ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57580.1— 2017

Безопасность финансовых (банковских) операций

ЗАЩИТА ИНФОРМАЦИИ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

Базовый состав организационных и технических мер

Издание официальное

Москва
Стандартинформ
2020

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Центральным банком Российской Федерации (Банк России) и Научно-производственной фирмой «КРИСТАЛЛ» (НПФ «КРИСТАЛЛ»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 122 «Стандарты финансовых операций»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 822-ст

4 ВВЕДЕН ВПЕРВЫЕ

5 ИЗДАНИЕ (февраль 2020 г.) с Поправкой (ИУС 4—2018)

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Стандартинформ, оформление, 2017, 2020

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения . . . 1
2 Нормативные ссылки . . . 1
3 Термины и определения . . . 2
4 Обозначения и сокращения . . . 6
5 Назначение и структура стандарта . . . 6
6 Общие положения . . . 7
7 Требования к системе защиты информации . . . 10
7.1 Общие положения . . . 10
7.2 Процесс 1 «Обеспечение защиты информации при управлении доступом» . . . 11
7.3 Процесс 2 «Обеспечение защиты вычислительных сетей» . . . 19
7.4 Процесс 3 «Контроль целостности и защищенности информационной инфраструктуры» . . . 25
7.5 Процесс 4 «Защита от вредоносного кода» . . . 28
7.6 Процесс 5 «Предотвращение утечек информации» . . . 31
7.7 Процесс 6 «Управление инцидентами защиты информации» . . . 33
7.8 Процесс 7 «Защита среды виртуализации» . . . 38
7.9 Процесс 8 «Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств» . . . 42
8 Требования к организации и управлению защитой информации . . . 44
8.1 Общие положения . . . 44
8.2 Направление 1 «Планирование процесса системы защиты информации» . . . 45
8.3 Направление 2 «Реализация процесса системы защиты информации» . . . 46
8.4 Направление 3 «Контроль процесса системы защиты информации» . . . 47
8.5 Направление 4 «Совершенствование процесса системы защиты информации» . . . 48
9 Требования к защите информации на этапах жизненного цикла автоматизированных систем и приложений . . . 49
Приложение А (справочное) Основные положения базовой модели угроз и нарушителей безопасности информации . . . 54
Приложение Б (справочное) Состав и содержание организационных мер, связанных с обработкой финансовой организацией персональных данных . . . 56
Приложение В (справочное) Перечень событий защиты информации, потенциально связанных с несанкционированным доступом и инцидентами защиты информации, рекомендуемых для выявления, регистрации и анализа . . . 59
Библиография . . . 60

Введение

Развитие и укрепление банковской системы Российской Федерации, развитие и обеспечение стабильности финансового рынка Российской Федерации и национальной платежной системы являются целями деятельности Банка России [1]. Одним из основных условий реализации этих целей является обеспечение необходимого и достаточного уровня защиты информации в кредитных организациях, некредитных финансовых организациях РФ, а также субъектах национальной платежной системы (далее при совместном упоминании — финансовые организации).

В случаях наступления инцидентов защиты информации их негативные последствия в работе отдельных финансовых организаций могут привести к быстрому развитию системного кризиса банковской системы, финансового рынка Российской Федерации и (или) национальной платежной системы, нанести существенный ущерб интересам собственников и клиентов финансовых организаций. Поэтому для финансовых организаций угрозы безопасности информации представляют существенную опасность, а обеспечение защиты информации является для финансовых организаций одним из основополагающих аспектов их деятельности.

Для противостояния угрозам безопасности информации и их влиянию на операционный риск финансовым организациям следует обеспечить необходимый и достаточный уровень защиты информации, а также сохранять этот уровень при изменении условий как внутри, так и вне организаций.

Банк России в пределах своей компетенции [1], [2] по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, устанавливает в нормативных актах Банка России для финансовых организаций требования к обеспечению защиты информации при осуществлении банковской деятельности и деятельности в сфере финансовых рынков.

Основными целями настоящего стандарта являются:

- определение уровней защиты информации и соответствующих им требований к содержанию базового состава организационных и технических мер защиты информации (далее при совместном упоминании — мер защиты информации), применяемых финансовыми организациями для реализации требований к обеспечению защиты информации, установленных нормативными актами Банка России;
- достижение адекватности состава и содержания мер защиты информации, применяемых финансовыми организациями, актуальным угрозам безопасности информации и уровню принятого финансовой организацией операционного риска (риск-аппетиту);
- обеспечение эффективности и возможности стандартизированного контроля мероприятий по защите информации, проводимых финансовыми организациями.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Безопасность финансовых (банковских) операций

ЗАЩИТА ИНФОРМАЦИИ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

Базовый состав организационных и технических мер

Security of financial (banking) operations. Information protection of financial organizations.
Basic set of organizational and technical measures

Дата введения — 2018—01—01

1 Область применения

Настоящий стандарт определяет уровни защиты информации и соответствующие им требования к содержанию базового состава мер защиты информации, которые применяются финансовыми организациями для реализации требований к обеспечению защиты информации, установленных нормативными актами Банка России.

Положения настоящего стандарта предназначены для использования кредитными организациями, некредитными финансовыми организациями, указанными в части первой статьи 76.1 Федерального закона «О Центральном банке Российской Федерации (Банке России)» [1], а также субъектами национальной платежной системы.

Базовый состав мер защиты информации, определяемый настоящим стандартом, применим к совокупности объектов информатизации, в том числе автоматизированным системам (АС), используемым финансовыми организациями для выполнения бизнес-процессов и (или) технологических процессов, связанных с предоставлением финансовых, банковских услуг, а также услуг по осуществлению переводов денежных средств (далее при совместном упоминании — финансовые услуги).

