ООО «Цифровой Платеж»
115093, г. Москва, Партийный пер., д.1, корп.57, стр.1, этаж 2, офис 319
ОГРН 1137746565934
ИНН/ КПП 7714909651/ 772501001
www.sendy.land , тел. 8 800 700 25 89

У Т В Е Р Ж Д Е Н О
Приказом Генерального директора
ООО «Цифровой Платеж»
от «» 2022 г. №

Введено в действие с ..2022

ПОЛОЖЕНИЕ
о защите информации в Платежной системе «Sendy»

Москва, 2022

СОДЕРЖАНИЕ

Используемые сокращения....3
Термины и определения....4
1. Общие положения....6
2. Цель и задачи СОИБ....7
3. Распределение ролей и обязанностей....8
4. Защищаемые ресурсы....10
5. Модель угроз ИБ и модель потенциального нарушителя ИБ....12
6. Организационные и технические меры защиты информации....21
7. Мониторинг и конфигурирование средств защиты информации....36
8. Порядок предоставления доступа к СЗИ....38
9. Порядок внесения изменений....39
Приложение №1....40

Используемые сокращения

АРМ	Автоматизированное рабочее место
БД	База данных
ГО	Головной офис
ИБ	Информационная безопасность
ИБП	Источник бесперебойного питания
ИС	Информационная система
НСД	Несанкционированный доступ
ОИБ	Отдел информационной безопасности
ОП	Обособленное подразделение
ОС	Операционная система
ПО	Программное обеспечение
ПС	Платежная система «Sendy»
СМСИБ	Серверы мониторинга событий ИБ
СВТ	Средства вычислительной техники
СЗИ	Средство защиты информации
СЗИ НСД	Средство защиты информации от несанкционированного доступа
СКЗИ	Средство криптографической защиты информации
СОБ ИВС	Система обеспечения безопасности информационно-вычислительных систем
СОИБ	Система обеспечения информационной безопасности
УЭИС	Управление эксплуатации информационных систем
ЭП	Электронная подпись

Термины и определения

Банковский счет Участника	Банковский счет (корреспондентский), открытый Прямому участнику Расчетным центром, для осуществления расчетов в Платежной системе.
Информационная безопасность (ИБ)	Безопасность, связанная с угрозами в информационной сфере.
Клиент	Юридическое или физическое лицо, или индивидуальный предприниматель, обладающее полной дееспособностью/ правоспособностью в соответствии с действующим законодательством, совершившие действия, направленные на заключение договора об оказании услуг посредством акцепта условий оферты Участника и(или) которым предоставляется Услуги по Переводу денежных средств в рамках комплекса услуг Платежной системы «Sendy».
Платежный клиринговый центр	Организация, созданная в соответствии с законодательством Российской Федерации, обеспечивающая в рамках Платежной системы прием к исполнению распоряжений Участников Платежной системы об осуществлении Перевода денежных средств и выполнение иных действий, предусмотренных Федеральным законом от 27.06.2011 №161-ФЗ «О национальной платежной системе».
Система обеспечения информационной безопасности (СОИБ)	Совокупность защитных мер, защитных средств, процессов их эксплуатации и управления, включая ресурсное и административное (организационное) обеспечение.
Средство защиты информации (СЗИ)	Техническое, программное, программно-техническое средство, вещество и(или) материал, предназначенные или используемые для защиты информации.
Участники платежной системы	Организации, присоединившиеся к Правилам Платежной системы в целях оказания услуг по Переводу денежных средств.

Электронные денежные средства (ЭДС)	Денежные средства, которые предварительно предоставлены Клиентом Участнику, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счета, для исполнения денежных обязательств Клиента, перед третьими лицами, и в отношении которых Клиент имеет право передавать распоряжения исключительно с использованием электронного средства платежа.
Электронное средство платежа (ЭСП)	Средство и(или) способ, позволяющие Клиенту Участника составлять, удостоверять и передавать распоряжения в целях осуществления Перевода денежных средств (в том числе ЭДС) в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств.
ЭСП Sendy	Электронное средство платежа, предназначенное для совершения Клиентом операций с денежными средствами, учтенными на банковском счете Клиента или на счете ЭДС. ЭСП Sendy выпускается без физического носителя. Доступ к ЭСП Sendy может быть осуществлен с использованием Мобильного приложения или API.

Положение о защите информации в Платежной системе «Sendy»

1. Общие положения

1.1. Настоящее «Положение о защите информации в Платежной системе «Sendy» (далее – Положение) является основополагающим документом Общества с ограниченной ответственностью «Цифровой Платеж» (далее – Общество) для обеспечения защиты информации в Платежной системе «Sendy», содержащим основные положения и принципы реализации Системы обеспечения информационной безопасности Общества (далее – СОИБ) и Платежной системы «Sendy» (далее – ПС).

1.2. Положение разработано с целью определения состава организационно-распорядительных документов по ИБ, программно-технических средств защиты информации, средств контроля и управления ИБ в ПС и в Обществе.

1.3. Основные положения и требования Положения распространяются на все структурные подразделения Общества, в т.ч. осуществляющие контроль соблюдения требований по защите информации в ПС Операторами УПИ и Участниками.

1.4. Настоящее Положение является основой для:

- внедрения и соблюдения Правил в области обеспечения безопасности информации Операторами УПИ и Участниками ПС;
- координации деятельности структурных подразделений Общества при проведении работ по развитию и модернизации ПС с соблюдением требований по обеспечению безопасности информации;
- разработки предложений по совершенствованию технического и организационного обеспечения безопасности информации в ПС и в Обществе.

1.5. Настоящее Положение базируется на следующих нормативно-правовых актах по обеспечению информационной безопасности, действующих на территории Российской Федерации:

1) Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2) Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».
3) Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (с учетом изменений и дополнений).
4) Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе».
5) Постановление Правительства Российской Федерации от 13.06.2012 № 584 «Об утверждении Положения о защите информации в платежной системе».
6) Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
7) Положение Банка России от 03.10.2017 № 607-П «О требованиях к порядку обеспечения бесперебойности функционирования платежной системы, показателям бесперебойности функционирования платежной системы и методикам анализа рисков в платежной системе, включая профили рисков».

8) Положение Банка России от 04.06.2020 № 719-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».
9) Положение Банка России от 09.06.2012 № 381-П «О порядке осуществления надзора за соблюдением не являющимися кредитными организациями операторами платежных систем, операторами услуг платежной инфраструктуры требований Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе», принятых в соответствие с ним нормативных актов Банка России.
10) Указание Банка России от 09.06.2012 № 2831-У «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств».
11) ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

2. Цель и задачи СОИБ

Целью СОИБ является реализация и совершенствование мер, необходимых и достаточных для обеспечения защиты информации при осуществлении переводов денежных средств в ПС на основе выполнения требований российского законодательства, международных стандартов, требований отраслевых и регулирующих органов к обеспечению защиты информации. Для достижения цели должны быть решены следующие задачи:

1) Распределение обязанностей, ответственности и назначение ролей в СОИБ в Обществе и в рамках ПС.
2) Определение Перечня защищаемой информации, инвентаризация защищаемых ресурсов (перечень элементов информационных технологий (ИТ) – инфраструктуры ПС).
3) Моделирование потенциального нарушителя ИБ и потенциальных угроз ИБ в Обществе и ПС.
4) Определение и реализация организационных и технических мер защиты информации по нейтрализации угроз ИБ в ПС, процедур менеджмента ИБ в Обществе и ПС.
5) Оценка соответствия принятых мер требованиям Положения Банка России от 04.06.2020 № 719-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». По результатам оценки – планирование и реализация мер по совершенствованию СКЗИ.
6) Осуществление контроля за соблюдением требований СОИБ в Обществе и в части обеспечения защиты информации в Платежной системе «Sendy».

3. Распределение ролей и обязанностей

3.1. Организация и контроль исполнения практических мероприятий по реализации и сопровождению СОИБ в Обществе возлагается на Отдел информационной безопасности. Приказом Генерального директора Общества из числа должностных лиц Отдела информационной безопасности и ответственных за информационные технологии назначаются:

1) Администратор информационной безопасности ИС (ПС);
2) Администратор ИС (ПС).

3.2. Отдел информационной безопасности отвечает за:

- организацию работ по реализации СОИБ Общества;
- анализ состояния, выработку рекомендаций и указаний по совершенствованию СОИБ и контроль их выполнения;
- разработку основных регламентирующих и нормативных документов СОИБ в Обществе и осуществление контроля выполнения требований указанных документов;
- координацию работ по реализации СОИБ в структурных подразделениях Общества;
- контроль выполнения требований по защите информации в ИС Общества;
- учет фактов нарушений информационной безопасности, организацию проведения расследований по данным фактам и разработку предложений по устранению недостатков и предупреждению подобного рода нарушений;
- ознакомление работников, которые допущены к работе с защищаемой информацией ПС, с внутренними документами СОИБ.

3.3. Начальник Отдела информационной безопасности имеет право:

- представлять работнику, ответственному за вопросы обеспечения ИБ от имени Общества (далее – Куратор) свои предложения по развитию и повышению эффективности СОИБ Общества;
- обращаться к руководителям подразделений Общества по вопросам оказания необходимой технической и методологической помощи в своей работе.

3.4. Администраторы информационной безопасности отвечают за:

- установку, настройку и сопровождение программно-аппаратных средств защиты информации;
- контроль эффективности защиты информации в ИС;
- контроль исполнения пользователями ИС требований информационной безопасности;
- контроль соблюдения пользователями ИС требований по учету, использованию и хранению машинных носителей информации;
- контроль соблюдения пользователями ИС правил копирования и передачи информации по каналам связи;

- проверки рабочих станций пользователей ИС с целью недопущения установки, использования, хранения и размножения в ИС программных средств, не связанных с выполнением функциональных задач;
- анализ журналов учета событий, регистрируемых встроенными средствами ИС и средствами защиты информации, с целью выявления фактов несанкционированного доступа в ИС;
- своевременность доклада представлять Начальнику Отдела информационной безопасности о выявленных нарушениях информационной безопасности, с изложением факта нарушения, предпринятые и(или) рекомендуемые им действия.

