РЕКОМЕНДАЦИИ В ОБЛАСТИ
СТАНДАРТИЗАЦИИ
БАНКА РОССИИ

РС БР ИББС-2.9-2016

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРЕДОТВРАЩЕНИЕ УТЕЧЕК ИНФОРМАЦИИ

Дата введения: 2016-05-01

Москва
2016

Предисловие

1. ПРИНЯТЫ И ВВЕДЕНЫ в действие Приказом Банка России от 11 апреля 2016 года № ОД-1205.

2. ВВЕДЕНЫ ВПЕРВЫЕ.

Содержание

Введение

В соответствии с действующим стандартом Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения” (далее – СТО БР ИББС-1.0) организациям банковской системы Российской Федерации (далее – БС РФ) следует принимать меры по обеспечению конфиденциальности обрабатываемой информации.

Наибольшими возможностями для нанесения ущерба, в том числе неумышленного, организации БС РФ и (или) ее клиентам в части возможного нарушения конфиденциальности обрабатываемой информации обладают работники организации БС РФ и (или) иные лица, обладающие легальным доступом к информации, – возможные внутренние нарушители информационной безопасности. При этом утечка информации является одной из актуальных угроз нарушения информационной безопасности (далее – ИБ), которую могут реализовать возможные внутренние нарушители ИБ.

Одним из направлений деятельности организации БС РФ по обеспечению конфиденциальности обрабатываемой информации являются мониторинг и контроль информационных потоков, осуществляемые для предотвращения утечек информации. Настоящий документ устанавливает рекомендации, реализация которых направлена на обеспечение организацией БС РФ мониторинга и контроля информационных потоков, осуществляемых для выявления и предотвращения утечек информации в результате действия работников организации БС РФ и (или) иных лиц, обладающих легальным доступом к информации, – возможных внутренних нарушителей ИБ.

РЕКОМЕНДАЦИИ В ОБЛАСТИ СТАНДАРТИЗАЦИИ БАНКА РОССИИ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРЕДОТВРАЩЕНИЕ УТЕЧЕК ИНФОРМАЦИИ

Дата введения 2016–05–01

1. Область применения

Настоящие рекомендации распространяются на организации БС РФ, по результатам оценки рисков принявшие решения проводить деятельность по предотвращению утечек информации конфиденциального характера, не содержащей сведения, составляющие государственную тайну, в результате действия работников организации БС РФ и (или) иных лиц, обладающих легальным доступом к информации или легальным физическим доступом в помещения, в которых осуществляется обработка информации, – возможных внутренних нарушителей ИБ.

В настоящем документе содержатся рекомендации, выполнение которых обеспечивает снижение рисков утечки информации путем мониторинга и контроля информационных потоков. В настоящем документе не рассматриваются рекомендации, выполнение которых косвенно влияет на снижение рисков утечки информации (например, рекомендации к обеспечению защиты от воздействия вредоносного кода, межсетевому экранированию и разделению вычислительных сетей, к проведению аудитов ИБ, к организации логического доступа).

Настоящие рекомендации не распространяются на организации БС РФ, решением которых обработка информации осуществляется с использованием облачных технологий или передана на аутсорсинг сторонней организации.

Настоящие рекомендации не включают положения, направленные на предотвращение утечек информации по техническим каналам, в том числе каналам побочных электромагнитных излучений и наводок, а также в результате действия работников организации БС РФ и иных лиц, не обладающих легальным доступом к информации или легальным физическим доступом в помещения, в которых осуществляется обработка информации, – внешних нарушителей ИБ.

Настоящий документ рекомендован для применения путем прямого использования устанавливаемых в нем положений при проведении деятельности по предотвращению утечек информации, а также путем включения ссылок на него и (или) прямого включения содержащихся в нем положений во внутренние документы организации БС РФ.

Положения настоящих рекомендаций применяются на добровольной основе. В конкретной организации БС РФ для проведения деятельности по предотвращению утечек информации могут использоваться иные рекомендации и (или) требования, отражающие специфику и сложившуюся практику организации БС РФ.

2. Нормативные ссылки

В настоящих рекомендациях в области стандартизации Банка России использованы нормативные ссылки на следующие документы:

СТО БР ИББС-1.0.

РС БР ИББС-2.5 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности” (далее – РС БР ИББС-2.5).

РС БР ИББС-2.7 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Ресурсное обеспечение информационной безопасности” (далее – РС БР ИББС-2.7).

3. Термины и определения

В настоящих рекомендациях применяются термины в соответствии с СТО БР ИББС-1.0, РС БР ИББС-2.5, РС БР ИББС-2.7, а также следующие термины с соответствующими определениями:

3.1. **Обработка информации** – любое действие (операция) или совокупность действий (операций), включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение информации.

3.2. **Утечка информации** – несанкционированное предоставление или распространение информации конфиденциального характера, не контролируемое организацией БС РФ.

Примечание.

В настоящем документе рассматриваются только случаи утечки информации, реализуемые в результате действия работников организации БС РФ и (или) иных лиц, обладающих легальным доступом к информации или легальным доступом в помещения, в которых осуществляется обработка информации.

3.3. **Доступ к информации** – возможность получения информации и ее использования.

3.4. **Предоставление информации** – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

3.5. **Распространение информации** – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

3.6. **Защита информации от утечки** – деятельность, направленная на предотвращение неконтролируемого предоставления или распространения информации конфиденциального характера.

3.7. **Информация конфиденциального характера** – информация, для которой в соответствии с законодательством Российской Федерации, в том числе нормативными актами Банка России, и внутренними документами организации БС РФ обеспечивается сохранение свойства конфиденциальности.

3.8. **Возможный внутренний нарушитель ИБ** – работник организации БС РФ и (или) иное физическое лицо, обладающие легальным доступом к информации конфиденциального характера или легальным физическим доступом в помещения, в которых осуществляется обработка информации конфиденциального характера.

3.9. **Владелец информационного актива** – подразделение организации БС РФ и (или) работник организации БС РФ, являющееся инициатором создания информационного актива, определяющее цели сбора и обработки информации, состав обрабатываемой информации, а также осуществляющее распоряжение доступом к информационному активу в пределах своих полномочий.

4. Обозначения и сокращения

АБС – автоматизированная банковская система;
БС – банковская система;
ИБ – информационная безопасность;
РФ – Российская Федерация;
СОИБ – система обеспечения информационной безопасности;
СМИБ – система менеджмента информационной безопасности.

5. Общие положения

5.1. Для защиты информации конфиденциального характера от возможных утечек организации БС РФ рекомендуется обеспечивать:

- идентификацию и формирование перечня категорий информации конфиденциального характера, рекомендации к реализации которых установлены в разделе 6 настоящих рекомендаций;
- идентификацию и учет информационных активов (информационных ресурсов), содержащих информацию конфиденциального характера и объектов среды информационных активов, используемых для обработки и (или) хранения информации конфиденциального характера, рекомендации к реализации которых установлены в разделе 7 настоящих рекомендаций;
- определение категорий возможных внутренних нарушителей и актуальных угроз, связанных с их действиями, – потенциальных каналов утечки информации конфиденциального характера, рекомендации к выполнению которых установлены в разделе 8 настоящих рекомендаций;
- выполнение процессов системы обеспечения ИБ (далее – СОИБ), которые обеспечивают непосредственный мониторинг и контроль информационных потоков – потенциальных каналов утечки информации конфиденциального характера (далее – процессы непосредственного мониторинга и контроля информационных потоков), рекомендации к составу которых установлены в разделе 9 настоящих рекомендаций.