Область применения настоящего стандарта, определяющая обязанность финансовых организаций применять меры защиты информации, реализующие один из уровней защиты информации для конкретной совокупности объектов информатизации, в том числе АС, используемых финансовыми организациями для предоставления финансовых услуг, устанавливается в нормативных актах Банка России путем включения нормативной ссылки на настоящий стандарт, приводимой на основании статьи 27 Федерального закона «О стандартизации в Российской Федерации» [3].

Настоящий стандарт применяется путем включения нормативных ссылок на него в нормативных актах Банка России и (или) прямого использования устанавливаемых в нем требований во внутренних документах финансовых организаций, а также в договорах.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ 34.003 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения

ГОСТ Р ИСО/МЭК 7498-1 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель

ГОСТ Р 50739 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования

ГОСТ Р 50922 Защита информации. Основные термины и определения

Издание официальное

ГОСТ Р 56545 Защита информации. Уязвимости информационных систем. Правила описания уязвимостей

ГОСТ Р 56546 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем

ГОСТ Р 56938 Защита информации. Защита информации при использовании технологии виртуализации. Общие положения

ГОСТ Р ИСО/ТО 13569 Финансовые услуги. Рекомендации по информационной безопасности

ГОСТ Р ИСО/МЭК ТО 18044 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности

ГОСТ Р ИСО/МЭК 27033-1 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции

ГОСТ Р ИСО/МЭК 15408-3 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ Р 50922, ГОСТ 34.003, ГОСТ Р 56545, ГОСТ Р 56546, а также следующие термины с соответствующими определениями:

3.1 **меры защиты информации:** Организационные (в том числе управленческие) и технические меры, применяемые для защиты информации и обеспечения доступности АС.

Примечание — Адаптировано из ГОСТ Р ИСО/МЭК ТО 19791.

3.2 **техническая мера защиты информации:** Мера защиты информации, реализуемая с помощью применения аппаратных, программных, аппаратно-программных средств и (или) систем.

3.3 **организационная мера защиты информации:** Мера, не являющаяся технической мерой защиты информации, предусматривающая установление временных, территориальных, пространственных, правовых, методических и иных ограничений на условия использования и режимы работы объекта информатизации и (или) иных связанных с ним объектов.

3.4 **система защиты информации:** Совокупность мер защиты информации, применение которых направлено на непосредственное обеспечение защиты информации, процессов применения указанных мер защиты информации, ресурсного и организационного обеспечения, необходимого для применения указанных мер защиты информации.

3.5 **система организации и управления защитой информации:** Совокупность мер защиты информации, применение которых направлено на обеспечение полноты и качества защиты информации, предназначенных для планирования, реализации, контроля и совершенствования процессов системы защиты информации.

3.6 **объект информатизации финансовой организации (объект информатизации):** Совокупность объектов и ресурсов доступа, средств и систем обработки информации, в том числе АС, используемых для обеспечения информатизации бизнес-процессов и (или) технологических процессов финансовой организации, используемых для предоставления финансовых услуг.

Примечание — Адаптировано из ГОСТ Р 51275.

3.7 **технологический процесс финансовой организации (технологический процесс):** Набор взаимосвязанных операций с информацией и (или) объектами информатизации, используемых при

функционировании финансовой организации и (или) необходимых для предоставления финансовых услуг.

3.8 **объект доступа:** Объект информатизации, представляющий собой аппаратное средство, средство вычислительной техники и (или) сетевое оборудование, в том числе входящие в состав АС финансовой организации.

Примечание — В составе основных типов объектов доступа рекомендуется как минимум рассматривать:

- автоматизированные рабочие места (АРМ) пользователей;
- АРМ эксплуатационного персонала;
- серверное оборудование;
- сетевое оборудование;
- системы хранения данных;
- аппаратные модули безопасности (HSM);
- устройства печати и копирования информации;
- объекты доступа, расположенные в публичных (общедоступных) местах (в том числе банкоматы, платежные терминалы).

3.9 **ресурс доступа:** Объект информатизации, представляющий собой совокупность информации и программного обеспечения (ПО) обработки информации.

Примечание — В составе основных типов ресурсов доступа рекомендуется как минимум рассматривать:

- АС;
- базы данных;
- сетевые файловые ресурсы;
- виртуальные машины, предназначенные для размещения серверных компонентов АС;
- виртуальные машины, предназначенные для размещения АРМ пользователей и эксплуатационного персонала;
- ресурсы доступа, относящиеся к сервисам электронной почты;
- ресурсы доступа, относящиеся к WEB-сервисам финансовой организации в сетях Интранет и Интернет.

3.10 **контур безопасности:** Совокупность объектов информатизации, определяемая областью применения настоящего стандарта, используемых для реализации бизнес-процессов и (или) технологических процессов финансовой организации единой степени критичности (важности), для которой финансовой организацией применяется единая политика (режим) защиты информации (единый набор требований к обеспечению защиты информации).

3.11 **уровень защиты информации:** Определенная совокупность мер защиты информации, входящих в состав системы защиты информации и системы организации и управления защитой информации, применяемых совместно в пределах контура безопасности для реализации политики (режима) защиты информации, соответствующей критичности (важности) защищаемой информации бизнес-процессов и (или) технологических процессов финансовой организации.

3.12 **физический доступ к объекту доступа (физический доступ):** Доступ к объекту доступа, включая доступ в помещение, в котором расположен объект доступа, позволяющий осуществить физическое воздействие на него.