3.5. Администратор информационной безопасности имеет право:

- требовать от пользователей ИС соблюдения установленных правил и выполнения инструкций по обеспечению безопасности и защите информации;
- инициировать проведение служебных расследований по фактам нарушения установленных требований по обеспечению информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИС;
- представлять Начальнику Отдела информационной безопасности свои предложения по совершенствованию программно-аппаратных и организационных мер защиты СОИБ;
- обращаться к ответственному за информационные технологии работнику Общества по вопросам оказания необходимой технической и методологической помощи в своей работе.

3.6. Администратор ИС (ПС) отвечает за:

- работоспособность элементов ИС (ПС) и локальной вычислительной сети;
- установку, настройку и своевременное обновление элементов ИС (ПС);
- резервирование и восстановление работоспособности программных и аппаратных средств ИС (ПС);
- контроль за порядком учета и хранения резервных копий;
- допуск к ИС (заведение учетных записей пользователей и прав доступа), контроль за правильностью использования административных паролей ИС (ПС);
- выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт;
- своевременность принятия мер по реагированию, в случае возникновения внештатных и аварийных ситуаций, с целью ликвидации их последствий.

3.7. Администратор ИС (ПС) имеет право:

- запрещать пользователям ИС (ПС) устанавливать на своих рабочих станциях нештатное программное и аппаратное обеспечение;
- проводить проверки использования вычислительной техники и информационных ресурсов ИС (ПС) и пресекать случаи их нецелевого использования;

- информировать Администратора ИБ и Начальника Отдела информационной безопасности о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИС (ПС);
- требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИС (ПС) или средств защиты;
- представлять Начальнику Отдела информационной безопасности свои предложения по модификации существующего аппаратно-программного обеспечения с целью повышению эффективности использования ИС (ПС);
- обращаться к ответственному за информационные технологии работнику Общества по вопросам оказания необходимой технической и методологической помощи в своей работе.

3.8. Куратор по вопросам обеспечения ИБ от руководства Общества осуществляет общий контроль исполнения мероприятий по реализации СОИБ, а также вносит предложения по финансированию данных мероприятий на утверждение Генеральному директору Общества.

4. Защищаемые ресурсы

4.1. К защищаемой информации при осуществлении переводов денежных средств относится:

- информация о средствах и методах обеспечения информационной безопасности в том числе:
  - ключевая информация средств криптографической защиты информации, используемой при осуществлении переводов денежных средств;
  - информация о конфигурации, автоматизированных систем, программного обеспечения, телекоммуникационного оборудования, используемого для осуществления переводов денежных средств;
- информация, используемая при осуществлении перевода денежных средств, в том числе:
  - информация об остатках денежных средств на банковских счетах Участников;
  - информация об остатках ЭДС;
  - информация о совершенных переводах денежных средств;
  - информация, содержащаяся в распоряжениях Клиентов, Участников и Платежного клирингового центра;
  - информация, содержащейся в извещениях (подтверждениях), касающихся приема к исполнению распоряжений Участников и, в случае применимости, Платежного клирингового центра, а также в извещениях (подтверждениях), касающихся исполнения данных распоряжений;
  - информация, необходимая для удостоверения Клиентами права распоряжения денежными средствами;
- информация о совершенных переводах и взаиморасчетах;

- персональные данные клиентов;
- информация, составляющая коммерческую тайну;
- иная информация, подлежащая защите, в соответствии с законодательством Российской Федерации.

4.2. Объектами среды обработки защищаемой информации (элементами ИТ-инфраструктуры), в зависимости от конкретной ПС, могут являться:

1) Виртуальный сервер – роутер
2) Виртуальный сервер БД
3) Веб-сервер
4) Сервер БД
5) Система хранения данных
6) ПО СУБД
7) БД
8) Приложение (серверная часть)
9) Канал провайдера
10) Структурированной кабельной системы, пассивное сетевое оборудование
11) Активное сетевое оборудование
12) Межсетевой экран
13) Типовое АРМ в составе:
    - системный блок;
    - монитор;
    - клавиатура;
    - мышь;
    - принтер (сетевой или автономный);
    - приложение (клиентская часть).

Список объектов защищаемой информации ПС формируется и актуализируется на регулярной основе в соответствии с внутренним документом Общества.

4.3. Кроме того, должны учитываться помещения, где расположены элементы ИТ-инфраструктуры, оснащение данных помещений охранными системами (электронные замки, сигнализация), системами видеонаблюдения, системами пожаротушения, кондиционирования, ИБП.

Список помещений, где расположены элементы ИТ-инфраструктуры ПС, требующие оснащения охранными системами формируется и актуализируется на регулярной основе в соответствии с внутренним документом Общества.

5. Модель угроз ИБ и модель потенциального нарушителя ИБ

5.1. Под угрозами ИБ понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой защищаемой информации и(или) несанкционированными и(или) непреднамеренными воздействиями на нее.

5.2. Угрозы ИБ реализуются источником угрозы, тем или иным способом, используя скрытые или явные уязвимости в ИТ-инфраструктуре ПС, в том числе в СОИБ платежной системы.

5.3. Реализация угроз ИБ приводит к нарушению одной или нескольких характеристик безопасности защищаемой информации (конфиденциальность, целостность, доступность), и, как следствие, приводит к негативным последствиям для ПС.

5.4. Обобщенная схема реализации угроз ИБ представлена на рисунке 1.

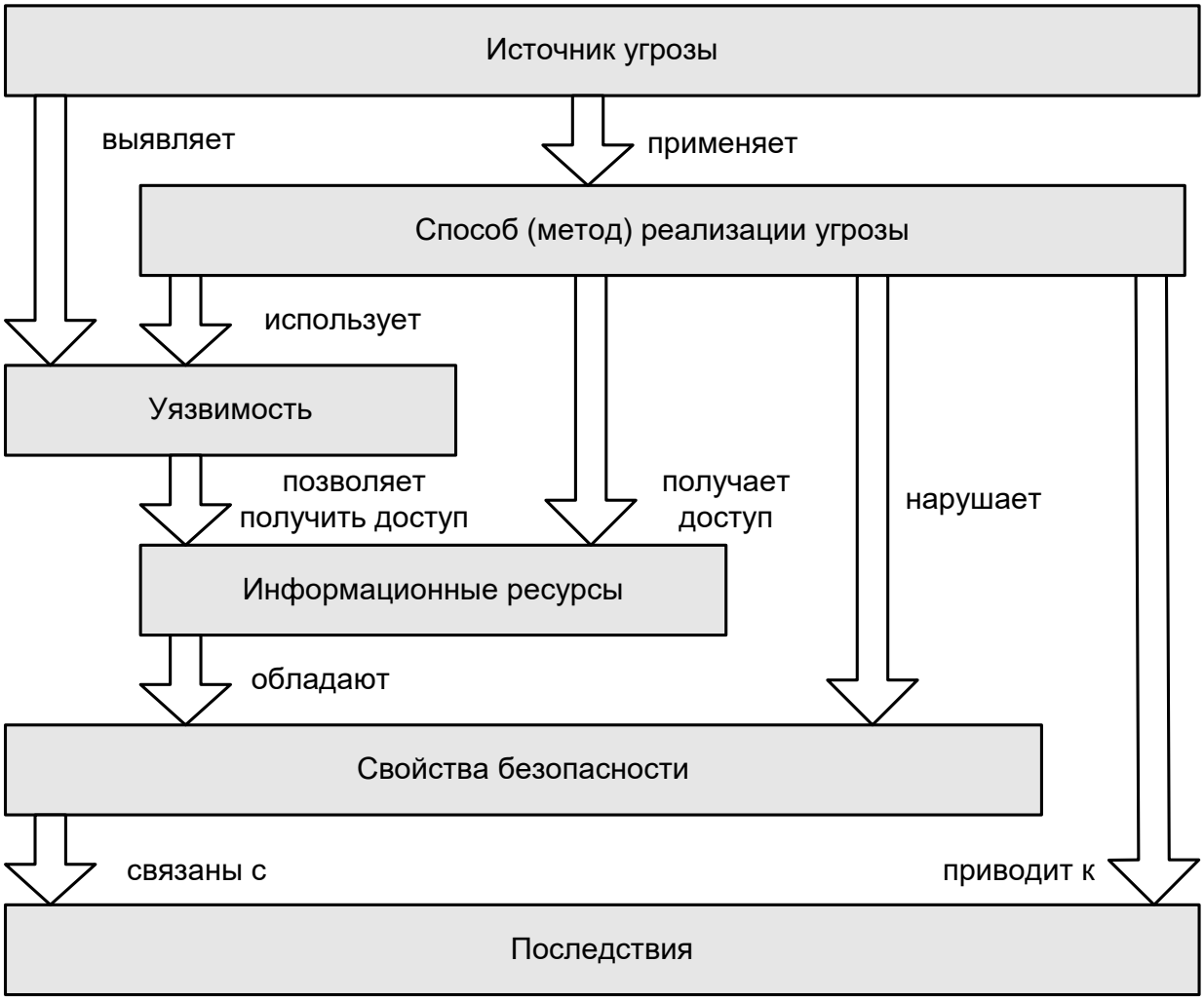

Рисунок 1. Обобщенная схема реализации угроз ИБ

5.5. Источниками угроз ИБ могут быть:

- антропогенные источники (внешний или внутренний нарушитель);

- техногенные источники (внешние или внутренние);
- стихийные источники.

5.6. Пример классификации потенциальных источников угроз ИБ приведен в таблице 1.