5.2. Организации БС РФ рекомендуется реализовать процессы системы менеджмента ИБ (далее – СМИБ), полнота и качество выполнения которых обеспечивают должный уровень зрелости выполнения процессов непосредственного мониторинга и контроля информационных потоков. Реализацию указанных процессов СМИБ рекомендуется осуществлять с учетом положений РС БР ИББС-2.7 и рекомендаций, установленных в разделе 10 настоящих рекомендаций.

6. Рекомендации к реализации идентификации и формирования перечня категорий информации конфиденциального характера

6.1. Организации БС РФ рекомендуется установить и документировать классификацию обрабатываемой информации. Рекомендуется выделение как минимум двух классов информации, например классов “информация конфиденциального характера” и “открытая информация”. Классификацию рекомендуется проводить на основе оценивания степени тяжести последствий для организации БС РФ от возможных утечек информации конфиденциального характера.

6.2. Организации БС РФ рекомендуется обеспечить документирование и выполнение правил установления перечня категорий информации, включаемых в каждый из классов информации конфиденциального характера. В составе правил установления перечня категорий информации рекомендуется определить:

– обязанность отдельного подразделения, например службы ИБ, организации БС РФ составлять и вести перечень категорий информации для каждого из классов информации конфиденциального характера на основе предложений, формируемых функциональными подразделениями организации БС РФ, в компетенцию которых входит определение целей и правил создания, обработки и (или) сбора соответствующей информации конфиденциального характера;
– обязанность функциональных подразделений организации БС РФ своевременно предоставлять в службу ИБ предложения по перечню категорий информации, включаемых в каждый из классов информации конфиденциального характера;
– порядок проведения пересмотра перечня категорий информации, включаемых в каждый из классов информации конфиденциального характера, например не реже одного раза в год и (или) при возникновении соответствующих предложений функциональных подразделений организаций БС РФ;
– порядок обязательного ознакомления работников организации БС РФ с перечнем категорий информации, включаемых в каждый из классов информации конфиденциального характера, с документальной фиксацией факта такого ознакомления.

Перечень категорий информации, включаемых в каждый из классов информации конфиденциального характера, рекомендуется устанавливать организационным актом (приказом, распоряжением) организации БС РФ.

В случае использования организацией БС РФ двух классов информации возможно определение только перечня категорий информации, которые включаются в класс “информация конфиденциального характера”. В этом случае любая иная информация классифицируется как “открытая информация”.

6.3. При формировании перечня категорий информации, включаемых в класс “информация конфиденциального характера”, следует как минимум рассматривать следующую информацию:

– информация, для которой свойство конфиденциальности обеспечивается в соответствии с требованиями законодательства Российской Федерации, в том числе нормативных актов Банка России:
  • банковская тайна [2];
  • персональные данные [3];
  • информация, защищаемая в соответствии с законодательством о национальной платежной системе [4];
  • инсайдерская информация (за исключением коммерческой и банковской тайн) [5];
  • информация, входящая в состав кредитной истории [6];
  • иная информация, доступ к которой ограничен в соответствии с законодательством Российской Федерации, в том числе нормативными актами Банка России;
– информация, для которой свойство конфиденциальности обеспечивается в соответствии с требованиями внутренних документов организации БС РФ, устанавливаемых среди прочего в соответствии с законодательством о коммерческой тайне [7], в том числе, например:
  • информация об управлении организацией;
  • информация о планировании коммерческой деятельности организации;
  • информация о финансовом состоянии организации;
  • информация об автоматизации деятельности организации;
  • информация организационного характера;
  • информация об обеспечении безопасности и защиты информации организации.

6.4. Примерный состав категорий информации, рекомендуемых для включения в класс “информация конфиденциального характера”, приведен в приложении А к настоящему документу.

7. Рекомендации к реализации идентификации и учета информационных активов информации конфиденциального характера и объектов среды информационных активов, используемых для обработки информации конфиденциального характера

7.1. Организации БС РФ рекомендуется документировать и обеспечить выполнение идентификации и учета всех информационных активов информации конфиденциального характера и объектов среды информационных активов. В составе правил идентификации и учета информационных активов и объектов среды информационных активов рекомендуется определить:

– перечень типов информационных активов и объектов среды информационных активов (средств вычислительной техники и переносных носителей информации), подлежащих идентификации и учету;
– состав учетных данных, хранимых для каждого информационного актива и объекта среды информационного актива;
– обязанность подразделений информатизации и (или) функциональных подразделений организации БС РФ осуществлять идентификацию и учет информационных активов и объектов среды информационных активов;
– способы выполнения подразделениями информатизации и (или) функциональных подразделений организации БС РФ идентификации и учета информационных активов и объектов среды информационных активов, в том числе с использованием средств автоматизации идентификации и учета;
– обязанность службы ИБ организации БС РФ осуществлять контроль соответствия фактического состава информационных активов и объектов среды информационных активов учетным данным;
– способы выполнения службой ИБ контроля фактического состава информационных активов и объектов среды информационных активов, в том числе с использованием средств автоматизации идентификации и контроля;
– правила размещения и (или) запрета размещения информационных активов разных классов информации конфиденциального характера на одном объекте среды информационных активов;
– правила идентификации и учета работниками организации БС РФ носителей информации конфиденциального характера;
– правила обработки работниками организации БС РФ информации конфиденциального характера на бумажных и переносных носителях информации.

7.2. В качестве типов информационных активов, подлежащих идентификации и учету, рекомендуется рассматривать следующие типы:

– базы данных;
– сетевые файловые ресурсы;
– виртуальные машины, предназначенные для размещения серверных компонентов автоматизированных банковских систем (далее – АБС);
– виртуальные машины, предназначенные для размещения автоматизированных рабочих мест пользователей и эксплуатирующего персонала;
– ресурсы доступа, относящиеся к сервисам электронной почты;
– ресурсы доступа, относящиеся к web-сервисам информационно-телекоммуникационной сети “Интернет” (далее – сети Интернет).

7.3. В качестве типов объектов среды информационных активов, подлежащих идентификации и учету, рекомендуется рассматривать следующие:

– серверное оборудование, хранилища данных;
– рабочие станции пользователей и эксплуатационного персонала;
– переносные (портативные) средства вычислительной техники (например, ноутбуки, планшетные компьютеры, смартфоны);
– переносные носители информации (например, CD/DVD/blu-ray-диски, флеш-память, карты памяти, внешние HDD-диски, магнитные ленты);
– бумажные носители информации.

7.4. Для каждого информационного актива рекомендуется обеспечивать хранение как минимум следующих учетных данных:

– данные, позволяющие идентифицировать информационный актив;
– данные, позволяющие установить средство вычислительной техники – объект среды информационного актива;
– данные, устанавливающие класс информации конфиденциального характера информационного актива;
– данные, устанавливающие тип информационного актива, в том числе из числа указанных в пункте 7.2 настоящих рекомендаций;
– данные, определяющие владельца информационного актива.

Класс информации конфиденциального характера информационного актива определяется путем сопоставления фактической информации об информационном активе, предоставляемой (определяемой) его владельцем, с перечнем категорий информации конфиденциального характера, входящих в соответствующий класс.