3.13 **логический доступ к ресурсу доступа (логический доступ):** Доступ к ресурсу доступа, в том числе удаленный, реализуемый с использованием вычислительных сетей, позволяющий, в том числе без физического доступа, осуществить доступ к защищаемой информации или выполнить операции по обработке защищаемой информации.

3.14 **субъект доступа:** Работник финансовой организации или иное лицо, осуществляющий физический и (или) логический доступ, или программный сервис, осуществляющий логический доступ.

Примечание — В составе основных типов субъектов доступа в настоящем стандарте как минимум рассматриваются следующие:

- пользователи — субъекты доступа, в том числе клиенты финансовой организации, осуществляющие доступ к объектам и (или) ресурсам доступа с целью использования финансовых услуг, предоставляемых информационной инфраструктурой финансовой организации;
- эксплуатационный персонал — субъекты доступа, в том числе представители подрядных организаций, которые решают задачи обеспечения эксплуатации и (или) администрирования объектов и (или) ресурсов доступа, для которых необходимо осуществление логического доступа, включая задачи, связанные с эксплуатацией и администрированием технических мер защиты информации;
- технический (вспомогательный) персонал — субъекты доступа, в том числе представители подрядных организаций, решающие задачи, связанные с обеспечением эксплуатации объектов доступа, для выполнения которых

не требуется осуществление логического доступа, или выполняющие хозяйственную деятельность и осуществляющие физический доступ к объектам доступа без цели их непосредственного использования;

- программные сервисы — процессы выполнения программ в информационной инфраструктуре, осуществляющие логический доступ к ресурсам доступа.

3.15 **авторизация:** Проверка, подтверждение и предоставление прав логического доступа при осуществлении субъектами доступа логического доступа.

3.16 **идентификация:** Присвоение для осуществления логического доступа субъекту (объекту) доступа уникального признака (идентификатора); сравнение при осуществлении логического доступа предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов.

3.17 **аутентификация:** Проверка при осуществлении логического доступа принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

3.18 **регистрация событий защиты информации (регистрация):** Фиксация данных о совершенных субъектами доступа действиях или данных о событиях защиты информации.

3.19 **учетная запись:** Логический объект (информация), существующий в пределах одного или нескольких ресурсов доступа и представляющий субъекта доступа в его (их) пределах.

3.20 **техническая учетная запись:** Учетная запись, используемая для осуществления логического доступа программными сервисами.

3.21 **права логического доступа:** Набор действий, разрешенных для выполнения субъектом доступа над ресурсом доступа с использованием соответствующей учетной записи.

3.22 **роль логического доступа (роль):** Заранее определенная совокупность функций и задач субъекта доступа, для выполнения которых необходим определенный набор прав логического доступа.

3.23 **роль защиты информации:** Заранее определенная совокупность функций и задач субъекта доступа, в том числе работника финансовой организации, связанных с применением организационных и (или) технических мер защиты информации.

3.24 **легальный субъект доступа:** Субъект доступа, наделенный финансовой организацией полномочиями на осуществление физического и (или) логического доступа.

3.25 **аутентификационные данные:** Данные в любой форме и на любом носителе, известные или принадлежащие легальному субъекту доступа — легальному владельцу аутентификационных данных, или данные, которыми обладает легальный субъект доступа, используемые для выполнения процедуры аутентификации при осуществлении логического доступа.

3.26 **компрометация аутентификационных данных:** Событие, связанное с возникновением возможности использования аутентификационных данных субъектом, не являющимся легальным владельцем указанных аутентификационных данных.

3.27 **фактор аутентификации:** Блок данных, используемых при аутентификации субъекта или объекта доступа.

Примечания

1 Факторы аутентификации подразделяются на следующие три категории:

- что-то, что субъект или объект доступа знает, например пароли легальных субъектов доступа, ПИН-коды;
- что-то, чем субъект или объект доступа обладает, например данные, хранимые на персональных технических устройствах аутентификации: токенах, смарт-картах и иных носителях;
- что-то, что свойственно субъекту или объекту доступа, например биометрические данные физического лица — легального субъекта доступа.

2 Адаптировано из [4].

3.28 **однофакторная аутентификация:** Аутентификация, для осуществления которой используется один фактор аутентификации.

3.29 **многофакторная аутентификация:** Аутентификация, для осуществления которой используются два и более различных факторов аутентификации.

3.30 **двухсторонняя аутентификация:** Метод аутентификации объектов и ресурсов доступа, обеспечивающий взаимную проверку принадлежности предъявленных объектом (ресурсом) доступа идентификаторов при их взаимодействии.

Примечание — Адаптировано из [4].

3.31 **событие защиты информации:** Идентифицированное возникновение и (или) изменение состояния объектов информатизации финансовой организации, действия работников финансовой

организации и (или) иных лиц, указывающие на возможный (потенциальный) инцидент защиты информации.

Примечание — Адаптировано из ГОСТ Р ИСО/МЭК 27001.

3.32 **инцидент защиты информации:** Одно или серия связанных нежелательных или неожиданных событий защиты информации, которые могут привести к риску нарушения выполнения бизнес-процессов, технологических процессов финансовой организации и (или) нарушить безопасность информации.