Таблица 1. Классификация источников угроз

№ п/п	Источники угроз безопасности персональных данных
1.	**АНТРОПОГЕННЫЕ ИНСТОЧНИКИ**
1.1.	***Внешние антропогенные источники***
1.1.1	криминальные структуры
1.1.2	потенциальные преступники и хакеры
1.1.3	недобросовестные партнеры
1.1.4	технический персонал поставщиков телематических услуг
1.1.5	представители надзорных организаций и аварийных служб
1.1.6	представители силовых структур
1.2	***Внутренние антропогенные источники***
1.2.1	основной персонал (пользователи, программисты, разработчики)
1.2.2	представители службы защиты информации (администраторы)
1.2.3	вспомогательный персонал (уборщики, охрана)
1.2.4	технический персонал (жизнеобеспечение, эксплуатация)
1.2.5	внедренные и завербованные агенты
2.	**ТЕХНОГЕННЫЕ ИСТОЧНИКИ**
2.1	***Внешние техногенные источники угроз***
2.1.1	технические средства обработки информации (программно-аппаратные закладки)
2.1.2	программные средства обработки информации (вредоносные программы)
2.1.3	средства связи
2.1.4	сети инженерных коммуникаций (водоснабжения, канализации)
2.1.5	Транспорт
2.2	***Внутренние техногенные источники угроз***
2.2.1	некачественные технические средства обработки информации
2.2.2	некачественные программные средства обработки информации
2.2.3	вспомогательные средства (охраны, сигнализации, телефонии)
2.2.4	другие технические средства, применяемые в ИТ-инфраструктуре и помещениях
3.	**СТИХИЙНЫЕ ИСТОЧНИКИ УГРОЗ**
3.1	пожары
3.2	землетрясения
3.3	наводнения
3.4	ураганы
3.5	магнитные бури
3.6	другие форс-мажорные обстоятельства

5.7. Уязвимости, которые могут быть использованы источниками угроз, могут быть как объективно существующими в силу законов физики, так и умышленно или неумышленно созданными (субъективными), а также случайно возникшими в результате непредвиденных аварийных ситуаций.

5.8. Пример классификации потенциальных уязвимостей приведен в таблице 2.

Таблица 2. Классификация уязвимостей

№ п/п	Уязвимости объектов защиты
1.	**ОБЪЕКТИВНЫЕ**
1.1	**Сопутствующие техническим средствам излучения**
1.1.1	**электромагнитные**
1.1.1.1	побочные излучения элементов технических средств
1.1.1.2	кабельных линий технических средств
1.1.1.3	излучения на частотах работы генераторов
1.1.1.4	на частотах самовозбуждения усилителей
1.1.2	**электрические**
1.1.2.1	наводки электромагнитных излучений на линии и проводники
1.1.2.2	просачивание сигналов в цепи электропитания, в цепи заземления
1.1.3	**Звуковые**
1.1.3.1	Акустические
1.1.3.2	Виброакустические
1.2	**Определяемые особенностями элементов**
1.2.1	**элементы, обладающие электроакустическими преобразованиями**
1.2.1.1	телефонные аппараты
1.2.1.2	громкоговорители и микрофоны
1.2.1.3	катушки индуктивности
1.2.1.4	дроссели
1.2.1.5	трансформаторы и пр.
1.2.2	**элементы, подверженные воздействию электромагнитного поля**
1.2.2.1	магнитные носители
1.2.2.2	микросхемы
1.2.2.3	нелинейные элементы, поверженные ВЧ навязыванию
1.3	**Определяемые особенностями защищаемого объекта**
1.3.1	**местоположением объекта**
1.3.1.1	отсутствие контролируемой зоны
1.3.1.2	наличие прямой видимости объектов
1.3.1.3	удаленных и мобильных элементов объекта
1.3.1.4	вибрирующих отражающих поверхностей
1.3.2	**организацией каналов обмена информацией**
1.3.2.1	использование радиоканалов
1.3.2.2	глобальных информационных сетей
1.3.2.3	арендуемых каналов
1.3.2.4	локальных вычислительных сетей
1.3.3.	**обеспечением средствами защиты**
1.3.3.1	использование технических средств защиты
1.3.3.2	использование программных средств защиты
2.	**СУБЪЕКТИВНЫЕ**
2.1	**Ошибки**
2.1.1	**при подготовке и использовании программного обеспечения**
2.1.1.1	при разработке алгоритмов и программного обеспечения
2.1.1.2	инсталляции и загрузке программного обеспечения

2.1.1.3	эксплуатации программного обеспечения
2.1.1.4	вводе данных
2.1.2	**при управлении сложными системами**
2.1.2.1	при использовании возможностей самообучения систем
2.1.2.2	настройке сервисов универсальных систем
2.1.2.3	организации управления потоками обмена информации
2.1.3	**при эксплуатации технических средств**
2.1.3.1	при включении/выключении технических средств
2.1.3.2	использовании технических средств охраны
2.1.3.3	использовании средств обмена информацией
2.2	**Нарушения**
2.2.1	**режима охраны и защиты**
2.2.1.1	доступа на объект
2.2.1.2	доступа к техническим средствам
2.2.2	**режима эксплуатации технических средств**
2.2.2.1	энергообеспечения
2.2.2.2	жизнеобеспечения
2.2.3	**режима использования информации**
2.2.3.1	обработки и обмена информацией
2.2.3.2	хранения и уничтожения носителей информации
2.2.3.3	использование неразрешенного ПО
2.2.4	**режима конфиденциальности**
2.2.4.1	сотрудниками в нерабочее время
2.2.4.2	уволенными сотрудниками
3.	**СЛУЧАЙНЫЕ**
3.1	**Сбои и отказы**
3.1.1	**отказы и неисправности технических средств**
3.1.1.1	обрабатывающих информацию
3.1.1.2	обеспечивающих работоспособность средств обработки информации
3.1.1.3	обеспечивающих охрану и контроль доступа
3.1.2	**старение и размагничивание носителей информации**
3.1.2.1	дискет и съемных носителей
3.1.2.2	жестких дисков
3.1.2.3	элементов микросхем
3.1.2.4	кабелей и соединительных линий
3.1.3	**сбои программного обеспечения**
3.1.3.1	операционных систем и СУБД
3.1.3.2	прикладных программ
3.1.3.3	сервисных программ
3.1.3.4	антивирусных программ
3.1.4	**сбои электроснабжения**
3.1.4.1	оборудования, обрабатывающего информацию
3.1.4.2	обеспечивающего и вспомогательного оборудования
3.2	**Повреждения**
3.2.1	**жизнеобеспечивающих коммуникаций**
3.2.1.1	электро-, водо-, газо-, теплоснабжения, канализации
3.2.1.2	кондиционирования и вентиляции
3.2.2	**ограждающих конструкций**

3.2.2.1	внешних ограждений территорий, стен и перекрытий зданий
3.2.2.2	корпусов технологического оборудования

5.9. Пример классификации методов реализации угроз ИБ и возможных последствий приведен в таблице 3.

Таблица 3. Классификация методов реализации угроз и последствий

№	Методы и предпосылки реализации угроз	Возможные последствия реализации угроз
1	***Аналитические методы***	
1.1	***Активные аналитические методы***	
1.1.1	опрос в ходе публичных мероприятий (конференции и пр.)	Нарушение конфиденциальности путем прямого получения конфиденциальной информации
1.1.2	опрос бывших (уволенных) сотрудников	Нарушение конфиденциальности путем прямого получения конфиденциальной информации. Получение информации о номерах телефонов, IP адресах пользователей и подсетей, архитектуре сети, открытых серверах, структуре организации и др. информации для дальнейшей реализации угроз
1.1.3	проведение мнимых переговоров	Нарушение конфиденциальности путем прямого получения конфиденциальной информации. Получение информации о номерах телефонов, IP адресах, архитектуре сети, открытых серверах, структуре организации и др. информации для дальнейшей реализации угроз
1.1.4	сканирование и инвентаризация ИС	Определение функций ИС, способа представления информации, типа, параметров и версий ПО, носителей информации, идентификация СВТ, СЗИ, идентификация учетных записей пользователей, используемых сервисов и служб, поиск совместно используемых ресурсов, открытых портов, незашифрованных паролей для дальнейшей реализации угроз
1.2	***Пассивные аналитические методы***	
1.2.1	анализ информации из средств массовой информации (СМИ), глобальных ИС	Получение информации о номерах телефонов, IP адресах пользователей и подсетей, архитектуре сети, открытых серверах, структуре организации, дефектах ПО, оборудования, нарушениях при эксплуатации оборудования, инструментарии для дальнейшей реализации угроз.
1.2.2	агрегирование и инференция открытой информации	Нарушение конфиденциальности путем прямого получения конфиденциальной информации.

№	Методы и предпосылки реализации угроз	Возможные последствия реализации угроз
2	***Технические методы***	
2.1	***Активные технические методы***	
2.1.1	мониторинг (наблюдение) активности каналов связи	Получение информации о номерах телефонов, IP адресах пользователей и подсетей, архитектуре сети, открытых серверах, структуре организации, выявление наиболее уязвимых мест сети для дальнейшей реализации угроз.
2.1.2	радиационное и ионизирующее воздействие	Нарушение целостности и доступности информации при передаче по каналам связи, нарушение нормальной работы технических устройств, носителей информации.
2.1.3	электромагнитное воздействие	Нарушение целостности и доступности информации при передаче по каналам связи, нарушение нормальной работы технических устройств, носителей информации.
2.1.4	создание условий для сбоев и отказов оборудования и ПО	Нарушение целостности и доступности информации при передаче по каналам связи, нарушение нормальной работы технических устройств, носителей информации.
2.2	*Пассивные технические методы*	
2.2.1	визуально-оптическое наблюдение и фотографирование	Нарушение конфиденциальности путем прямого получения конфиденциальной информации.
2.2.2	перехват акустических и виброакустических сигналов	Нарушение конфиденциальности путем прямого получения конфиденциальной информации.
2.2.2	перехват информации в кабельных линиях связи	Нарушение конфиденциальности путем прямого получения конфиденциальной информации.
2.2.3	перехват ПЭМИ от технических средств	Нарушение конфиденциальности путем прямого получения конфиденциальной информации.
2.2.4	перехват оптоэлектронных сигналов	Нарушение конфиденциальности путем прямого получения конфиденциальной информации.
2.2.5	перехват информации методом ВЧ-навязывания	Нарушение конфиденциальности путем прямого получения конфиденциальной информации.
3	***Программно-аппаратные методы***	
3.1	*Активные программно-аппаратные методы*	
3.1.1	внедрение дезинформации	Нарушение целостности и доступности путем введения ложной информации в базы данных и информационные ресурсы, перегрузки системных ресурсов, каналов