7.5. Для каждого средства вычислительной техники – объекта среды информационных активов рекомендуется обеспечивать хранение как минимум следующих учетных данных:

– данные, позволяющие идентифицировать средство вычислительной техники;
– данные, позволяющие установить место физического размещения средств вычислительной техники;
– перечень информационных активов, размещенных на средстве вычислительной техники;
– данные, позволяющие идентифицировать логическое размещение средства вычислительной техники, например сетевой адрес, доменное имя;
– данные, устанавливающие тип вычислительной техники, в том числе из числа указанных в пункте 7.3 настоящих рекомендаций;
– данные, устанавливающие класс информации конфиденциального характера, размещенной на средстве вычислительной техники.

7.6. Организациям БС РФ рекомендуется использовать средства автоматизации для выполнения следующих видов деятельности:

– учет информационных активов и средств вычислительной техники – объектов среды информационных активов;
– идентификация информационных активов и средств вычислительной техники для цели контроля соответствия фактического состава информационных активов и объектов среды информационных активов учетным данным.

7.7. Организации БС РФ рекомендуется документировать и обеспечить выполнение работниками правил обработки информации конфиденциального характера на бумажных и переносных носителях информации, предусматривающих среди прочего:

– правила маркировки носителей информации, в том числе бумажных, выполняемой с целью определения класса информации конфиденциального характера;
– правила отнесения информации к конкретным классам информации конфиденциального характера на основе утвержденных перечней категорий информации, включаемых в каждый из классов информации конфиденциального характера;
– правила учета и хранения бумажных и переносных носителей информации, требования к организации доступа к ним;
– правила передачи бумажных и переносных носителей информации, в том числе передачи третьем лицам;
– правила использования переносных носителей информации за пределами объектов организации БС РФ;
– правила безопасного уничтожения бумажных и переносных носителей информации и удаления информации с переносных носителей информации, правила взаимодействия с архивной службой организации БС РФ.

7.8. В части безопасного уничтожения бумажных и переносных носителей информации организации БС РФ рекомендуется:

– физически уничтожать не используемые более переносные носители информации, либо уничтожить, удалить, перезаписать информацию на них с использованием методов, позволяющих сделать исходную информацию невосстанавливаемой, вместо стандартных функций удаления или форматирования;
– установить и использовать средства уничтожения бумажных документов (шредеры) вблизи мест расположения средств печати и копирования информации;
– при необходимости выбирать шредеры исходя из степени конфиденциальности уничтожаемых документов, при этом рекомендуется использовать шредеры с перекрестной резкой.

7.9. В организации БС РФ рекомендуется установить:

– персональную ответственность каждого работника организации БС РФ за соблюдение правил обработки информации в АБС и ответственность руководителей структурных подразделений организации БС РФ за организацию соблюдения указанных правил;
– персональную ответственность каждого работника организации БС РФ за соблюдение правил обработки информации на бумажных и переносных носителях информации и ответственность руководителей структурных подразделений организации БС РФ за организацию соблюдения указанных правил;
– персональную ответственность работников подразделений информатизации и (или) функциональных подразделений за соблюдение правил идентификации и учета информационных активов и средств вычислительной техники – объектов среды информационных активов и ответственность руководителей указанных подразделений за организацию соблюдения указанных правил;
– персональную ответственность работников подразделений информатизации и (или) функциональных подразделений за соблюдение правил размещения и (или) запрета размещения информационных ак-

тивов разных классов на одном средстве вычислительной техники и ответственность руководителей указанных подразделений за организацию соблюдения указанных правил;
– персональную ответственность руководителей службы ИБ за организацию деятельности по осуществлению контроля соответствия фактического состава информационных активов и средств вычислительной техники – объектов среды информационных активов учетным данным.

8. Рекомендации к определению категорий возможных внутренних нарушителей и потенциальных каналов утечки информации

8.1. Организации БС РФ рекомендуется рассматривать следующие категории возможных внутренних нарушителей:
– **Категория А.** Пользователи АБС и приложений – работники организации БС РФ, обладающие возможностями по доступу к информации конфиденциального характера в рамках реализации своих служебных обязанностей. Категорию пользователей АБС целесообразно разделять на следующие группы по уровню доверия:
  • **Категория А1.** Доверенный пользователь (например, высшее руководство организации БС РФ).
  • **Категория А2.** Пользователь (большинство работников организации БС РФ).
  • **Категория А3.** Пользователь “в зоне риска” (например, работники организации БС РФ на испытательном сроке, подавшие заявление на увольнение или ранее участвовавшие в инцидентах ИБ).
– **Категория Б.** Эксплуатационный персонал – лица, в том числе не являющиеся работниками организации БС РФ, обладающие возможностями по доступу к информации конфиденциального характера при осуществлении задач, связанных с эксплуатацией и (или) администрированием информационной инфраструктуры организации БС РФ, АБС и приложений организации БС РФ;
– **Категория В.** Технический и вспомогательный персонал – лица, в том числе не являющиеся работниками организации БС РФ, не обладающие полномочиями по доступу к информации конфиденциального характера, но осуществляющие непосредственный физический доступ в помещения, в которых осуществляется обработка такой информации;
– **Категория Г.** Лица, не являющиеся работниками организации БС РФ, обладающие доступом к информации конфиденциального характера на основании договорных отношений (например, аудиторы, партнеры и подрядчики), требований законодательства Российской Федерации (например, органы государственной власти) и (или) судебного решения.

8.2. Организации БС РФ рекомендуется рассматривать следующие потенциальные каналы утечки информации:
– передача информации за пределы контролируемой информационной инфраструктуры организации БС РФ с применением электронной почты;
– передача информации за пределы контролируемой информационной инфраструктуры организации БС РФ с применением сервисов сети Интернет и беспроводных сетей, в том числе социальных сетей и форумов;
– размещение информации конфиденциального характера на объекте информационной инфраструктуры организации БС РФ, не предназначенном для ее хранения;
– удаленный доступ к информационной инфраструктуре организации БС РФ с использованием сети Интернет;
– копирование информации на переносные носители информации;
– передача информации за пределы объектов организации БС РФ с использованием факсимильной, телефонной и (или) телетайпной связи;
– печать и (или) копирование информации на бумажные носители, в том числе с последующим их выносом за пределы организации БС РФ и (или) передачей информации за пределы объектов организации БС РФ с использованием факсимильной связи;
– использование и (или) утеря переносных носителей информации за пределами информационной инфраструктуры организации БС РФ;
– использование и (или) утеря переносных (портативных) средств вычислительной техники за пределами информационной инфраструктуры организации БС РФ;
– передача (вынос) средств вычислительной техники за пределы организации БС РФ, в том числе для технического обслуживания, ремонта и (или) утилизации;
– визуальное (включая фотографирование и видеосъемку) и слуховое (без использования специализированных технических средств) ознакомление с информацией.

8.3. Организации БС РФ рекомендуется организовать обработку информации конфиденциального характера возможными внутренними нарушителями **категории Г** с использованием только средств вычислительной техники, включенных в область действия процессов мониторинга и контроля потенциальных

каналов утечки информации, рекомендации к составу которых установлены в разделе 9 настоящих рекомендаций.