Примечания

1 В составе типов инцидентов защиты информации рекомендуется как минимум рассматривать:

- несанкционированный доступ к информации;
- нарушение в обеспечении защиты информации, включая нарушение работы технических мер защиты информации, появление уязвимостей защиты информации;
- нарушение требований законодательства Российской Федерации, в том числе нормативных актов Банка России, внутренних документов финансовой организации в области обеспечения защиты информации;
- нарушение регламентированных сроков выполнения процедур и операций в рамках предоставления финансовых услуг;
- нарушение установленных показателей предоставления финансовых услуг;
- нанесение финансового ущерба финансовой организации, ее клиентам и контрагентам;
- выполнение операций (транзакций), приводящих к финансовым последствиям финансовой организации, ее клиентов и контрагентов, осуществление переводов денежных средств по распоряжению лиц, не обладающих соответствующими полномочиями, или с использованием искаженной информации, содержащейся в соответствующих распоряжениях (электронных сообщениях).

2 Адаптировано из ГОСТ Р ИСО/МЭК 27001.

3.33 **управление инцидентами защиты информации:** Деятельность по своевременному обнаружению инцидентов защиты информации, адекватному и оперативному реагированию на них, направленная на минимизацию и (или) ликвидацию негативных последствий от инцидентов защиты информации для финансовой организации и (или) ее клиентов, а также на снижение вероятности повторного возникновения инцидентов защиты информации.

3.34 **группа реагирования на инциденты защиты информации; ГРИЗИ**: Действующая на постоянной основе группа работников финансовой организации и (или) иных лиц, привлекаемых ею, которая выполняет регламентированные в финансовой организации процедуры реагирования на инциденты защиты информации.

3.35 **информация конфиденциального характера:** Информация, для которой в соответствии с законодательством Российской Федерации, в том числе нормативными актами Банка России, и (или) внутренними документами финансовой организации обеспечивается сохранение свойства конфиденциальности.

3.36 **утечка информации:** Неконтролируемое финансовой организацией распространение информации конфиденциального характера.

Примечание — Адаптировано из ГОСТ Р 53114.

3.37 **защита информации от утечки:** Защита информации, направленная на предотвращение неконтролируемого финансовой организацией распространения информации конфиденциального характера.

Примечание — Адаптировано из ГОСТ Р 50922.

3.38 **серверные компоненты виртуализации:** Совокупность гипервизора, технических средств, необходимых для функционирования гипервизора, технических средств, предназначенных для управления и администрирования гипервизора, ПО, предназначенного для предоставления доступа к виртуальным машинам с АРМ пользователей (например, брокер соединений).

3.39 **базовый образ виртуальной машины:** Образ виртуальной машины, используемый в качестве первоначального образа при запуске (загрузке) виртуальной машины.

3.40 **текущий образ виртуальной машины:** Образ виртуальной машины в определенный (текущий) момент времени ее функционирования.

3.41 **информационный обмен между виртуальными машинами:** Межпроцессорное взаимодействие, а также сетевые информационные потоки между виртуальными машинами, в том числе реализуемые средствами гипервизора и виртуальными вычислительными сетями.

3.42 **система хранения данных виртуализации (система хранения данных):** Совокупность технических средств, предназначенных для хранения данных, используемых при реализации виртуализации, в том числе образов виртуальных машин и данных, обрабатываемых виртуальными машинами.

3.43 **защита от вредоносного кода на уровне гипервизора:** Способ реализации защиты от вредоносного кода виртуальных машин с использованием программных средств защиты от вредоносного кода, функционирующих как отдельные виртуальные машины на уровне гипервизора, без непосредственной установки агентов на защищаемые виртуальные машины.

3.44 **централизованное управление техническими мерами защиты информации:** Управление средствами и системами, реализующими технические меры защиты информации, множественно размещаемыми на АРМ пользователей и эксплуатационного персонала.

Примечание — В составе функций централизованного управления рассматриваются:

- автоматизированные установка и обновление ПО технических мер защиты информации, получаемых из единого (эталонного) источника;
- автоматизированное обновление сигнатурных баз в случае их использования, получаемых из единого (эталонного) источника, с установленной периодичностью;
- автоматизированное установление параметров настроек технических мер защиты информации, получаемых из единого (эталонного) источника;
- контроль целостности ПО технических мер защиты информации, параметров настроек технических мер защиты информации и сигнатурных баз при осуществлении их автоматизированной установки и (или) обновлении;
- контроль целостности единого (эталонного) источника ПО технических мер защиты информации, параметров настроек технических мер защиты информации и сигнатурных баз;
- централизованный сбор данных регистрации о событиях защиты информации, формируемых техническими мерами защиты информации.

3.45 **удаленный доступ работника финансовой организации (удаленный доступ):** Логический доступ работников финансовых организаций, реализуемый из-за пределов вычислительных сетей финансовых организаций.

3.46 **ресурс персональных данных:** База данных или иная совокупность персональных данных (ПДн) многих субъектов ПДн, объединенных общими целями обработки, обрабатываемых финансовой организацией с использованием или без использования объектов информатизации, в том числе АС.

4 Обозначения и сокращения

В настоящем стандарте применены следующие сокращения:

АРМ — автоматизированное рабочее место;
АС — автоматизированная система;
ПДн — персональные данные;
ИСПДн — информационные системы персональных данных;
МНИ — машинные носители информации;
НСД — несанкционированный доступ;
ПО — программное обеспечение;
СКЗИ — средства криптографической защиты информации;
СВТ — средство вычислительной техники;
СУБД — система управления базами данных.

5 Назначение и структура стандарта

Раздел 6 настоящего стандарта содержит:

- описание общей методологии применения финансовыми организациями требований к содержанию базового состава мер защиты информации, определенного в настоящем стандарте;
- определение уровней защиты информации, реализуемых финансовой организацией.