№	Методы и предпосылки реализации угроз	Возможные последствия реализации угроз
		связи.
3.1.2	загрузка нештатной ОС и ПО	Создание условий для дальнейшей реализации угроз, отключение механизмов защиты.
3.1.3	изменение конфигурации ИС и используемых сервисов	Отключение механизмов защиты, изменение полномочий пользователей отключение/включение сервисов, перенаправление информации, введение запрета на использование информации для дальнейшей реализации угроз.
3.1.4	маскировка под авторизованного пользователя (маскарад)	Нарушение конфиденциальности и целостности путем использования полномочий авторизованных пользователей по чтению и изменению информации.
3.1.5	модификация информации (данных)	Нарушение целостности путем модификации информации в базах данных и информационных ресурсах.
3.1.6	модификация ПО и(или) его настроек	Создание условий дальнейшей реализации угроз.
3.1.7	несанкционированное изменение полномочий	Нарушение конфиденциальности и целостности путем изменения (превышения) полномочий авторизованных пользователей по чтению и изменению информации.
3.1.8	перехват управления соединениями	Нарушение доступности и конфиденциальности путем стороннего управления активным сеансом.
3.1.9	перехват управления ИС	Нарушение конфиденциальности, целостности и доступности путем уничтожения, модификации информации, перегрузки системных ресурсов, нарушения нормальной работы
3.1.10	применение вредоносных программ	Нарушение конфиденциальности, целостности и доступности путем уничтожения, модификации информации, перезагрузки системных ресурсов, нарушения нормальной работы технических средств и ПО, физического разрушения технических средств и носителей информации, влияния на персонал ИС, накопления и перенаправления информации по скрытым каналам, введения запрета на использование информации, монопольный захват системных ресурсов.
3.1.11	применение отладочных режимов ИС	Создание предпосылок и условий дальнейшей реализации угроз, отключение механизмов защиты.
3.1.12	сканирование и модификация	Сокрытие следов несанкционированных действий после реализации угроз.

№	Методы и предпосылки реализации угроз	Возможные последствия реализации угроз
	журналов регистрации	
3.1.13	интенсивное обращение к ИС и каналам связи	Нарушение доступности путем перегрузки сетевых ресурсов и каналов связи.
3.2	*Пассивные программно-аппаратные методы*	
3.2.1	наблюдение за активностью работы в ИС	Определение функций ИС, способа представления информации, идентификация учетных записей пользователей, используемых сервисов и служб, незашифрованных паролей для дальнейшей реализации угроз.
3.2.2	установка нештатного оборудования или ПО	Создание предпосылок и условий дальнейшей реализации угроз.
3.2.3	чтение, копирование информации	Нарушение конфиденциальности путем прямого получения конфиденциальной информации. Получение паролей доступа, списков управления доступом, таблиц маршрутизации, информации о номерах телефонов и IP адресах, архитектуре сети, структуре организации для дальнейшей реализации угроз.
4	***Социальные методы***	
4.1	***Активные социальные методы***	
4.1.1	вербовка, подкуп или шантаж персонала	Нарушение конфиденциальности, целостности и доступности путем прямого получения конфиденциальной информации (данных), склонения к уничтожению, модификации информации, ПО. Получение информации о номерах телефонов и IP пользователей, адресах подсетей, архитектуре сети, открытых серверах, структуре организации, дефектах ПО, оборудования, нарушениях при эксплуатации оборудования, инструментарии для дальнейшей реализации угроз.
4.1.2	вхождение в доверие	Нарушение конфиденциальности путем прямого получения конфиденциальной информации. Получение информации о номерах телефонов и IP пользователей, адресах подсетей, архитектуре сети, открытых серверах, структуре организации, дефектах ПО, оборудования, нарушениях при эксплуатации оборудования, инструментарии для дальнейшей реализации угроз.
4.1.3	разжигание вражды	Создание предпосылок и условий для дальнейшей реализации угроз.
4.1.4	террористические методы (поджег,	Нарушение целостности и доступности путем уничтожения технических средств, носителей

№	Методы и предпосылки реализации угроз	Возможные последствия реализации угроз
	взрыв, уничтожение)	информации, ПО, каналов и линий связи.
5	***Организационные методы***	
5.1	*Активные организационные методы*	
5.1.1	доступ к носителям информации, техническим средствам	Нарушение конфиденциальности, целостности и доступности путем получения носителей информации, уничтожения технических средств и носителей информации, модификации информации, ПО.
5.1.2	подделка документов	Создание предпосылок и условий для дальнейшей реализации угроз.
5.1.3	разрушение коммуникаций	Нарушение целостности и доступности путем нарушения нормальной работы технических средств, каналов и линий связи.

5.10. В общем случае, при обработке защищаемой информации в ПС, возможна реализация следующих видов потенциальных угроз ИБ:

- угрозы утечки защищаемой информации по техническим каналам;
- угрозы несанкционированного доступа (НСД) к защищаемой информации.

5.11. Угрозы утечки информации по техническим каналам включают в себя:

- угрозы утечки акустической (речевой) информации;
- угрозы утечки видовой информации;
- угрозы утечки информации по каналу ПЭМИН (побочные электромагнитные излучения и наводки).

5.12. Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ПС, возможно при наличии функций голосового ввода информации в ПС или функций воспроизведения информации акустическими средствами ПС.

5.13. Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средства обработки графической, видео- и буквенно-цифровой информации, входящих в состав ПС.

5.14. Угрозы утечки информации по каналу ПЭМИН возможны из-за наличия электромагнитных излучений, в основном, монитора и системного блока компьютера. Основную опасность представляют угрозы утечки из-за наличия электромагнитных излучений монитора.

5.15. Угрозы НСД к защищаемой информации включают в себя:

1) Угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном и(или) прикладном программном обеспечении, используемом в информационной системе.
2) Угрозы, не связанные с наличием НДВ в системном и(или) прикладном ПО, но связанные с действиями нарушителей, имеющих доступ к ПС:
   - угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/ вывода (BIOS), перехват управления загрузкой;
   - угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах и т.п.);
   - угрозы внедрения вредоносных программ.
3) Угрозы, связанные с реализацией протоколов сетевого взаимодействия, реализуемые внутри распределенной сети:
   - угрозы типа «анализ сетевого трафика» с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации;
   - угрозы сканирования, направленные на выявление типа операционной системы ПС, сетевых адресов рабочих станций, открытых портов и служб, открытых соединений и др.;
   - угрозы выявления паролей;
   - угрозы получения НСД путем подмены доверенного объекта;
   - угрозы типа «отказ в обслуживании»;
   - угрозы удаленного запуска приложений;
   - угрозы внедрения по сети вредоносных программ.

5.16. С целью определения актуальных угроз безопасности информации ПС в Обществе разработана «Модель угроз безопасности персональных данных при их обработке в программном комплексе ПС Sendy».

6. Организационные и технические меры защиты информации

6.1. Для нейтрализации актуальных угроз ИБ и обеспечения защиты информации в ПС в соответствии с требованиями законодательства Российской Федерации, нормативных актов Банка России и других регулирующих органов, в Обществе применяются организационные и технические меры.

6.2. Обобщенный перечень организационно-технических мер защиты включает в себя следующие меры:

- (1) Криптозащита, туннелирование и векторизация IP-пакетов, имплементируемая в FireWall-устройства

- (2) Настройка политики безопасности при помощи FireWall-устройств
- (3) Туннелирование и векторизация IP-пакетов
- (4) Аутентификация на уровне транзакций
- (5) Контроль доступа на уровне транзакций
- (6) Электронная подпись, закрытие контекста на уровне документов
- (7) Контроль действий пользователей: протоколы событий, периодические или событийные повторы контроля полномочий, криптозащита информации в локальной сети
- (8) Работа с контролируемыми магнитными носителями, вирусопрофилактика
- (9) Контроль доступа пользователей к системе, варианты:
- (10) Усиленный режим контроля НСД на рабочем месте администратора СОБ ИВС; отключение от сети в пассивном состоянии
- (11) Особый режим хранения информации администратора СОБ-ИВС
- (12) Соглашения о конфиденциальности, меры индивидуальной ответственности
- (13) Офисный регламент мер безопасности
- (14) Контроль доступа посторонних в помещения, охрана помещения администратора
- (15) Соглашение с коммуникационными партнерами о соблюдении мер безопасности
- (16) Резервное копирование программ и данных
- (17) Резервирование аппаратно-программных средств системы
- (18) Аппаратные платформы с повышенной надежностью, бесперебойные источники питания
- (19) Диверсификация доступа к коммуникационным средам, резервирование выделенных линий
- (20) Обеспечение надежного сервисного обслуживания
- (21) Использование программ очистки свободного дискового пространства
- (22) Использование средств уничтожения производственных отходов
- (23) Защита помещения от утечек по техническим каналам
- (24) Высокая степень отладки ПО, самоконтроль ПО, контроль вводимой информации, обратимость операций

6.3. Меры защиты, относящиеся к категории программно-аппаратных, реализуется с помощью следующих механизмов:

- Аутентификационный обмен;
- Шифрование;
- Имитозащита;

- Электронная подпись.

6.4. Пример использования комплекса мер защиты для нейтрализации потенциальных атак на защищаемые информационные ресурсы приведен в таблице 4.