8.4. Организации БС РФ рекомендуется определить перечень угроз утечки информации конфиденциального характера, в которой необходимо установить потенциальные каналы утечки информации для каждого типа средств вычислительной техники – объекта среды информационных активов, в том числе из числа указанных в пункте 7.3 настоящих рекомендаций, и каждой категории возможных внутренних нарушителей. В качестве перечня угроз утечки информации конфиденциального характера рекомендуется использовать следующий:

Таблица 1. Перечень угроз утечки информации конфиденциального характера

Тип объекта среды	Возможный внутренний нарушитель	Потенциальный канал утечки информации
Серверное оборудование и рабочие станции эксплуатационного персонала	**Категория Б** – эксплуатационный персонал	1. Передача информации за пределы контролируемой информационной инфраструктуры организации БС РФ с применением электронной почты. 2. Передача информации за пределы контролируемой информационной инфраструктуры организации БС РФ с применением сервисов сети Интернет и беспроводных сетей, в том числе социальных сетей и форумов. 3. Удаленный доступ к информационной инфраструктуре организации БС РФ с использованием сети Интернет. 4. Копирование информации на переносные носители информации. 5. Передача (вынос) средств вычислительной техники за пределы организации БС РФ. 6. Визуальное и слуховое ознакомление с информацией.
Рабочие станции пользователей	**Категория А** – пользователи АБС и приложений	1. Передача информации за пределы контролируемой информационной инфраструктуры организации БС РФ с применением электронной почты. 2. Передача информации за пределы контролируемой информационной инфраструктуры организации БС РФ с применением сервисов сети Интернет и беспроводных сетей, в том числе социальных сетей и форумов. 3. Копирование информации на переносные носители информации. 4. Печать и (или) копирование информации на бумажные носители, в том числе с последующим их выносом за пределы организации БС РФ и (или) передачей информации за пределы объектов организации БС РФ с использованием факсимильной связи. 5. Визуальное и слуховое ознакомление с информацией.
	Категория В – технический и вспомогательный персонал	1. Передача (вынос) оборудования средств вычислительной техники за пределы организации БС РФ. 2. Визуальное и слуховое ознакомление с информацией.
	Категория Г – лица, не являющиеся работниками организации БС РФ	1. Передача информации за пределы контролируемой информационной инфраструктуры организации БС РФ с применением электронной почты. 2. Передача информации за пределы контролируемой информационной инфраструктуры организации БС РФ с применением сервисов сети Интернет и беспроводных сетей, в том числе социальных сетей и форумов. 3. Удаленный доступ к информационной инфраструктуре организации БС РФ с использованием сети Интернет. 4. Копирование информации на переносные носители информации. 5. Печать и (или) копирование информации на бумажные носители, в том числе с последующим их выносом за пределы организации БС РФ и (или) передачей информации за пределы объектов организации БС РФ с использованием факсимильной связи. 6. Визуальное и слуховое ознакомление с информацией.

Тип объекта среды	Возможный внутренний нарушитель	Потенциальный канал утечки информации
Переносные носители информации	**Категория А** – пользователи АБС **Категория Б** – эксплуатационный персонал **Категория Г** – лица, не являющиеся работниками организации БС РФ	1. Передача информации за пределы контролируемой информационной инфраструктуры организации БС РФ с применением сервисов сети Интернет и беспроводных сетей, в том числе социальных сетей и форумов. 2. Использование и (или) утеря переносных носителей информации за пределами информационной инфраструктуры организации БС РФ.
Переносные (портативные) средства вычислительной техники	**Категория А** – пользователи АБС **Категория Б** – эксплуатационный персонал **Категория Г** – лица, не являющиеся работниками организации БС РФ	1. Передача информации за пределы контролируемой информационной инфраструктуры организации БС РФ с применением сервисов сети Интернет и беспроводных сетей, в том числе социальных сетей и форумов. 2. Удаленный доступ к информационной инфраструктуре организации БС РФ с использованием сети Интернет. 3. Копирование информации на переносные носители информации. 4. Использование и (или) утеря переносных (портативных) средств вычислительной техники за пределами информационной инфраструктуры организации БС РФ. 5. Визуальное и слуховое ознакомление с информацией.
Бумажные носители информации	**Категория А** – пользователи АБС **Категория Б** – эксплуатационный персонал **Категория В** – технический и вспомогательный персонал **Категория Г** – лица, не являющиеся работниками организации БС РФ	1. Визуальное и слуховое ознакомление с информацией.

8.5. Работы по защите информации от потенциальных каналов утечки рекомендуется проводить с учетом приоритетов их реализации по результатам оценки рисков. Пример рекомендаций по приоритизации выполнения работ по защите информации от потенциальных каналов утечек информации приведен в приложении Б к настоящему документу.

9. Рекомендации к определению состава процессов мониторинга и контроля потенциальных каналов утечки информации

9.1. Состав и реализацию процессов СОИБ, направленных на мониторинг и контроль потенциальных каналов утечки информации, рекомендуется определять в соответствии с принципом “минимума полномочий” возможных внутренних нарушителей ИБ путем:

– блокирования техническими средствами и (или) организационными мерами возможности использования потенциальных каналов утечки информации, использование которых не требуется возможным внутренним нарушителям для выполнения служебных обязанностей;
– регламентирования и реализации процесса предоставления возможности (разблокирования) использования возможными внутренними нарушителями потенциальных каналов утечки информации;
– непрерывного мониторинга и контроля использования возможными внутренними нарушителями разблокированных потенциальных каналов утечки информации.

Пример реализации политики блокирования и непрерывного мониторинга и контроля использования возможными внутренними нарушителями потенциальных каналов утечки информации приведен в Приложении В к настоящему документу.

9.2. События ИБ, выявленные в рамках мониторинга и контроля использования возможными внутренними нарушителями потенциальных каналов утечки информации, рекомендуется обрабатывать в рамках процессов системы менеджмента инцидентов ИБ, реализуемой организацией БС РФ с учетом положений РС БР ИББС-2.5.

9.3. Организациям БС РФ рекомендуется реализовать следующий состав процессов СОИБ, выполнение которых позволит обеспечить мониторинг и контроль потенциальных каналов утечки информации, а также снизить риски утечки информации конфиденциального характера:

– мониторинг, контроль, блокирование использования сервисов электронной почты при передаче информации на внешние адреса электронной почты;

– мониторинг, контроль, блокирование использования беспроводных сетей и сети Интернет с использованием информационной инфраструктуры организации БС РФ;
– мониторинг, контроль, блокирование использования удаленного доступа к информационной инфраструктуре организации БС РФ с использованием сети Интернет;
– мониторинг публикации информации конфиденциального характера в сети Интернет, в том числе социальных сетях и форумах;
– мониторинг, контроль, блокирование копирования информации на переносные носители информации;
– контроль использования средств факсимильной связи;
– контроль (запрет или блокирование) использования личных средств связи (телефоны, смартфоны, планшеты и т.п.);
– мониторинг и контроль печати и (или) копирования информации на бумажных носителях;
– контроль (блокирование) возможности использования и (или) доступа к информации конфиденциального характера на переносных носителях информации за пределами информационной инфраструктуры организации БС РФ;
– блокирование возможности доступа к информации конфиденциального характера на средствах вычислительной техники за пределами информационной инфраструктуры организации БС РФ;
– мониторинг и анализ действий возможных внутренних нарушителей по доступу к информационным активам;
– контроль передачи (выноса) средств вычислительной техники за пределы организации БС РФ;
– контроль физического доступа с целью предотвращения визуального и слухового ознакомления с информацией.

9.4. Организации БС РФ с учетом результатов оценки рисков рекомендуется обеспечить реализацию:
– контроля и (или) запрета размещения на средствах вычислительной техники, используемых для обработки информации конфиденциального характера, и блокирования возможности использования программного обеспечения сервисов мгновенных сообщений (например: ICQ, WhatsUp, Viber, Skype);
– контроля и (или) запрета обработки личной информации с использованием информационной инфраструктуры и средств связи организации БС РФ;
– контроля и (или) запрета самостоятельного использования работниками публичных облачных технологий хранения и обработки информации конфиденциального характера.