Раздел 7 настоящего стандарта содержит для каждого из уровней защиты информации требования к содержанию базового состава мер защиты информации, применение которых направлено на непосредственное обеспечение защиты информации (требования к системе защиты информации).

Разделы 8 и 9 настоящего стандарта содержат для каждого из уровней защиты информации требования к содержанию базового состава мер защиты информации, направленных на обеспечение должной полноты и качества реализации системы защиты информации (требования к системе организации

и управлению защитой информации), включая требования к содержанию базового состава мер по обеспечению защиты информации на этапах жизненного цикла АС и приложений.

В приложении А настоящего стандарта приведено описание основных положений базовой модели угроз и нарушителей финансовых организаций.

В приложении Б настоящего стандарта приведены состав и содержание рекомендуемых организационных мер, связанных с обработкой финансовой организацией персональных данных.

В приложении В настоящего стандарта приведен перечень событий защиты информации, потенциально связанных с НСД и инцидентами защиты информации, рекомендуемых для выявления, регистрации и анализа.

6 Общие положения

6.1 Деятельности финансовой организации свойственен операционный риск, связанный с нарушением безопасности информации, что является объективной реальностью, и понизить этот риск можно лишь до определенного остаточного уровня. Для управления операционным риском, связанным с безопасностью информации, финансовой организации необходимо обеспечить:

- идентификацию и учет объектов информатизации, в том числе АС, включаемых в область применения настоящего стандарта в соответствии с требованиями нормативных актов Банка России, устанавливающих обязательность применения его положений (далее — область применения);
- применение на различных уровнях информационной инфраструктуры выбранных финансовой организацией мер защиты информации, направленных на непосредственное обеспечение защиты информации и входящих в систему защиты информации, требования к содержанию базового состава которых установлены в разделе 7 настоящего стандарта;
- применение выбранных финансовой организацией мер защиты информации, обеспечивающих приемлемые для финансовой организации полноту и качество защиты информации, входящих в систему организации и управления защитой информации, требования к содержанию базового состава которых установлены в разделе 8 настоящего стандарта;
- применение выбранных финансовой организацией мер защиты информации, направленных на обеспечение защиты информации на всех стадиях жизненного цикла АС и приложений, требования к содержанию базового состава которых установлены в разделе 9 настоящего стандарта;
- оценку остаточного операционного риска (финансового эквивалента возможных потерь), вызванного неполным или некачественным выбором и применением мер защиты информации, требования к содержанию базового состава которых установлены в разделах 7, 8, 9 настоящего стандарта, и обработку указанного риска в соответствии с процедурой, определенной требованиями нормативных актов Банка России.

Примечание — Рекомендации по оценке рисков информационной безопасности приведены в [5] и [6]. Результаты оценки рисков информационной безопасности могут быть использованы при оценке остаточного операционного риска, вызванного неполным или некачественным выбором и применением организационных и технических мер защиты информации.

6.2 При идентификации и учете объектов информатизации финансовой организации должны рассматриваться как минимум следующие основные уровни информационной инфраструктуры:

а) системные уровни:

- уровень аппаратного обеспечения;
- уровень сетевого оборудования;
- уровень сетевых приложений и сервисов;
- уровень серверных компонентов виртуализации, программных инфраструктурных сервисов;
- уровень операционных систем, систем управления базами данных, серверов приложений;

б) уровень АС и приложений, эксплуатируемых для оказания финансовых услуг в рамках бизнес-процессов или технологических процессов финансовой организации.

6.3 Выбор и применение финансовой организацией мер защиты информации включает:

- выбор мер защиты информации, требования к содержанию базового состава которых установлены в разделе 7 настоящего стандарта;
- адаптацию (уточнение) при необходимости выбранного состава и содержания мер защиты информации с учетом модели угроз и нарушителей безопасности информации финансовой организации и структурно-функциональных характеристик объектов информатизации, в том числе АС, включаемых в область применения настоящего стандарта;

- исключение из базового состава мер, не связанных с используемыми информационными технологиями;

- дополнение при необходимости адаптированного (уточненного) состава и содержания мер защиты информации мерами, обеспечивающими выполнение требований к защите информации, установленных нормативными правовыми актами в области обеспечения безопасности и защиты информации;

- применение для конкретной области адаптированного (уточненного) и дополненного состава мер защиты информации в соответствии с положениями разделов 8 и 9 настоящего стандарта.

6.4 При невозможности технической реализации отдельных выбранных мер защиты информации, а также с учетом экономической целесообразности на этапах адаптации (уточнения) базового состава мер могут разрабатываться иные (компенсирующие) меры, направленные на нейтрализацию угроз безопасности информации, определенных в модели угроз, и нарушителей безопасности информации финансовой организации.

В этом случае финансовой организацией должно быть проведено обоснование применения компенсирующих мер защиты информации.

Применение компенсирующих мер защиты информации должно быть направлено на обработку операционного риска, связанного с реализацией тех же угроз безопасности информации, на нейтрализацию которых направлены меры из базового состава мер защиты информации настоящего стандарта, не применяемые финансовой организацией в связи с невозможностью технической реализации и (или) экономической целесообразностью.

6.5 Снижение операционного риска, связанного с нарушением безопасности информации, обеспечивается путем надлежащего выбора, повышения полноты и качества применения соответствующих мер защиты информации. Полнота и качество применения мер защиты информации достигается планированием, реализацией, проверкой и совершенствованием системы защиты информации, осуществляемыми в рамках системы организации и управления защитой информации, а также применением мер защиты информации на этапах жизненного цикла АС и приложений.