Таблица 4. Примеры атак и мер защиты для их нейтрализации

Атаки	Меры защиты
Класс 1. Аппаратно-порожденные атак	
1. Физическое повреждение аппаратных средств	(16) Резервное копирование программ и данных (17) Резервирование аппаратно-программных средств системы
2. Физическое повреждение линий связи	(19) Диверсификация доступа к коммуникационным средам, резервирование выделенных линий
3. Отказ аппаратных средств	(16) Резервное копирование программ и данных (17) Резервирование аппаратно-программных средств системы (20) Обеспечение надежного сервисного обслуживания
4. Перебои в электропитании	(16) Резервное копирование программ и данных (18) Аппаратные платформы с повышенной надежностью, бесперебойные источники питания
5. Прерывание процесса передачи и обработки информации	(16) Резервное копирование программ и данных (17) Резервирование аппаратно-программных средств системы (19) Диверсификация доступа к коммуникационным средам, резервирование выделенных линий
Класс 2. Модификации, повреждение, разрушение программного обеспечения	
6. Анализ и модификация программного обеспечения	(2) Настройка политики безопасности при помощи FireWall-устройств (3) Туннелирование и векторизация IP-пакетов (7) Контроль действий оператора: протоколы событий, периодические или событийные повторы контроля полномочий, криптозащита информации в локальной сети (8) Работа с контролируемыми магнитными носителями, вирусопрофилактика (9) Контроль доступа операторов к системе (12) Соглашения о конфиденциальности, меры индивидуальной ответственности (13) Офисный регламент мер безопасности (14) Контроль доступа посторонних в помещения, охрана помещения администратора
7. Наличие «закладок» и «скрытых каналов» в ПО	(2) Настройка политики безопасности при помощи FireWall-устройств (3) Туннелирование и векторизация IP-пакетов (7) Контроль действий оператора: протоколы событий, периодические или событийные повторы контроля полномочий, криптозащита информации в локальной сети (8) Работа с контролируемыми магнитными носителями, вирусопрофилактика

Атаки	Меры защиты
	(9) Контроль доступа операторов к системе, варианты (10) Усиленный режим контроля НСД на рабочем месте администратора СОБ-ИВС; отключение от сети в пассивном состоянии (11) Особый режим хранения информации администратора СОБ-ИВС
8. Внедрение вредоносных программ	(2) Настройка политики безопасности при помощи FireWall-устройств (3) Туннелирование и векторизация IP-пакетов (7) Контроль действий оператора: протоколы событий, периодические или событийные повторы контроля полномочий, криптозащита информации в локальной сети (8) Работа с контролируемыми магнитными носителями, вирусопрофилактика
Класс 3. Несанкционированный доступ персонала, превышение полномочий	
9. Несанкционированное получение и использование привилегий	(7) Контроль действий оператора: протоколы событий, периодические или событийные повторы контроля полномочий, криптозащита информации в локальной сети (8) Работа с контролируемыми магнитными носителями, вирусопрофилактика (9) Контроль доступа операторов к системе, варианты (12) Соглашения о конфиденциальности, меры индивидуальной ответственности (13) Офисный регламент мер безопасности (14) Контроль доступа посторонних в помещения, охрана помещения администратора
10. Несанкционированный доступ к наборам данных других участников	(7) Контроль действий оператора: протоколы событий, периодические или событийные повторы контроля полномочий, криптозащита информации в локальной сети (8) Работа с контролируемыми магнитными носителями, вирусопрофилактика (9) Контроль доступа операторов к системе, варианты (12) Соглашения о конфиденциальности, меры индивидуальной ответственности (13) Офисный регламент мер безопасности (14) Контроль доступа посторонних в помещения, охрана помещения администратора
11. Несанкционированный доступ к базам данных, архивам	(7) Контроль действий оператора: протоколы событий, периодические или событийные повторы контроля полномочий, криптозащита информации в локальной сети (8) Работа с контролируемыми магнитными носителями, вирусопрофилактика (9) Контроль доступа операторов к системе, варианты (12) Соглашения о конфиденциальности, меры индивидуальной ответственности (13) Офисный регламент мер безопасности (14) Контроль доступа посторонних в помещения, охрана

Атаки	Меры защиты
	помещения администратора
Класс 4. Нарушение конфиденциальности, угрозы безопасности со стороны персонала	
12. Выполнение действий одним участником от имени другого	(7) Контроль действий оператора: протоколы событий, периодические или событийные повторы контроля полномочий, криптозащита информации в локальной сети (8) Работа с контролируемыми магнитными носителями, вирусопрофилактика (9) Контроль доступа операторов к системе, варианты (12) Соглашения о конфиденциальности, меры индивидуальной ответственности (13) Офисный регламент мер безопасности (14) Контроль доступа посторонних в помещения, охрана помещения администратора
13. Маскировка под зарегистрированного участника	(7) Контроль действий оператора: протоколы событий, периодические или событийные повторы контроля полномочий, криптозащита информации в локальной сети (8) Работа с контролируемыми магнитными носителями, вирусопрофилактика (9) Контроль доступа операторов к системе, варианты (12) Соглашения о конфиденциальности, меры индивидуальной ответственности (13) Офисный регламент мер безопасности (14) Контроль доступа посторонних в помещения, охрана помещения администратора
14. Отказ от факта получения сообщения	(7) Контроль действий оператора: протоколы событий, периодические или событийные повторы контроля полномочий, криптозащита информации в локальной сети (8) Работа с контролируемыми магнитными носителями, вирусопрофилактика (9) Контроль доступа операторов к системе, варианты (12) Соглашения о конфиденциальности, меры индивидуальной ответственности (13) Офисный регламент мер безопасности (14) Контроль доступа посторонних в помещения, охрана помещения администратора (15) Соглашение с коммуникационными партнерами о соблюдении мер безопасности
15. Ложная отправка сообщения	(7) Контроль действий оператора: протоколы событий, периодические или событийные повторы контроля полномочий, криптозащита информации в локальной сети (8) Работа с контролируемыми магнитными носителями, вирусопрофилактика (9) Контроль доступа операторов к системе, варианты (12) Соглашения о конфиденциальности, меры индивидуальной ответственности (13) Офисный регламент мер безопасности

Атаки	Меры защиты
	(14) Контроль доступа посторонних в помещения, охрана помещения администратора (15) Соглашение с коммуникационными партнерами о соблюдении мер безопасности
16. Прерывание процесса передачи и обработки информации	(4) Аутентификация на уровне транзакций (5) Контроль доступа на уровне транзакций (6) Электронная подпись, закрытие контекста на уровне документов (7) Контроль действий оператора: протоколы событий, периодические или событийные повторы контроля полномочий, криптозащита информации в локальной сети (8) Работа с контролируемыми магнитными носителями, вирусопрофилактика (9) Контроль доступа операторов к системе, варианты (12) Соглашения о конфиденциальности, меры индивидуальной ответственности (13) Офисный регламент мер безопасности (14) Контроль доступа посторонних в помещения, охрана помещения администратора
17. Разглашение реализации программной защиты	(12) Соглашения о конфиденциальности, меры индивидуальной ответственности (13) Офисный регламент мер безопасности
18. Раскрытие, перехват, хищение кодов, ключей, паролей	(2) Настройка политики безопасности при помощи FireWall-устройств (3) Туннелирование и векторизация IP-пакетов (7) Контроль действий оператора: протоколы событий, периодические или событийные повторы контроля полномочий, криптозащита информации в локальной сети (14) Контроль доступа посторонних в помещения, охрана помещения администратора
19. Установка подслушивающих устройств	(13) Офисный регламент мер безопасности (14) Контроль доступа посторонних в помещения, охрана помещения администратора
20. Чтение остаточной информации в оперативной памяти и на магнитных носителях	(7) Контроль действий оператора: протоколы событий, периодические или событийные повторы контроля полномочий, криптозащита информации в локальной сети (9) Контроль доступа операторов к системе, варианты (21) Использование программ очистки свободного дискового пространства
21. Хищение носителей информации, производственных отходов	(13) Офисный регламент мер безопасности (14) Контроль доступа посторонних в помещения, охрана помещения администратора (22) Использование средств уничтожения производственных отходов
Класс 5. Промышленный шпионаж, внешние атаки на систему безопасности	
22. Наблюдение за работой системы	(1) Криптозащита, туннелирование и векторизация IP-пакетов, имплементируемая в FireWall-устройства

Атаки	Меры защиты
	(9) Контроль доступа операторов к системе, варианты (12) Соглашения о конфиденциальности, меры индивидуальной ответственности (13) Офисный регламент мер безопасности (14) Контроль доступа посторонних в помещения, охрана помещения администратора (23) Защита помещения от утечек по техническим каналам
23. Применение подслушивающих устройств	(12) Соглашения о конфиденциальности, меры индивидуальной ответственности (13) Офисный регламент мер безопасности (14) Контроль доступа посторонних в помещения, охрана помещения администратора (23) Защита помещения от утечек по техническим каналам
24. Перехват информации на линиях связи	(1) Криптозащита, туннелирование и векторизация IP-пакетов, имплементируемая в FireWall-устройства (3) Туннелирование и векторизация IP-пакетов (4) Аутентификация на уровне транзакций (6) Электронная подпись, закрытие контекста на уровне документов
25. Перехват электронных излучений	(13) Офисный регламент мер безопасности (14) Контроль доступа посторонних в помещения, охрана помещения администратора (23) Защита помещения от утечек по техническим каналам
26. Перехват акустических излучений	(13) Офисный регламент мер безопасности (14) Контроль доступа посторонних в помещения, охрана помещения администратора (23) Защита помещения от утечек по техническим каналам
27. Дистанционное фотографирование	(13) Офисный регламент мер безопасности (14) Контроль доступа посторонних в помещения, охрана помещения администратора (23) Защита помещения от средств внешней разведки
28. Принудительное электронно-магнитное облучение линий связи	(14) Контроль доступа посторонних в помещения, охрана помещения администратора (23) Защита помещения от утечек по техническим каналам
29. Хищение носителей информации, производственных отходов	(13) Офисный регламент мер безопасности (14) Контроль доступа посторонних в помещения, охрана помещения администратора (22) Использование средств уничтожения производственных отходов
Класс 6. Имитоатаки, диверсии, хакерство, НСД из публичных сетей	
30. Подмена и модификация сообщения	(1) Криптозащита, туннелирование и векторизация IP-пакетов, имплементируемая в FireWall-устройства (2) Настройка политики безопасности при помощи FireWall-устройств (3) Туннелирование и векторизация IP-пакетов (4) Аутентификация на уровне транзакций (5) Контроль доступа на уровне транзакций