10. Рекомендации к реализации процессов системы менеджмента информационной безопасности для обеспечения зрелости процессов мониторинга и контроля потенциальных каналов утечки информации

10.1. Организации БС РФ рекомендуется обеспечить необходимый и достаточный уровень зрелости процессов мониторинга и контроля потенциальных каналов утечки информации, для чего в соответствии с положениями РС БР ИББС-2.7 следует:
– обеспечить необходимую и достаточную область действия процессов мониторинга и контроля потенциальных каналов утечки информации;
– разработать и утвердить внутренние документы, регламентирующие выполнение процессов мониторинга и контроля потенциальных каналов утечки информации, обеспечить их своевременную корректировку;
– обеспечить необходимую и достаточную автоматизацию процессов мониторинга и контроля потенциальных каналов утечки информации;
– обеспечить выполнение программ по обучению и повышению осведомленности работников организации БС РФ в части вопросов предотвращения утечки информации конфиденциального характера;
– обеспечить контроль выполнения процессов мониторинга и контроля потенциальных каналов утечки информации.

10.2. В части обеспечения необходимой и достаточной области действия процессов мониторинга и контроля потенциальных каналов утечки информации организации БС РФ рекомендуется:
– обеспечить мониторинг и контроль использования сервисов электронной почты (в том числе с использованием web-интерфейса) при передаче информации на внешние адреса электронной почты для всего трафика электронной почты и для всех учетных записей сервисов электронной почты;
– обеспечить мониторинг и контроль использования сети Интернет для всех средств вычислительной техники, расположенных в группах сегментов вычислительной сети организации БС РФ, предназначенных для обработки и (или) хранения информации конфиденциального характера, и для всех учетных записей, используемых для осуществления доступа к сети Интернет;

– определить перечень ресурсов сети Интернет, на которых высока вероятность публикации информации конфиденциального характера:
  • ресурсы “блогосферы”;
  • “банковские” сайты: официальные сайты кредитных организаций, сайты, на которых реализована возможность ведения дискуссий (форумов);
  • социальные сети;
  • ресурсы для хранения файлов данных;
– обеспечить мониторинг содержания указанных выше ресурсов сети Интернет с целью возможной публикации информации конфиденциального характера;
– обеспечить мониторинг, контроль, блокирование копирования информации на переносные носители информации для всех средств вычислительной техники, мобильных устройств независимо от следующих факторов:
  • типа и наличия подключения средства вычислительной техники, мобильного устройства к вычислительной сети организации БС РФ;
  • осуществления обработки информации конфиденциального характера на средстве вычислительной техники, мобильных устройствах;
– обеспечить мониторинг и контроль печати и (или) копирования информации на бумажных носителях для сегментов вычислительной сети организации БС РФ, предназначенных для обработки и (или) хранения информации конфиденциального характера, и для всех учетных записей, используемых для осуществления печати информации;
– обеспечить контроль (блокирование) возможности использования и (или) доступа к информации конфиденциального характера на переносных носителях информации за пределами информационной инфраструктуры организации БС РФ для всех переносных носителей информации вне зависимости от их использования для обработки и (или) хранения информации конфиденциального характера;
– обеспечить блокирование возможности доступа к информации конфиденциального характера для всех средств вычислительной техники, используемых за пределами информационной инфраструктуры организации БС РФ, вне зависимости от их использования для обработки и (или) хранения информации конфиденциального характера и всех информационных активов организации БС РФ, к которым осуществляется удаленный доступ;
– определить перечень действий возможных внутренних нарушителей, связанных с доступом к информационным активам конфиденциальной информации, подвергаемых мониторингу и анализу для цели выявления потенциальных утечек информации. При этом рекомендуется подвергать мониторингу и анализу следующие действия:
  • идентификация, аутентификация и авторизация возможных внутренних нарушителей;
  • действия с информацией конфиденциального характера, в том числе чтение, изменение, копирование, удаление информации конфиденциального характера;
  • печать информации конфиденциального характера;
– обеспечить мониторинг и анализ всех действий возможных внутренних нарушителей, связанных с доступом к информационным активам конфиденциальной информации, согласно определенному перечню для всех учтенных информационных активов;
– обеспечить контроль передачи (выноса) всех средств вычислительной техники независимо от осуществления обработки и (или) хранения информации конфиденциального характера;
– обеспечить контроль физического доступа с целью предотвращения визуального и слухового ознакомления с информацией во все помещения, в которых осуществляется обработка и (или) хранение информации конфиденциального характера.

Режим блокирования возможности использования потенциальных каналов утечки информации или режим их непрерывного мониторинга и контроля рекомендуется определять в зависимости от правил доступа для различных категорий потенциальных внутренних нарушителей, рекомендации к содержанию которых установлены в приложении В к настоящему документу.

Применение режима блокирования возможности использования потенциальных каналов утечки информации не отменяет целесообразность выполнения регулярного контроля со стороны службы информационной безопасности организации БС РФ, направленного на корректность реализации процессов мониторинга, и контроля потенциальных каналов утечки информации.

10.3. В части разработки внутренних документов, регламентирующих выполнение процессов мониторинга и контроля потенциальных каналов утечки информации, рекомендуется обеспечить наличие следующих актуальных документов, устанавливающих:
– для всех процессов мониторинга и контроля потенциальных каналов утечки информации:

- правила разблокирования потенциальных каналов утечки информации, предусматривающие согласование возможности разблокирования со службой ИБ организации БС РФ и утверждение решения о разблокировании возможного канала утечки информации лицами из числа руководства организации БС РФ и (или) лицами, определенными руководством организации БС РФ;
- ответственность работников организации БС РФ за невыполнение установленных правил, направленных на предотвращение утечек информации;