6.6 Оценка остаточного операционного риска, связанного с неполным или некачественным применением мер защиты информации, входящих в систему защиты информации, осуществляется в соответствии с процедурой, определенной требованиями нормативных актов Банка России, на основе оценки показателей соответствия реализации системы защиты информации финансовой организации требованиям разделов 7, 8 и 9 настоящего стандарта.

Оценку показателей соответствия реализации системы защиты информации финансовой организации требованиям, установленным в разделах 7, 8 и 9 настоящего стандарта, следует осуществлять в соответствии с методикой, приведенной в соответствующем национальном стандарте.

6.7 Настоящий стандарт определяет три уровня защиты информации:

- уровень 3 — минимальный;
- уровень 2 — стандартный;
- уровень 1 — усиленный.

В финансовой организации формируются один или несколько контуров безопасности, для которых может быть установлен разный уровень защиты информации.

Уровень защиты информации финансовой организации для конкретного контура безопасности устанавливается нормативными актами Банка России на основе:

- вида деятельности финансовой организации, состава предоставляемых финансовых услуг, реализуемых бизнес-процессов и (или) технологических процессов в рамках данного контура безопасности;
- объема финансовых операций;
- размера организации, отнесения финансовой организации к категории малых предприятий и микропредприятий;
- значимости финансовой организации для финансового рынка и национальной платежной системы.

6.8 Реализацию требований к содержанию базового состава мер защиты информации для следующих уровней защиты информации, установленных настоящим стандартом, рекомендуется использовать финансовыми организациями для обеспечения выполнения требований к защите персональных данных при их обработке в информационных системах персональных данных (ИСПДн):

- для обеспечения соответствия четвертому уровню защищенности персональных данных при их обработке в ИСПДн, установленных Правительством Российской Федерации [7], рекомендуется использовать требования, установленные настоящим стандартом для уровня 3 — минимальный;

- для обеспечения соответствия третьему и второму уровням защищенности персональных данных при их обработке в ИСПДн, установленных Правительством Российской Федерации [7], рекомендуется использовать требования, установленные настоящим стандартом для уровня 2 — стандартный;
- для обеспечения соответствия первому уровню защищенности персональных данных при их обработке в ИСПДн, установленных Правительством Российской Федерации [7], рекомендуется использовать требования, установленные настоящим стандартом для уровня 1 — усиленный.

Справочная информация по составу и содержанию рекомендуемых организационных мер, подлежащих реализации финансовой организацией в связи с обработкой ПДн в соответствии с требованиями [8], приведена в приложении Б к настоящему стандарту.

6.9 Основой для реализации правильного и эффективного способа минимизации возможных появлений в деятельности финансовой организации неприемлемых для нее операционных рисков, связанных с нарушением безопасности информации, являются принятые и контролируемые руководством финансовой организации документы, определяющие:

- политику обеспечения защиты информации финансовой организации;
- область применения системы защиты информации, описанной как перечень бизнес-процессов, технологических процессов и (или) АС финансовой организации;
- целевые показатели величины допустимого остаточного операционного риска, связанного с нарушением безопасности информации.

Содержание политики обеспечения защиты информации финансовой организации должно среди прочего определять:

- цели и задачи защиты информации;
- основные типы защищаемой информации;
- основные принципы и приоритеты выбора организационных и технических мер системы защиты информации и системы организации и управления защитой информации;
- положения о выделении необходимых и достаточных ресурсов, используемых при применении организационных и технических мер, входящих в систему защиты информации.

6.10 При проведении работ по предоставлению доступа к защищаемой информации финансовой организации следует руководствоваться следующими принципами, установленными для рынка финансовых услуг в ГОСТ Р ИСО/ТО 13569:

- «знать своего клиента»: принцип, реализация которого в основном направлена на обладание информацией в отношении благонадежности клиента, его основных потребностей, отсутствия его незаконной или нелегальной деятельности;
- «знать своего работника»: принцип, реализация которого в основном направлена на обладание информацией об отношении работников финансовой организации к своим служебным обязанностям, наличии у них возможных проблем, в том числе финансовых, имущественных или личных, которые могут потенциально привести к действиям, направленным на нарушение требований к защите информации;
- «необходимо знать»: принцип, реализация которого в основном направлена на ограничение прав логического и (или) физического доступа работников финансовой организации на уровне, минимально необходимом для выполнения служебных обязанностей;
- «двойное управление»: принцип, реализация которого в основном направлена на сохранение целостности и неизменности информации путем дублирования (алгоритмического, временного, ресурсного или иного) действий субъектов доступа в рамках реализации финансовых операций и транзакций, выполняемого до их окончательного завершения.

6.11 Финансовой организации рекомендуется обеспечивать автоматизацию предоставляемых финансовых услуг, бизнес-процессов, технологических процессов и (или) обработку защищаемой информации с использованием АС и приложений, создаваемых (модернизируемых) финансовой организацией самостоятельно и (или) с привлечением сторонних организаций.

Обязанность обеспечения финансовой организацией автоматизации бизнес-процессов, технологических процессов и (или) обработки защищаемой информации только с применением АС устанавливается требованиями нормативных актов Банка России.

6.12 Финансовая организация самостоятельно определяет необходимость использования средств криптографической защиты информации (СКЗИ), если иное не предусмотрено федеральными законами и иными нормативными правовыми актами Российской Федерации, в том числе нормативными актами Банка России, стандартами, правилами профессиональной деятельности, и (или) правилами платежной системы.