Атаки	Меры защиты
	(6) Электронная подпись, закрытие контекста на уровне документов
31. Прерывание процесса передачи и обработки информации	(1) Криптозащита, туннелирование и векторизация IP-пакетов, имплементируемая в FireWall-устройства (2) Настройка политики безопасности при помощи FireWall-устройств (3) Туннелирование и векторизация IP-пакетов (4) Аутентификация на уровне транзакций (5) Контроль доступа на уровне транзакций (6) Электронная подпись, закрытие контекста на уровне документов
32. Ложная отправка сообщения	(1) Криптозащита, туннелирование и векторизация IP-пакетов, имплементируемая в FireWall-устройства (2) Настройка политики безопасности при помощи FireWall-устройств (3) Туннелирование и векторизация IP-пакетов (4) Аутентификация на уровне транзакций (5) Контроль доступа на уровне транзакций (6) Электронная подпись, закрытие контекста на уровне документов (14) Контроль доступа посторонних в помещения, охрана помещения администратора
33. Нарушение целостности потока сообщений	(1) Криптозащита, туннелирование и векторизация IP-пакетов, имплементируемая в FireWall-устройства (2) Настройка политики безопасности при помощи FireWall-устройств (3) Туннелирование и векторизация IP-пакетов (4) Аутентификация на уровне транзакций (5) Контроль доступа на уровне транзакций (6) Электронная подпись, закрытие контекста на уровне документов
34. Взлом системы (хакерами)	(1) Криптозащита, туннелирование и векторизация IP-пакетов, имплементируемая в FireWall-устройства (2) Настройка политики безопасности при помощи FireWall-устройств (3) Туннелирование и векторизация IP-пакетов (4) Аутентификация на уровне транзакций (5) Контроль доступа на уровне транзакций (6) Электронная подпись, закрытие контекста на уровне документов
Класс 7. Неумышленные действия персонала	
35. Некорректное выполнение расчетов	(24) Высокая степень отладки ПО, самоконтроль ПО, контроль вводимой информации, обратимость операций
36. Ошибочный ввод данных	(5) Контроль доступа на уровне транзакций (6) Электронная подпись, закрытие контекста на уровне документов (7) Контроль действий оператора: протоколы событий,

Атаки	Меры защиты
	периодические или событийные повторы контроля полномочий, криптозащита информации в локальной сети (24) Высокая степень отладки ПО, самоконтроль ПО, контроль вводимой информации, обратимость операций
Класс 8. Атака на информационную часть системы защиты	
37. Взлом системы	(2) Настройка политики безопасности при помощи FireWall-устройств (3) Туннелирование и векторизация IP-пакетов (10) Усиленные режим контроля НСД на рабочем месте администратора системы безопасности; отключение от сети в пассивном состоянии (11) Особый режим хранения информации администратора системы безопасности (14) Контроль доступа посторонних в помещения, охрана помещения администратора
38. Нарушение базы данных защиты	(10) Усиленные режим контроля НСД на рабочем месте администратора системы безопасности; отключение от сети в пассивном состоянии (11) Особый режим хранения информации администратора системы безопасности (14) Контроль доступа посторонних в помещения, охрана помещения администратора
39. Раскрытие, перехват, хищение кодов, ключей, паролей	(1) Криптозащита, туннелирование и векторизация IP-пакетов, имплементируемая в FireWall-устройства (3) Туннелирование и векторизация IP-пакетов (7) Контроль действий оператора: протоколы событий, периодические или событийные повторы контроля полномочий, криптозащита информации в локальной сети (8) Работа с контролируемыми магнитными носителями, вирусопрофилактика (9) Контроль доступа операторов к системе, варианты (10) Усиленные режим контроля НСД на рабочем месте администратора системы безопасности; отключение от сети в пассивном состоянии (11) Особый режим хранения информации администратора системы безопасности (14) Контроль доступа посторонних в помещения, охрана помещения администратора

6.5. Требования по выполнению организационных мер защиты информации в ПС определены во внутренних нормативных документах.

6.6. Технические меры, принимаемые для защиты информации в ПС, актуализируются на регулярной основе и результатах инвентаризации информационных активов (элементов ИТ-инфраструктуры) Общества, включают:

	Наименование средств защиты
1)	Средства идентификации и аутентификации
2)	Средства управления доступом
3)	Средства межсетевого экранирования
4)	Средства защиты каналов передачи данных
5)	Антивирус и антиспам
6)	Средства обнаружения вторжений
7)	Средства анализа защищенности
8)	Средства мониторинга событий ИБ
9)	Средства защиты среды виртуализации
10)	Средства резервного копирования
11)	Физическая охрана, СКУД, средства видеонаблюдения, противопожарная сигнализация

6.7. Средства идентификации и аутентификации

Идентификация и аутентификация пользователей происходит встроенными средствами ОС, а также установленными групповыми политиками безопасности домена и Active Directory (AD).

– В групповых политиках безопасности установлено сложность пароля, и смена пароля не реже чем через 30 дней.

– Настроена блокировка пользователя при не верном вводе пароля.

– Учетные данные проверяются по базе данных диспетчера учетных записей безопасности в Active Directory, присоединенном к домену, через службу Winlogon.

6.8. Система управления доступом (СУД)

Система управления доступом (СУД) внедрена в организацию для реализации управления правами доступа пользователей к корпоративным документам.

СУД позволяет решить следующие задачи:

– наладить работу с учетными записями сотрудников;

– автоматически выполнять синхронизацию кадровых изменений;

– автоматически выдавать право доступа пользователю к информационной системе;

– упростить аудит прав;

– автоматически определять неиспользуемые учетные записи;

– предотвращать случаи несанкционированного использования данных.

Файловые информационные ресурсы (ФИР), представляющие собой сочетания файлов и папок, которые хранятся в отдельной базе (корневой каталог).

Файловые составные ресурсы. Могут включать один или более файловых ресурсов. Сюда также входит вложенный ресурс.

Точка входа, группа доступа пользователей и промежуточный каталог. Под точкой входа понимается каталог файловой системы, к которому пользователи могут получить сетевой доступ. Под группой доступа пользователей подразумевается набор пользователей, наделенных полномочиями, позволяющими им пользоваться файловыми информационными ресурсами. Промежуточный каталог представляет собой такой каталог, который находится между точкой входа в ФИР и корневым каталогом.

- Разграничение доступа происходит исключительно на уровне каталогов.
- Права назначаются на основе групп, а не отдельных пользователей.
- Разграничены права исключительно на уровне файловой системы.
- Запрещено создавать файловые информационные ресурсы на компьютерах пользователей.
- Запрещено размещение и создание ФИР в системных каталогах, хранящихся на серверах.
- Запрещено создание нескольких точек входа в ФИР.
- Запрещено создавать вложенные ФИР, если хранящиеся в них данные включают конфиденциальную информацию.
- Для изменения учетных данных пользователь формирует заявку, в которой указывает причины необходимости внесения изменений в учетную запись. Заявка согласуется с ответственным администратором.

6.9. Средства межсетевого экранирования и защиты каналов передачи данных

Для защиты периметра ЛВС, а также ЛВС Дата-Центра ЦОД Общества от различных типов угроз используются сетевые программно-аппаратные средства защиты информации:

- Программный маршрутизатор/ файрволл используется в ЛВС офиса.
- Межсетевой экран используется в ЛВС Дата-Центра ЦОД Общества.
- Антивирус.
- Маршрутизаторы для сегментирования трафика V-Lan используется в ЛВС офиса.

Программный маршрутизатор/ файрволл выполняет следующие функции ИБ в ЛВС офиса:

- Межсетевое экранирование.
- Фильтрация траффика на уровне приложений.
- Маршрутизатор.
- Система обнаружения и предотвращения вторжений.
- Система выявления и предотвращения вредоносной активности сети (в том числе «бот-сетей»).
- Поточный антивирус HAVP antivirus и SquidGuard.

- Создание сети VLAN для сегментации трафика.
- Повышает надежность и отказоустойчивость сети.
- Позволяет настраивать site-to-site и point-to-site VPN.
- Открывает порты в NAT (Port forwarding).
- Стандартная фильтрация на основе адресов и портов источника/ назначения.
- Фильтрация на основе фингерпринтинга ОС, с которой устанавливается соединение (используется средство пассивного фингерпринтинга p0f).
- Прозрачный брандмауэр второго уровня.
- Нормализация пакетов отбрасывание пакетов с неправильно сформированными полями, которые могу быть и специфическим путем атаки.
- Поддержка состояния соединений возможности бэкенда. Поддерживается в том числе и Syn-прокси для защиты некоторых служб от Syn-flood-атак.
- Гибкая поддержка NAT.
- VPN – поддерживаются IPSec, PPTP и OpenVPN.
- Мониторинг и статистика. Рисование графиков с помощью RRD и в реальном времени.

Межсетевой экран выполняет следующие функции ИБ для защиты серверного сегмента:

- Межсетевое экранирование.
- Фильтрация траффика на уровне приложений.
- Маршрутизатор.
- Система обнаружения и предотвращения вторжений.
- Система выявления и предотвращения вредоносной активности сети (в том числе «бот-сетей»).
- Создание сети VLAN для сегментации трафика.
- Повышает надежность и отказоустойчивость сети.
- Позволяет настраивать site-to-site и point-to-site VPN.
- Поточный антивирус.

Маршрутизаторы (коммутаторы) выполняют следующие функции ИБ в ЛВС офиса ЦП:

- Создание сети VLAN для сегментации трафика.
- Маршрутизация трафика.

Настройки и конфигурация сетевого оборудования и сетевых программно-аппаратных средств защиты информации:

1. На коммутаторах настроен межсетевой доступ.