– для процесса мониторинга, контроля, блокирования использования сервисов электронной почты при передаче информации на внешние адреса электронной почты:
  - правила и ограничения на передачу работниками организации БС РФ информации на внешние адреса электронной почты с использованием сервисов электронной почты;
  - перечень возможных протоколов и сервисов сетевого взаимодействия, используемых для осуществления передачи сообщений электронной почты;
  - перечень форматов файлов данных, разрешенных к передаче в качестве вложений в сообщения электронной почты, и ограничения на размеры передаваемых файлов данных;
– для процесса мониторинга, контроля, блокирования использования беспроводных сетей и сети Интернет с использованием информационной инфраструктуры организации БС РФ, удаленного доступа к информационной инфраструктуре организации БС РФ с использованием сети Интернет, а также мониторинга публикации информации конфиденциального характера в сети Интернет, в том числе социальных сетях и форумах:
  - правила использования ресурсов сети Интернет, включая перечень сайтов или типов сайтов, запрещенных к использованию;
  - правила размещения средств вычислительной техники, предназначенной для использования ресурсов сети Интернет, в сегментах вычислительных сетей организации БС РФ;
  - правила по ограничению (запрета) использования средств вычислительной техники, предназначенных для доступа к сети Интернет, для обработки информации конфиденциального характера;
  - перечень разрешенных к использованию протоколов и сервисов сетевого взаимодействия и сетевых портов при осуществлении взаимодействия с сетью Интернет;
  - правила использования беспроводных сетей в информационной инфраструктуре организации БС РФ;
  - правила организации и осуществления удаленного доступа к информационной инфраструктуре организации БС РФ с использованием ресурсов сети Интернет;
– для процесса мониторинга, контроля, блокирования копирования информации на переносные носители информации:
  - правила и ограничения (запрета) использования переносных носителей информации на средствах вычислительной техники, предназначенных для обработки информации конфиденциального характера;
  - перечень типов разрешенных к использованию портов ввода-вывода информации;
– для процесса контроля использования средств факсимильной связи:
  - правила и ограничения использования работниками организации БС РФ средств факсимильной связи;
  - правила и ограничения (запрета) размещения средств факсимильной связи в помещениях организации БС РФ, в которых осуществляется обработка и (или) хранение информации конфиденциального характера;
  - правила организации доступа в помещения, в которых размещены средства факсимильной связи;
– для процесса мониторинга и контроля печати и (или) копирования информации на бумажных носителях:
  - правила и ограничения использования работниками организации БС РФ устройств печати и копирования информации на бумажных носителях для печати и (или) копирования информации конфиденциального характера;
  - правила размещения устройств печати и копирования информации на бумажных носителях, в сегментах вычислительных сетей организации БС РФ, предназначенных для обработки информации конфиденциального характера;
  - правила организации доступа в помещения, в которых размещены устройства печати и копирования информации на бумажных носителях;
– для процесса контроля (блокирования) возможности использования и (или) доступа к информации конфиденциального характера на переносных носителях информации за пределами информационной инфраструктуры организации БС РФ:
  - правила использования переносных носителей информации за пределами информационной инфраструктуры организации БС РФ;
  - требования к хранению (шифрованию) информации конфиденциального характера на переносных носителях информации, используемых за пределами информационной инфраструктуры организации БС РФ;

- требования к переносным носителям информации, ограничивающие техническую возможность их использования за пределами информационной инфраструктуры организации БС РФ;

– для процесса блокирования возможности доступа к информации конфиденциального характера на средствах вычислительной техники за пределами информационной инфраструктуры организации БС РФ:
  - правила и ограничения предоставления удаленного доступа к информационным активам, включая правила размещения (публикации) информационных активов в отдельных сегментах вычислительных сетей организации БС РФ, используемых для осуществления удаленного доступа;
  - правила и ограничения использования работниками организации БС РФ средств вычислительной техники за пределами информационной инфраструктуры организации БС РФ;
  - требования к хранению (шифрованию) информации конфиденциального характера на средствах вычислительной техники, используемых за пределами информационной инфраструктуры организации БС РФ;
– для процесса контроля передачи (выноса) средств вычислительной техники за пределы организации БС РФ:
  - правила подготовки средств вычислительной техники, в том числе правила гарантированного удаления информации, перед передачей (выносом) средств вычислительной техники;
– для процесса контроля физического доступа с целью предотвращения визуального и слухового ознакомления с информацией:
  - правила организации доступа в помещения, в которых осуществляется обработка информации конфиденциального характера;
  - требования к применяемым техническим и (или) организационным мерам, ограничивающие доступ в помещения, в которых осуществляется обработка информации конфиденциального характера.

Внутренние документы, регламентирующие выполнение процессов мониторинга и контроля потенциальных каналов утечки информации, рекомендуется устанавливать организационным актом (приказом, распоряжением) организации БС РФ. Данные документы должны содержать описание полномочий работников служб ИБ организаций БС РФ по контролю за их реализацией при проведении мониторинга и контроля потенциальных каналов утечки информации.

10.4. В части обеспечения необходимой и достаточной автоматизации процессов мониторинга и контроля потенциальных каналов утечки информации организации БС РФ рекомендуются:

– реализация автоматизированного протоколирования и (или) блокирования передачи информации на основе контентного анализа передаваемой (переносимой) информации для следующих информационных потоков и потенциальных каналов утечки информации:
  - передача информации конфиденциального характера на внешние адреса электронной почты;
  - передача информации конфиденциального характера в сеть Интернет, в том числе с использованием информационной инфраструктуры организации БС РФ;
  - печать информации конфиденциального характера;
  - копирование информации конфиденциального характера на переносные носители информации;
– реализация автоматизированного протоколирования и (или) блокирования передачи информации на основе контентного анализа информации:
  - на границе контролируемой информационной инфраструктуры организации БС РФ;
  - на средствах вычислительной техники, используемых за пределами информационной инфраструктуры организации БС РФ, имеющих непосредственный доступ к сети Интернет;
  - на средствах вычислительной техники, предназначенных для обработки информации конфиденциального характера, используемых для ее печати;
  - на средствах вычислительной техники с разблокированными портами ввода (вывода) информации, позволяющими осуществить копирование информации на переносные носители информации;
  - осуществляемого с использованием технологии цифрового отпечатка документа и технологии нахождения ключевых слов;
– применение централизованного управления техническими средствами блокирования и (или) протоколирования передачи информации на основе ее контентного анализа, предусматривающего:
  - централизованное установление политик контентного анализа, правил блокирования и протоколирования передачи информации;
  - обеспечение выполнений функций блокирования и (или) протоколирования в режиме “offline” в условиях отсутствия постоянного сетевого взаимодействия с серверами управления;
  - централизованный сбор протоколов работы технических средств, связанных с выполнением функций по блокированию и (или) протоколированию передачи информации;
– реализация для процесса мониторинга, контроля, блокирования использования сервисов электронной почты при передаче информации на внешние адреса электронной почты:

- контентного анализа передаваемой информации по протоколам исходящего почтового обмена;
- ведение единого архива электронных сообщений с архивным доступом на срок не менее 1 года и оперативным доступом на срок не менее 3 месяцев;
- ограничений на перечень протоколов сетевого взаимодействия, используемых для осуществления передачи сообщений электронной почты;
- ограничений на перечень форматов файлов данных, разрешенных к передаче в качестве вложений в сообщения электронной почты, и ограничения на размеры передаваемых файлов данных;

