данных (совместно используемые различными пользователями и группами пользователей);

2) передачи по каналам связи;

3) создании рабочих, архивных и резервных копий на любых съемных носителях данных долговременного хранения.

33. Для шифрования (расшифровки) информации, принадлежащей различным пользователям (группам пользователей), необходимо использовать различные криптографические ключи.

34. Операция шифрования (расшифровки) информации может выполняться только пользователями и/или группами пользователей, имеющими специальный доступ к соответствующим криптографическим ключам.

35. Организация и контроль работ по шифрованию (расшифровке) ведется ответственным лицом банковской организации, который выполняет:

1) учет, хранение и сопровождение программных средств криптографирования;

2) генерацию криптографических ключей, учет, хранение и выдачу информационных носителей, содержащих ключи;

3) ведение списка владельцев криптографических ключей;

4) обеспечение владельцев криптографических ключей необходимыми инструкциями.

Глава 7. Технология и документирование процесса разработки информационных систем

36. Процесс разработки, внедрения и сопровождения информационных систем в банковских организациях должен включать определение этапов разработки, порядка внесения изменений, приема, тестирования и ввода в промышленную эксплуатацию, требования к документированию всех этапов.

37. Разработка, внедрение и сопровождение информационных систем в банковских организациях выполняется в соответствии с действующим на территории Республики Казахстан стандартами информационных технологий и требованиями, установленными в банковской организации.

38. Разработка информационных систем должна выполняться на основании технического задания на систему, утвержденного соответствующим органом управления банковской организации, и в строгом соответствии с этапами проектирования.

39. Программное обеспечение информационной системы, находящейся в промышленной эксплуатации, должно поддерживаться в неизменном виде.

40. В целях исключения несанкционированного изменения программного обеспечения и/или данных информационной системы при необходимости внесения изменений (для устранения недостатков или доработки системы) в программное обеспечение, процесс внесения изменений и его документирования осуществляются в соответствии с техническим заданием, стандартами информационных технологий, действующими на территории Республики Казахстан, и внутренними требованиями, установленными в банковской организации.

Глава 8. Контроль и ответственность

41. Контроль за разработкой политики безопасности и соблюдением норм Правил осуществляется должностными лицами банковской организации.

42. Ответственность за реальное исполнение политики безопасности должна возлагаться на специально назначенных ответственных исполнителей.

43. Ответственность за соблюдение информационной безопасности банковских организаций, как правило в соответствии с должностными обязанностями, несут:

1) первые руководители;

2) руководители подразделений, ответственные за создание и поддержание работоспособности информационных систем и системы их защиты, обеспечивающие доведение политики безопасности до пользователей и контакты с пользователями;

3) администраторы безопасности информационных систем, обеспечивающие непрерывное функционирование информационных систем и реализацию технических мер, необходимых для проведения в жизнь политики безопасности;

4) пользователи, несущие ответственность за использование информационной системы в соответствии с политикой безопасности, обязаны подчиняться распоряжениям лиц, отвечающих за отдельные аспекты безопасности, ставить в известность руководство обо всех подозрительных ситуациях.

44. Должностные лица банковских организаций:

1) осуществляют проведение анализа рисков, выявление объектов, требующих защиты, и уязвимых мест информационных систем, оценивая размер возможного ущерба от нарушения режима безопасности и выбирая эффективные средства защиты;

2) обеспечивают проведение обучения персонала мерам безопасности и правилам поведения в чрезвычайных (экстренных) ситуациях, путем обращения особого внимания на вопросы, связанные с антивирусным контролем и правильным вхождением в систему (с указанием при регистрации только своего идентификатора);

3) в случае перевода какого-либо работника в другое подразделение, нахождения в отпуске, в командировке либо увольнении, обеспечивают незамедлительное информирование об этом специально назначенных ответственных исполнителей и администраторов безопасности информационных систем.

45. Администраторы безопасности информационных систем выполняют работы по ежедневному управлению и поддержанию работоспособности и непрерывного функционирования системы защиты.

46. Администраторы безопасности информационных систем обязаны:

1) обеспечивать обязательность процедуры идентификации и аутентификации для доступа к ресурсам информационных систем;

2) не допускать получения права доступа к информационным ресурсам неавторизованными пользователями, представлять пользователям входные имена и начальные пароли только после заполнения регистрационных форм;

3) контролировать регулярность выполнения резервного копирования информации, обрабатываемой информационной системой;

4) проводить плановую и внеплановую проверку надежности защиты ресурсов системы, информировать специально назначенных ответственных исполнителей об эффективности существующей политики безопасности и вносить на их рассмотрение предложения об улучшении системы защиты;

5) обеспечивать защиту оборудования корпоративной сети, в том числе специальных межсетевых программных средств;

6) оперативно и эффективно реагировать на события, содержащие угрозу, принимать меры по отражению угрозы и выявлению нарушителей, фиксировать и информировать специально назначенных ответственных исполнителей о попытках нарушения защиты;

7) использовать проверенные программно-технические средства отслеживания процесса функционирования информационной системы с целью обнаружения подозрительных ситуаций, наличия зловредного программного обеспечения и его влияния на работу информационной системы и ее компонентов;

8) ежедневно анализировать регистрационную информацию, относящуюся к информационной системе в целом и к файловым серверам, в особенности;

9) проводить обзор новинок в области информационной безопасности, информировать о них пользователей и специально назначенных ответственных исполнителей.

47. Администраторы безопасности информационных систем не вправе использовать данные им полномочия в корыстных целях или со злым умыслом.

48. Работники подразделений банковских организаций (пользователи) обязаны:

1) знать и соблюдать внутренние требования, обеспечивающие безопасность информационных систем;

2) использовать доступные зарегистрированные защитные механизмы для обеспечения конфиденциальности и целостности своей информации;

3) выбирать личные пароли длиной не менее восьми буквенно-цифровых символов;

4) обеспечивать недоступность личных паролей другим лицам;

5) информировать администраторов безопасности информационных систем и/или специально назначенных ответственных исполнителей о нарушениях безопасности и иных подозрительных ситуациях;

6) в случае обнаружения слабых мест в защите ресурсов информационных систем, незамедлительно сообщать об этом администраторам безопасности информационных систем и/или специально назначенным ответственным исполнителям;

7) обеспечивать представление корректной идентификационной и аутентификационной информации;

8) обеспечивать резервное копирование информации с жесткого диска своего компьютера;

9) выполнять процедуры для предупреждения проникновения опасного кода, для его обнаружения и уничтожения;

10) выполнять нормы поведения в экстренных ситуациях,последовательность действий при ликвидации последствий аварий и иных обстоятельств непреодолимой силы.

49. Работники подразделений банковских организаций (пользователи) не вправе совершать неавторизованную работу с данными информационных систем , создавать помехи другим пользователям, осуществлять попытку работать от имени других пользователей.

50. Национальный Банк осуществляет контроль за применением требований Правил в период проверок деятельности банковских организаций в рамках его полномочий, установленных действующим законодательством Республики Казахстан.

Председатель
Национального Банка