2. Настроена автоматическая отправка файлов событий в систему управления событиями информационной безопасности (SIEM).
3. Идентификация и авторизация на сетевом оборудовании производится в соответствии с внутренними требованиями по парольной политике Общества.
4. Настроен Port Security, с целью исключения несанкционированного подключения к ЛВС Общества сторонних устройств. В случае, если подключается устройство с неизвестным ранее MAC-адресом, порт автоматически отключается, в журнал событий безопасности делается соответствующая запись.

Настройки программного маршрутизатора/ файрволла:

1. Топология сети Общества скрыта со стороны сети Интернет.
2. Запрещен удаленный доступ к инфраструктуре Общества. Разрешен только для VPN удаленной работы сотрудников.
3. Контур формирования электронных сообщений и контур контроля реквизитов электронных сообщений платежной системы Банка России размещены в разных сегментах ЛВС. Реализована сетевая изоляция с использованием NAT указанных контуров, а также однонаправленная передача данных.
4. Заблокированы файлообменные сети.
5. Заблокирован протокол QUIC.
6. Заблокированы приложения анонимного доступа, в том числе TOR.
7. Заблокированы бот-сети.
8. Разрешен доступ к сети Интернет и VPN для удаленной работы сотрудников.
9. Запрещено всё, что не разрешено.
10. Включена система обнаружения и предотвращения вторжений.
11. Настроена автоматическая отправка файлов событий на систему управления событиями информационной безопасности (SIEM).
12. Настроены белые списки сайтов, необходимых сотрудникам для выполнения служебных обязанностей. Тем сотрудникам, которым Интернет не нужен для выполнения служебных обязанностей, Интернет заблокирован полностью.
13. Заблокированы социальные сети.
14. Заблокирован доступ к сайтам с подозрением на вредоносную активность.
15. Настроен поточный антивирус HAVP antivirus и SquidGuard для проверки входящего трафика.
16. Настроена сегментация распределения сетевого трафика V-Lan.

6.10. Антивирус и антиспам выполняет следующие функции ИБ:

– Обеспечение антивирусной защиты на компьютерах под управлением Windows.

– Централизованная установка антивирусных агентов (с возможностью настройки ПО агентов на сервере до его установки на клиентские машины).

- Упрощенное управление рабочими станциями антивирусной сети за счет использования механизма групп.
- Возможность использования на антивирусной станции спам-фильтра.
- Быстрое и эффективное распространение сервером Dr.Web Enterprise Security Suite обновлений вирусных баз и программных модулей на защищаемые рабочие станции.
- Минимизация сетевого трафика локальных сетей, построенных на основе протоколов TCP/IP, IPX, за счет применения специальных алгоритмов сжатия.
- Возможность шифрования данных при обмене между различными компонентами системы.
- Детектирование и нейтрализация вирусов и вредоносных кодов различного типа, спама, фишинг-, фарминг-, скамминг- и bounce-сообщений.
- Корректная обработка большинства известных типов архивов, в том числе многотомных и самораскрывающихся (SFX).
- Защита работы собственных модулей от сбоев.
- Отправка уведомлений о результатах проверки как получателям, так и другим лицам.
- Изоляция зараженных объектов и спама в карантине.
- Ведение статистики, учитывающей все аспекты работы системы.
- Активная защита от атак спамеров и хакеров.
- Проверка подлинности IP-адреса.
- Защита от спам-ловушек.
- Экономия интернет-трафика за счет проведения ряда проверок до полной загрузки сообщения.
- Возможность регулирования доступа к Open Relays серверам.
- Фильтрация доступа к ресурсам сети Интернет по типу (mime), по размеру файлов, по названию хоста.
- Регулирование доступа к веб-ресурсам различного типа.

Настройки и конфигурация Антивируса:

1. На рабочих станциях настроена комплексная защита компьютеров под управлением Windows от вирусов и спама.
2. Настроена групповая политика безопасности на ежедневное сканирование рабочих станция для выявления вредоносных программ.
3. Включено распространение сервером обновлений вирусных баз и программных модулей на защищаемые рабочие станции.
4. Групповой политикой запрещено паролем закрывание и приостановка сканирования антивируса пользователем.
5. Включена поточная проверка сетевого трафика.
6. Групповой политикой включена принудительная проверка съемных носителей.
7. Включено блокирование внешних съемных носителей, не зарегистрированных в ЦУ.

8. Включена активная защита от атак спамеров и хакеров.
9. Включен спам-фильтр.
10. Настроена автоматическая отправка файлов событий на систему управления событиями информационной безопасности (SIEM).

6.11. Средства обнаружения вторжений и мониторинга событий ИБ (SIEM) выполняет следующие функции ИБ:

- Осуществляется сбор логов из различных программных и аппаратных источников, что позволяет работать с ними в рамках единого интерфейса.
- Ведется анализ событий и формирование инцидентов в соответствии с правилами. Детектирование угроз путем выявления корреляций событий и(или) инцидентов.
- Настроено автоматическое извещение ответственных лиц об инцидентах и предоставление информации, необходимой для проведения расследования.
- Производится вычитка и анализ журнала Windows Event Log, контроллеров доменов и серверов Windows, вычитка и анализ по протоколу LDAP информации об учётных записях.

6.12. Средства анализа защищенности сканер уязвимостей

- В Обществе используется профессиональный сканер уязвимостей, позволяющий оценить состояние защищенности IT-инфраструктуры. Выявляет компоненты сети, анализирует их на уязвимости и предоставляет подробные рекомендации по устранению.
- Сканер своевременно обнаруживает уязвимости в инфраструктуре компании и тем самым предотвращает возможные атаки с их использованием до наступления негативных последствий.
- Помогает соответствовать требованиям закона № 152-ФЗ, приказов ФСТЭК № 21, 17, 31 и 239, международного стандарта PCI DSS.

6.13. Средства защиты среды виртуализации выполняет следующие функции ИБ:

- Формирует единый контур защиты виртуализации для сред VMware, Microsoft Hyper-V. Это унифицирует политики безопасности и отчетности в гетерогенной среде.
- Контроль рабочего места администратора, сервера управления и хоста гипервизора обеспечивает целостную защиту приложений от атак со стороны виртуальной инфраструктуры.
- Корреляция событий и среды виртуализации выявляет несанкционированную активность и позволяет обнаружить инцидент до того, как он приведет к разрушительным последствиям.
- Встроенные шаблоны настроек безопасности обеспечивают требуемый регуляторами уровень защиты ИТ-инфраструктуры с минимальными усилиями со стороны обслуживающего персонала.

6.14. Средства резервного копирования и восстановление данных выполняют следующие функции ИБ:

- Средство резервного копирования проверяет приложения на предмет наличия открытых уязвимостей методом обращения к непрерывно обновляемым базам уязвимостей ОС Windows и Linux и приложений, работающих под их управлением.
- Выгрузка снимков виртуальных машин VMware.
- Дедупликация блоков переменного размера.
- Резервное копирование виртуальных машин под управлением гипервизоров VMWare, Hyper-V, Scale Computing, а также KVM oVirt, zVirt, Rosa Virtualization, Red Hat Virtualization.
- Защита от вирусов-шифровальщиков, непрерывно обучаемый выявлению несанкционированных операций шифрования ИИ работает на базе специального модуля, который анализирует содержимое и тип данных до изменения и реагирует при выявлении изменений.
- Защита от криптомайнеров, автоматическое выявление и остановка процессов майнинга криптовалют в реальном времени.
- Оценка уязвимостей ОС и приложений, оценка уязвимостей для противодействия атакам для Windows и Linux методом сканирования машин и сравнения результатов с центральными базами уязвимостей, информирование администраторов и службы ИБ об открытых уязвимостях с указанием степени их критичности в интерфейсе консоли или методом автоматического сохранения и рассылки отчётов.

6.15. В Обществе, не реже 1 раза в 2 года, проводится оценка соответствия СОИБ ПС требованиям законодательства Российской Федерации и нормативных актов Банка России по защите платежных систем. Результаты оценки оформляются в виде Отчета по форме, установленной Банком России.

7. Мониторинг и конфигурирование средств защиты информации

7.1. Каждое средство защиты информации, установленное в ГО, должно быть настроено работниками УЭИС на отправку событий ИБ на серверы мониторинга событий ИБ (СМСИБ). Под событиями ИБ понимаются события аутентификации, авторизации, сеансов входа или выхода из системы, изменение конфигурации и компонентов системы.

7.2. Мониторинг состояния ИБ осуществляется с целью выполнения требований Политики ИБ Общества, требований действующего Стандарта Банка России СТО ИББС, на основании требований Стандарта PCI DSS и на основании нормативных документов Общества, перечисленных п. 1.5 настоящего Положения.

7.3. Регистрация событий ИБ на средствах защиты информации в ГО обеспечивается централизованно для каждого средства в режиме доступа к логам событий с периодом за 3 месяца. Установленное и используемое средство защиты информации должно быть переключено на мониторинг на выделенный сервер СМСИБ. Средство защиты информации настраивается на хранение всех событий регистрации пользователей и событий ИБ.

7.4. На средстве защиты информации должна фиксироваться любая попытка регистрации операторов с передачей данных на сервер регистрации событий. В лог-файлах должны фиксироваться следующие данные: уникальный идентификатор администратора или оператора сетевого оборудования, назначаемый руководителем или его заместителем в УЭИС, время доступа, IP адрес доступа, время окончания сессии.

Доступ к лог-файлам событий данного сервера в режиме чтения должен быть доступен Администраторам ИБ или работникам ОИБ по согласованию с УЭИС.

7.5. Средства защиты информации в ГО, ОП и у Партнера должны быть настроены на централизованные сервера учета времени (по протоколу ntp) с ежедневной синхронизацией времени.

7.6. Журналы регистрации событий ИБ и регистрации пользователей должны храниться на серверах СМСИБ в режиме доступа не менее чем за 3 месяца. В режиме архивации журналы регистрации событий должны храниться за период не менее 1 года.

7.7. Доступ к электронным журналам ИБ, хранимых в СМСИБ, предоставляется по требованию Администраторов ИБ или работников ОИБ в режиме чтения.