– реализация для процесса мониторинга, контроля, блокирования использования беспроводных сетей и сети Интернет с использованием информационной инфраструктуры организации БС РФ, удаленного доступа к информационной инфраструктуре организации БС РФ с использованием сети Интернет, а также мониторинга публикации информации конфиденциального характера в сети Интернет, в том числе социальных сетей и форумов:
  - контентного анализа передаваемой информации;
  - автоматической классификации ресурсов сети Интернет с целью блокировки доступа к сайтам или типам сайтов, запрещенных к использованию в соответствии с установленными правилами;
  - ограничений на перечень протоколов сетевого взаимодействия и сетевых портов, используемых при осуществлении взаимодействия с сетью Интернет;
  - мониторинга общедоступных ресурсов сети Интернет с целью выявления публикации информации конфиденциального характера и (или) использования сервисов мониторинга общедоступных ресурсов сети Интернет, предоставляемых сторонними организациями;
  - сбор протоколов сеансов удаленного доступа к информационной инфраструктуре организации БС РФ с использованием сети Интернет;
  - сбор протоколов работы технических средств информационной инфраструктуры организации БС РФ, обеспечивающих функционирование беспроводных сетей;
– реализация для процесса мониторинга, контроля, блокирования копирования информации на переносные носители информации:
  - контентного анализа информации, копируемой на отчуждаемые носители информации;
  - блокирование не разрешенных к использованию портов ввода-вывода информации;
  - блокирование возможности использования незарегистрированных (не разрешенных к использованию) переносных носителей информации;
– реализация для процесса мониторинга и контроля печати и (или) копирование информации на бумажных носителях:
  - контентного анализа информации, передаваемой на печать;
  - протоколирование фактов отправки информации на печать;
  - использования специализированных многофункциональных устройств печати с возможностью получения результатов выполнения задания на печать по паролю и (или) персональной карточке доступа;
– реализация для процесса контроля (блокирования) возможности использования и (или) доступа к информации конфиденциального характера на переносных носителях информации за пределами информационной инфраструктуры организации БС РФ:
  - шифрования информации конфиденциального характера на съемных и переносных носителях информации;
  - обеспечения технической невозможности использования съемных и переносных носителей информации за пределами информационной инфраструктуры организации БС РФ;
– реализация для процесса блокирования возможности доступа к информации конфиденциального характера на средствах вычислительной техники за пределами информационной инфраструктуры организации БС РФ:
  - шифрование информации конфиденциального характера на средствах вычислительной техники, используемых за пределами информационной инфраструктуры организации БС РФ;
  - централизованное управление и мониторинг использования средств вычислительной техники (мобильных устройств) с применением подсистемы централизованного управления и мониторинга мобильных устройств (Mobile Device Management, MDM[1]), реализующей: возможность удаленного уничтожения информации конфиденциального характера; уничтожение данных при попытках удаления программных компонентов MDM, уничтожение данных после ряда последовательных неудачных попыток аутентификации на мобильном устройстве;
– реализация в рамках процесса мониторинга и анализа действий возможных внутренних нарушителей автоматического выполнения правил фильтрации, агрегации и корреляции событий ИБ, связанных с

[1] Например, XenMobile, MobileIron, SAP Afaria, IBM Endpoint Manager.

указанными действиями, свидетельствующих о наличии приготовления к реализации утечки информации, в том числе:

- нетипичных действий возможных внутренних нарушителей;
- действий возможных внутренних нарушителей, направленных на доступ к определенной (конкретной) информации конфиденциального характера:
- действий возможных внутренних нарушителей по копированию на переносные носители информации или передаче с использованием сервисов электронной почты значительного объема информации конфиденциального характера.

10.5. В части обеспечения программ выполнения по обучению и повышению осведомленности работников организации БС РФ по предотвращению утечки информации конфиденциального характера организации БС РФ рекомендуется:

– своевременно осуществлять информирование работников организации БС РФ об установленных в соответствии с рекомендациями пункта 10.3 настоящих рекомендаций правилах, запретах и ограничениях при обработке информации конфиденциального характера, применимых к их деятельности;
– своевременно осуществлять информирование работников об установленной ответственности за несоблюдение установленных правил предотвращения утечек информации;
– при необходимости информировать работников организации БС РФ о зафиксированных случаях нарушения правил предотвращения утечек информации и принятых дисциплинарных мерах ответственности.

10.6. В части обеспечения контроля выполнения процессов мониторинга и контроля потенциальных каналов утечки информации службе ИБ организации БС РФ рекомендуется:

– осуществлять автоматизированный контроль включения в область действия процессов мониторинга и контроля потенциальных каналов утечки информации всех учтенных объектов среды информационных активов информации конфиденциального характера;
– участвовать в разработке и согласовывать внутренние документы, регламентирующие выполнение процессов мониторинга и контроля потенциальных каналов утечки информации, разрабатываемые в соответствии с рекомендациями пункта 10.3 настоящих рекомендаций;
– осуществлять периодический контроль реализации организационных мер предотвращения утечек информации, применяемых в соответствии с внутренними документами, разрабатываемыми в соответствии с рекомендациями пункта 10.3 настоящих рекомендаций;
– осуществлять регулярный автоматизированный контроль эксплуатации и использования средств автоматизации, применяемых в соответствии с рекомендациями пункта 10.4 настоящих рекомендаций;
– осуществлять непрерывный мониторинг информационных потоков, реализуемый с использованием средств автоматизации, реализующих контентный анализ, применяемых в соответствии с рекомендациями пункта 10.4 настоящих рекомендаций;
– осуществлять мониторинг общедоступных ресурсов сети Интернет с целью выявления публикаций информации конфиденциального характера.

Приложение А
(справочное)
Примерный состав категорий информации, рекомендуемых для включения в класс “информация конфиденциального характера”

1. Коммерческая тайна

Категория информации – информация об управлении организацией БС РФ:

– информация по стратегическому планированию деятельности организации;
– организационно-распорядительные акты (приказы, распоряжения) организации БС РФ;
– протоколы собраний акционеров организации БС РФ, заседаний руководства организации БС РФ и комитетов по направлениям деятельности организации БС РФ.

Категория информации – информация о планировании коммерческой деятельности организации БС РФ:

– аналитическая информация, сформированная в организации БС РФ;
– информация о результатах исследований в области бизнеса, результатах маркетинговых исследований, методах продвижения услуг на рынок и расчета их стоимости;
– информация об анализе сделок и межбанковских операций;
– информация о методах оценки кредитоспособности заемщиков организации БС РФ;
– информация о планировании объемов и структуры размещения активов;
– информация о планировании объемов и структуры привлечения пассивов.

Категория информации – информация о финансовом состоянии организации БС РФ:

– информация о кредитно-денежной политике организации БС РФ;
– информация о бизнес-планировании организации БС РФ.

Категория информации – информация об автоматизации деятельности организации БС РФ:

– информация о предоставленных правах доступа к АБС организации БС РФ;
– техническая документация на программные компоненты, используемые в организации БС РФ, включая исходные коды программных компонентов.

Категория информации – информация организационного характера:

– информация о штатной структуре организации БС РФ, задачах, решаемых ее структурными подразделениями, должностных обязанностях отдельных работников;
– информация о результатах социологических и психологических исследованиях, проводимых среди работников организации БС РФ;
– информация о конфликтах среди работников организации БС РФ.

Категория информации – информация об обеспечении безопасности и защиты информации организации БС РФ:

– информация о параметрах и (или) свойствах средств технической и информационной защиты, используемых в организации БС РФ;
– информация о конкретных методах или способах обеспечения безопасности и защиты информации в организации БС РФ;
– пароли и закрытые ключи, используемые в программных компонентах организации БС РФ;
– информация о маршрутах движения, объемах или условиях перевозки денежных средств и ценностей;
– данные результатов проверок обеспечения экономической и информационной безопасности, мер технической защиты и систем охраны;
– информация об организации охраны и режиме работы систем технической безопасности организации БС РФ.

2. Банковская тайна

– информация, содержащаяся в кассовых документах организации БС РФ;
– информация об операциях, о счетах и вкладах организация БС РФ и клиентов организации БС РФ.

3. Персональные данные

– персональные данные партнеров и клиентов организации БС РФ;
– персональные данные работников организации БС РФ.

4. Инсайдерская информация

– информация о переговорах с клиентами и партнерами организации БС РФ и их содержании;
– информация о претензиях и исках в отношении БС РФ и их составе и содержании;
– информация о составе и результатах внешних проверок организации БС РФ;
– информация о составе и результатах внутренних проверок организации БС РФ;
– информация об организационно-штатной структуре и ее изменениях;
– информация о предконтрактных переговорах организации БС РФ.

5. Информация, входящая в состав кредитной истории

– кредитные дела клиентов организации БС РФ.