Работы финансовой организации по обеспечению защиты информации с помощью СКЗИ проводятся в соответствии с требованиями законодательства РФ [9], [10] и [11] и технической документацией на СКЗИ.

В случае если финансовая организация применяет СКЗИ российского производителя, указанные СКЗИ должны иметь сертификаты или разрешения федерального органа, уполномоченного в области обеспечения безопасности.

6.13 Юридические лица или индивидуальные предприниматели, привлекаемые финансовой организацией для проведения работ по обеспечению защиты информации, должны иметь лицензию на деятельность по технической защите конфиденциальной информации.

7 Требования к системе защиты информации

7.1 Общие положения

7.1.1 Настоящий раздел устанавливает требования к содержанию базового состава мер защиты информации для следующих процессов (направлений) защиты информации:

а) процесс 1 «Обеспечение защиты информации при управлении доступом»:

- управление учетными записями и правами субъектов логического доступа;
- идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа;
- защита информации при осуществлении физического доступа;
- идентификация, классификация и учет ресурсов и объектов доступа;

б) процесс 2 «Обеспечение защиты вычислительных сетей»:

- сегментация и межсетевое экранирование вычислительных сетей;
- выявление сетевых вторжений и атак;
- защита информации, передаваемой по вычислительным сетям;
- защита беспроводных сетей;

в) процесс 3 «Контроль целостности и защищенности информационной инфраструктуры»;

г) процесс 4 «Защита от вредоносного кода»;

д) процесс 5 «Предотвращение утечек информации»;

е) процесс 6 «Управление инцидентами защиты информации»:

- мониторинг и анализ событий защиты информации;
- обнаружение инцидентов защиты информации и реагирование на них;

ж) процесс 7 «Защита среды виртуализации»;

и) процесс 8 «Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств».

7.1.2 Меры защиты информации, входящие в систему защиты информации, реализуются:

- в соответствии с положениями разделов 6, 8, 9 настоящего стандарта;
- с ограничениями и условиями, определенными в разделе 6 настоящего стандарта, обусловленными технической возможностью и экономической целесообразностью (риск-аппетитом) финансовой организации.

7.1.3 В случае возникновения в информационной инфраструктуре финансовой организации зафиксированных нештатных ситуаций (аварий или существенного снижения функциональности компонентов информационной инфраструктуры), при которых временно отсутствует техническая возможность применения всех мер защиты информации, входящих в систему защиты информации, финансовая организация должна предусмотреть осуществление эксплуатационным персоналом действий, направленных на выполнение своих служебных обязанностей в условиях отсутствия применения отдельных мер защиты информации, а также должный контроль указанных действий.

7.1.4 Меры защиты информации, входящие в систему защиты информации, реализуются в том числе для обеспечения защиты:

- резервных копий ресурсов доступа, баз данных и архивных хранилищ информации;
- информации, обрабатываемой на виртуальных машинах, а также при реализации технологии виртуализации.

7.1.5 При формировании данных регистрации о событиях защиты информации, предусмотренных настоящим стандартом (рекомендуемый для выявления, регистрации и анализа перечень событий

защиты информации установлен в приложении В настоящего стандарта), для каждого фиксируемого действия и (или) операции определяется следующий набор параметров:

- данные, позволяющие идентифицировать выполненное действие или операцию;
- дата и время осуществления действия или операции;
- результат выполнения действия или операции (успешно или неуспешно);
- идентификационные данные субъекта доступа, выполнившего операцию;
- идентификационные данные ресурса доступа, в отношении которого выполнена операция;
- идентификационные данные, используемые для адресации объекта доступа, который использовался субъектами доступа для выполнения операции[1)].

7.1.6 Способы реализации мер защиты информации, установленные в таблицах раздела 7 настоящего стандарта, обозначены следующим образом:

- «О» — реализация путем применения организационной меры защиты информации[2)];
- «Т» — реализация путем применения технической меры защиты информации;
- «Н» — реализация является необязательной.

7.2 Процесс 1 «Обеспечение защиты информации при управлении доступом»

7.2.1 Подпроцесс «Управление учетными записями и правами субъектов логического доступа»

7.2.1.1 Применяемые финансовой организацией меры по управлению учетными записями и правами субъектов логического доступа должны обеспечивать:

- организацию и контроль использования учетных записей субъектов логического доступа;
- организацию и контроль предоставления (отзыва) и блокирования логического доступа;
- регистрацию событий защиты информации, связанных с операциями с учетными записями и правами логического доступа, и контроль использования предоставленных прав логического доступа.

При реализации подпроцесса «Управление учетными записями и правами субъектов логического доступа» рекомендуется использовать ГОСТ Р 50739.

7.2.1.2 Базовый состав мер по организации и контролю использования учетных записей субъектов логического доступа применительно к уровням защиты информации приведен в таблице 1.

Таблица 1 — Базовый состав мер по организации и контролю использования учетных записей субъектов логического доступа

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
УЗП.1	Осуществление логического доступа пользователями и эксплуатационным персоналом под уникальными и персонифицированными учетными записями	Т	Т	Т
УЗП.2	Контроль соответствия фактического состава разблокированных учетных записей фактическому составу легальных субъектов логического доступа	О	О	Т
УЗП.3	Контроль отсутствия незаблокированных учетных записей: - уволенных работников; - работников, отсутствующих на рабочем месте более 90 календарных дней; - работников внешних (подрядных) организаций, прекративших свою деятельность в организации	О	О	Т
УЗП.4	Контроль отсутствия незаблокированных учетных записей неопределенного целевого назначения	О	О	О

[1)] В зависимости от технической реализации идентификационной информацией является IP-адрес, MAC-адрес, номер SIM-карты и (или) иной идентификатор объекта доступа.