7.8. Внесение изменений в конфигурацию средств защиты информации в ГО производится работниками ГО УЭИС на основании заявки на доступ (смотри Приложение 1). Работник УЭИС обязан обеспечивать точное заполнение вышеперечисленных заявок и, в случае возникновения инцидента, ИБ обязан документально известить руководителей УЭИС.

7.9. Сохранность конфигураций по средствам защиты информации обеспечивается регулярным копированием текущей и загруженной конфигурации СЗИ на выделенный сервер хранения конфигураций в УЭИС в ГО и ОП с подсчетом контрольных сумм сохраненных файлов конфигураций. Доступ к серверам хранения конфигураций предоставляется работникам УЭИС и ОИБ в соответствии с возложенными на них обязанностями (на основании должностных инструкций).

7.10. Проведение профилактических и плановых работ на средствах защиты информации проводится только с разрешения руководителя подразделения, ответственного за сопровождение и эксплуатацию средств защиты информации ГО или ОП, и при наличии согласованного плана работ. В случае возникновения риска простоя оборудования необходимо оповестить руководителя эксплуатирующего подразделения Общества с указанием возможного времени простоя оборудования в официальном порядке служебной запиской.

7.11. Все работы специалистами УЭИС по изменению конфигурации средств защиты информации производятся только в рамках выполнения ими своих должностных обязанностей. Вносимые изменения в конфигурацию оборудования должны фиксироваться на выделенном сервере хранения конфигураций в УЭИС.

7.12. При внесении изменений в конфигурацию средств защиты информации работники УЭИС должны убедиться в наличии предыдущей конфигурации. После внесения изменений в конфигурацию работники УЭИС обязаны сохранить ее в новой редакции на сервере хранения конфигураций.

7.13. Использование незащищенных протоколов связи (http/telnet/ftp/tftp) при конфигурировании средств защиты информации запрещено, для конфигурирования должны быть использованы защищенные протоколы такие как SSL/SSH. На оборудовании при использовании SNMP community должны быть изменены их имена таким образом, чтобы они содержали не менее 8 символов, числа и спецсимволы.

7.14. Хранение конфигураций средств защиты информации СЗИ обеспечивается в УЭИС на выделенном ресурсе, доступном только работникам подразделения. Администратор ИБ в режиме чтения обязан регулярно проводить аудит действующей конфигурации средств защиты информации СЗИ.

7.15. Внесение изменений в конфигурацию оборудования проводится вначале на тестовом стенде с и только после положительного результата тестирования и согласования с руководством УЭИС эти изменения заносятся в работающую конфигурацию.

7.16. На вновь установленном средстве защиты информации должны быть изменены все заводские логины и пароли, установленные производителем по умолчанию. В случае невозможности смены заводских паролей эти учетные записи или записи с гостевым входом должны быть отключены.

7.17. УЭИС не реже одного раза в год проводит инвентаризацию средств защиты информации в ГО с помощью аппаратно-программных средств компании Cisco и других. Данные мониторинга актуализируется на серверах резервного копирования. В ходе инвентаризации определяется количество установленных устройств, версии операционных систем и установленные обновления, а также проверяются роли доступа.

7.18. Регулярно УЭИС совместно с ОИБ проводит мероприятия ИБ по мониторингу состояния средств защиты информации путем сравнения результатов предыдущей инвентаризации средств защиты информации с текущей и анализа лог-файлов событий ИБ.

7.19. Доступ к средствам защиты информации предоставляется работникам УЭИС, назначенным Администратором СЗИ приказом Общества.

7.20. Внесение изменений в конфигурацию средств защиты информации СЗИ производится по согласованию с руководителем УЭИС на основании Приложения 5.

8. Порядок предоставления доступа к СЗИ

8.1. Средства защиты информации делится на четыре области – СЗИ установленное в ГО, ОП, у партнера и установленное за пределами опорной сети Общества.

8.2. Доступ к средствам защиты информации предоставляется на основании распоряжения руководителя УЭИС в соответствии с должностными обязанностями и требованиями нормативных документов Общества. Доступ предоставляется в режиме оператора на основании распоряжения руководителя УЭИС и в режиме администратора – на основании приказа Общества.

Доступ представителям сторонних организаций к просмотру конфигураций средств защиты информации может быть предоставлен только в рамках выполнения ими функций по техническому сопровождению оборудования или программного обеспечения при заключении сервисного договора на обслуживание. Порядок организации доступа, а также проводимые работы должны быть согласованны с ОИБ. При проведении аудита СЗИ доступ к средствам защиты информации предоставляется только в режиме чтения при непосредственном участии администратора данного сетевого комплекса и АИБ.

8.3. Выполнение функций по сопровождению и администрированию средств защиты информации должно производиться только с АРМ администраторов средств защиты информации с назначенными правами доступа на межсетевом экране.

8.4. Каждое средство защиты информации должно иметь защищенный интерфейс к административной консоли с использованием протоколов ssh, https.

8.5. Доступ в режиме администратора предоставляется работникам, которые выполняют функции администрирования средств защиты информации. Доступ должен

быть персонализирован с уникальной учетной записью каждого работника в режиме администрирования согласно требованиям настоящего Положения, в том числе и Приложения 1.

8.6. Доступ к средствам защиты информации в режиме оператора предоставляется в режиме чтения аудиторам, администраторам ИБ и другим работникам для выполнения ими своих функций по мониторингу и контролю состояния ИБ в рамках выполнения ими своих должностных обязанностей.

8.7. Предоставление доступа работнику ГО к средствам защиты информации производится на основании Раздела 3 Регламента предоставления пользователям доступа к информационным ресурсам вычислительной сети УЭИС путем заведения руководителем УЭИС или его заместителем идентификатора пользователя и указания его роли (администратор или оператор). Каждый работник, выполняющий функции администратора или оператора, должен соблюдать установленный порядок обращения с паролями доступа, закрепленный Правилами выбора пароля в Раздела 5 Регламента предоставления пользователям доступа к информационным ресурсам вычислительной сети.

9. Порядок внесения изменений

9.1. Внесение изменений в требования к защите информации в ПС производится в следующих случаях:

- при изменениях в законодательных актах Российской Федерации;
- при изменениях в нормативных актах Банка России, регулирующих отношения в национальной платежной системе;
- при совершенствовании ПС и(или) порядка защиты информации в ПС;
- при изменении Правил ПС и(или) порядка оказания услуг.

9.2. При внесении изменений во внутренние организационно-распорядительные документы СОИБ необходимо руководствоваться требованиями внутреннего нормативного документа «Процедура управления документами СОИБ».

Приложение №1

к Положению о защите информации
в Платежной системе «Sendy»

Порядок внесения изменений в средства защиты информации

1. Общие положения

1.1. Любые процессы внесения изменений в конфигурацию средств защиты информации и сетевые соединения обязательно подвергаются процедуре тестирования в УЭИС. Типовые инструкции по процедуре настройке средств защиты информации разрабатываются в УЭИС.

1.2. Результаты внесения изменений документируются работниками из числа администраторов СЗИ. В процессе тестировании должны принимать участие работники всех заинтересованных подразделений1.

1.3. Положительное решение о внесении изменений в СЗИ принимается только в случае отсутствия замечаний со стороны других подразделений.

2. Изменение конфигурации

2.1. Внесение изменений в конфигурацию или установка обновлений на средстве защиты информации производится только после тестирования изменений в тестовой среде данной конфигурации с участием УЭИС. В случае необходимости создается новая процедура тестирования с участием работников из других подразделений Общества.

2.2. Администратор СЗИ УЭИС выполняют следующую последовательность шагов по внесению изменений в сетевом оборудовании:

- сохраняют действующую конфигурацию средства защиты информации;
- проводит изменения в имеющихся стандартах конфигурирования на основании согласованных результатов тестирования или полученными рекомендациями от производителей, ОИБ;
- выполняют проверку работоспособности после внесенных изменений;
- в случае неработоспособности внесенных изменений в конфигурацию средств защиты информации выполняется процедура отката, созданная на этапе тестирования.

3. Контроль и сохранение конфигурации

3.1. В УЭИС должен быть настроен механизм копирования конфигурации средств защиты информации на выделенный сервер хранения конфигураций.

[1] Под заинтересованными подразделениями понимаются эксплуатирующее, сопровождающее и подразделение, контролирующее состояние ИБ.

3.2. Доступ к серверу хранения конфигурация предоставляется Администраторам резервного копирования в режиме администрирования. По конфигурациям, хранимым на сервере конфигураций, после копирования их со средств защиты информации должен проводиться подсчет контрольных сумм в формате MD5.

3.3. После внесения изменений Администратором СЗИ в конфигурацию оборудования и Администратор резервного копирования производит проверку загруженной и сохраненной конфигурации за текущий день.

3.4. Периодичность сохранения конфигурации (загруженной и сохраненной) составляет не менее 1 года. На сервере сохранения конфигураций должны фиксироваться следующие данные:

- дата конфигурации;
- сохраненная конфигурация;
- загруженная конфигурация;
- название устройства;
- место расположения устройства.

3.5. На средствах защиты информации должен быть настроен разрешенный механизм передачи конфигураций на сервер хранения конфигураций. Передача конфигураций осуществляется только по защищенному протоколу SSH.

3.6. Доступ на сервер хранения конфигураций настраивается по защищенному протоколу SSH только с IP адресов рабочих мест Администраторов резервного копирования. Ограничение доступа по протоколу SSH настраивается штатными средствами сервиса SSHD.

3.7. На сервере должны быть запрещены все неиспользуемые протоколы. Данный сервер используется также для еженедельного сохранения конфигураций СМСИБ.

3.8. На сервере хранения конфигураций обеспечивается регулярная проверка загруженной и сохраненной конфигурации. При возникновении расхождения в контрольных суммах файлов сервер хранения конфигураций отсылает сообщение по электронной почте Администраторам резервного копирования.

3.9. Администраторы резервного копирования производят обновление системы хранения конфигураций при появлении критических уязвимостей ОС с периодичностью по мере выхода обновлений, остальные обновления устанавливаются не реже 1 раза в год.