Приложение Б
(справочное)
Пример рекомендаций по приоритизации выполнения работ по защите информации от потенциальных утечек информации

Потенциальный канал утечки	Объект среды информационного актива	Величина риска	Сложность реализации защитных мер	Приоритет реализации
Передача информации с применением электронной почты	Серверное оборудование	Низкая	Низкая	Низкий
	Рабочие станции	Высокая	Низкая	Высокий
Передача информации с применением сервисов сети Интернет, в том числе социальных сетей и форумов	Серверное оборудование	Низкая	Средняя	Средний
	Рабочие станции	Высокая	Средняя	Высокий
	Переносные носители информации	Высокая	Средняя	Высокий
	Переносные (портативные) средства вычислительной техники	Низкая	Средняя	Средний
Удаленный доступ с использованием сети Интернет	Серверное оборудование	Высокая	Средняя	Высокий
	Рабочие станции	Высокая	Средняя	Высокий
	Переносные (портативные) средства вычислительной техники	Низкая	Средняя	Средний
Копирование информации на переносные носители информации	Серверное оборудование	Высокая	Средняя	Высокий
	Рабочие станции	Высокая	Средняя	Высокий
	Переносные (портативные) средства вычислительной техники	Высокая	Средняя	Высокий
Печать и (или) копирование информации на бумажные носители	Рабочие станции	Средняя	Низкая	Высокий
Использование и (или) утеря за пределами информационной инфраструктуры	Переносные носители информации	Высокая	Средняя	Высокий
	Переносные (портативные) средства вычислительной техники	Высокая	Средняя	Высокий
Передача (вынос) средств вычислительной техники за пределы организации БС РФ	Серверное оборудование	Средняя	Низкая	Средний
	Рабочие станции	Средняя	Низкая	Средний
Ознакомление с информацией	Серверное оборудование	Низкая	Низкая	Низкий
	Рабочие станции	Средняя	Низкая	Средний
	Переносные (портативные) средства вычислительной техники	Низкая	Низкая	Низкий
	Бумажные носители информации	Средняя	Низкая	Средний

Приложение В
(справочное)
Пример матриц доступа для различных категорий потенциальных внутренних нарушителей

Потенциальный канал утечки	Серверное оборудование	Рабочие станции	Переносные носители информации	Переносные (портативные) средства вычислительной техники	Бумажные носители информации
Категория А1 – доверенный пользователь:					
Передача информации с применением электронной почты		Мониторинг и контроль			
Передача информации с применением сервисов сети Интернет, в том числе социальных сетей и форумов		Мониторинг и контроль	Мониторинг и контроль	Мониторинг и контроль	
Удаленный доступ с использованием сети Интернет				Мониторинг и контроль	
Копирование информации на переносные носители информации		Мониторинг и контроль		Мониторинг и контроль	
Печать информации		Мониторинг и контроль			
Использование и (или) утеря за пределами организации БС РФ			Контроль с использованием организационных мер	Контроль с использованием организационных мер	
Ознакомление с информацией		Мониторинг и контроль		Мониторинг и контроль	Контроль с использованием организационных мер
Категория А2 – пользователь:					
Передача информации с применением электронной почты		Мониторинг и контроль			
Передача информации с применением сервисов сети Интернет, в том числе социальных сетей и форумов		Блокирование	Блокирование	Блокирование	
Удаленный доступ с использованием сети Интернет				Мониторинг и контроль	
Копирование информации на переносные носители информации		Блокирование		Блокирование	
Печать информации		Мониторинг и контроль			
Использование и (или) утеря за пределами организации БС РФ			Контроль с использованием организационных мер	Контроль с использованием организационных мер	
Ознакомление с информацией		Мониторинг и контроль		Мониторинг и контроль	Контроль с использованием организационных мер
Категория А3 – пользователь “в зоне риска”:					
Передача информации с применением электронной почты		Блокирование			
Передача информации с применением сервисов сети Интернет, в том числе социальных сетей и форумов		Блокирование	Блокирование	Блокирование	

Потенциальный канал утечки	Серверное оборудование	Рабочие станции	Переносные носители информации	Переносные (портативные) средства вычислительной техники	Бумажные носители информации
Удаленный доступ с использованием сети Интернет				Мониторинг и контроль	
Копирование информации на переносные носители информации		Блокирование		Блокирование	
Печать информации		Блокирование			
Использование и (или) утеря за пределами организации БС РФ			Контроль с использованием организационных мер	Контроль с использованием организационных мер	
Ознакомление с информацией		Мониторинг и контроль		Блокирование	Контроль с использованием организационных мер
Категория Б – эксплуатационный персонал:					
Передача информации с применением электронной почты	Блокирование	Мониторинг и контроль			
Передача информации с применением сервисов сети Интернет, в том числе социальных сетей и форумов	Блокирование	Мониторинг и контроль	Контроль с использованием организационных мер	Мониторинг и контроль	
Удаленный доступ с использованием сети Интернет	Блокирование	Мониторинг и контроль		Мониторинг и контроль	
Копирование информации на переносные носители информации	Блокирование	Мониторинг и контроль		Мониторинг и контроль	
Использование и (или) утеря за пределами информационной инфраструктуры			Контроль с использованием организационных мер	Мониторинг и контроль	
Передача (вынос) средств вычислительной техники	Мониторинг и контроль	Мониторинг и контроль			
Ознакомление с информацией	Блокирование	Мониторинг и контроль		Блокирование	Контроль с использованием организационных мер
Категория В – технический и вспомогательный персонал:					
Передача (вынос) средств вычислительной техники		Блокирование			
Ознакомление с информацией		Блокирование			Блокирование
Категория Г – лица, не являющиеся работниками организации БС РФ:					
Передача информации с применением электронной почты		Контроль с использованием организационных мер			
Передача информации с применением сервисов сети Интернет, в том числе социальных сетей и форумов		Контроль с использованием организационных мер	Контроль с использованием организационных мер	Блокирование	
Удаленный доступ с использованием сети Интернет		Мониторинг и контроль		Мониторинг и контроль	
Копирование информации на переносные носители информации		Контроль с использованием организационных мер		Блокирование	

Потенциальный канал утечки	Серверное оборудование	Рабочие станции	Переносные носители информации	Переносные (портативные) средства вычислительной техники	Бумажные носители информации
Использование и (или) утеря за пределами информационной инфраструктуры			Контроль с использованием организационных мер	Мониторинг и контроль	
Печать информации		Контроль с использованием организационных мер			
Ознакомление с информацией		Контроль с использованием организационных мер		Блокирование	Контроль с использованием организационных мер

Библиография

1. Федеральный закон от 27.07.2006 № 149-ФЗ “Об информации, информационных технологиях и о защите информации”.
2. Статья 26 Федерального закона от 02.12.1990 № 395-1 “О банках и банковской деятельности”.
3. Статья 7 Федерального закона от 27.07.2006 № 152-ФЗ “О персональных данных”.
4. Пункт 2.1 Положения Банка России от 9 июня 2012 № 382-П “О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств”.
5. Статья 6 Федерального закона от 27.07.2010 № 224-ФЗ “О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации”.
6. Статьи 6 и 7 Федерального закона от 30.12.2004 № 218-ФЗ “О кредитных историях”.
7. Федеральный закон от 29.07.2004 № 98-ФЗ “О коммерческой тайне”.

Ключевые слова: банковская система Российской Федерации, система обеспечения информационной безопасности, система менеджмента информационной безопасности, служба информационной безопасности, предотвращение утечек информации конфиденциального характера, управление инцидентами информационной безопасности.