[2)] По решению финансовой организации способ «О» может быть реализован путем применения технической меры защиты информации.

7.2.1.3 Базовый состав мер по организации, контролю предоставления (отзыва) и блокированию логического доступа применительно к уровням защиты информации приведен в таблице 2.

Таблица 2 — Базовый состав мер по организации, контролю предоставления (отзыва) и блокированию логического доступа

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
УЗП.5	Документарное определение правил предоставления (отзыва) и блокирования логического доступа	Н	О	О
УЗП.6	Назначение для всех ресурсов доступа распорядителя логического доступа (владельца ресурса доступа)	О	О	О
УЗП.7	Предоставление прав логического доступа по решению распорядителя логического доступа (владельца ресурса доступа)	О	О	О
УЗП.8	Хранение эталонной информации о предоставленных правах логического доступа и обеспечение целостности указанной информации	О	Т	Т
УЗП.9	Контроль соответствия фактических прав логического доступа эталонной информации о предоставленных правах логического доступа	О	Т	Т
УЗП.10	Исключение возможного бесконтрольного самостоятельного расширения пользователями предоставленных им прав логического доступа	Т	Т	Т
УЗП.11	Исключение возможного бесконтрольного изменения пользователями параметров настроек средств и систем защиты информации, параметров настроек АС, связанных с защитой информации	Т	Т	Т
УЗП.12	Контроль необходимости отзыва прав субъектов логического доступа при изменении их должностных обязанностей	О	О	О
УЗП.13	Контроль прекращения предоставления логического доступа и блокирование учетных записей при истечении периода (срока) предоставления логического доступа	О	Т	Т
УЗП.14	Установление фактов неиспользования субъектами логического доступа предоставленных им прав на осуществление логического доступа на протяжении периода времени, превышающего 90 дней	О	Т	Н
УЗП.15	Установление фактов неиспользования субъектами логического доступа предоставленных им прав на осуществление логического доступа на протяжении периода времени, превышающего 45 дней	Н	Н	Т
УЗП.16	Реализация контроля со стороны распорядителя логического доступа целесообразности дальнейшего предоставления прав логического доступа, не использованных субъектами на протяжении периода времени, указанного в мерах УЗП.14, УЗП.15 настоящей таблицы	О	О	О
УЗП.17	Реализация возможности определения состава предоставленных прав логического доступа для конкретного ресурса доступа	О	Т	Т
УЗП.18	Реализация возможности определения состава предоставленных прав логического доступа для конкретного субъекта логического доступа	О	Т	Т
УЗП.19	Определение состава ролей, связанных с выполнением операции (транзакции) в АС, имеющих финансовые последствия для финансовой организации, клиентов и контрагентов, и ролей, связанных с контролем выполнения указанных операций (транзакций), запрет выполнения указанных ролей одним субъектом логического доступа	О	Т	Т
УЗП.20	Реализация правил управления правами логического доступа, обеспечивающих запрет совмещения одним субъектом логического доступа ролей, предусмотренных мерой УЗП.19 настоящей таблицы	О	Т	Т

Окончание таблицы 2

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
УЗП.21	Реализация правил управления правами логического доступа, обеспечивающих запрет совмещения одним субъектом логического доступа следующих функций: - эксплуатация и (или) контроль эксплуатации ресурса доступа, в том числе АС, одновременно с использованием по назначению ресурса доступа в рамках реализации бизнес-процесса финансовой организации; - создание и (или) модернизация ресурса доступа, в том числе АС, одновременно с использованием по назначению ресурса доступа в рамках реализации бизнес-процесса финансовой организации; - эксплуатация средств и систем защиты информации одновременно с контролем эксплуатации средств и систем защиты информации; - управление учетными записями субъектов логического доступа одновременно с управлением правами субъектов логического доступа	Н	О	Т

7.2.1.4 Базовый состав мер по регистрации событий защиты информации и контролю использования предоставленных прав логического доступа применительно к уровням защиты информации приведен в таблице 3.

Таблица 3 — Базовый состав мер по регистрации событий защиты информации и контролю использования предоставленных прав логического доступа

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
УЗП.22	Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего привилегированными правами логического доступа, позволяющими осуществить деструктивное воздействие, приводящие к нарушению выполнения бизнес-процессов или технологических процессов финансовой организации	Н	Т	Т
УЗП.23	Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала и пользователей, обладающих правами логического доступа, в том числе в АС, позволяющими осуществить операции (транзакции), приводящие к финансовым последствиям для финансовой организации, клиентов и контрагентов	Т	Т	Т
УЗП.24	Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего правами по управлению логическим доступом	Т	Т	Т
УЗП.25	Регистрация событий защиты информации, связанных с действиями по управлению учетными записями и правами субъектов логического доступа	Т	Т	Т
УЗП.26	Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего правами по управлению техническими мерами, реализующими многофакторную аутентификацию	Н	Т	Т
УЗП.27	Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего правами по изменению параметров настроек средств и систем защиты информации, параметров настроек АС, связанных с защитой информации	Н	Т	Т
УЗП.28	Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего правами по управлению криптографическими ключами	Т	Т	Т
УЗП.29	Закрепление АРМ пользователей и эксплуатационного персонала за конкретными субъектами логического доступа	Н	Н	О

7.2.2 Подпроцесс «Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа»

7.2.2.1 Применяемые финансовой организацией меры по идентификации, аутентификации, авторизации (разграничению доступа) при осуществлении логического доступа должны обеспечивать:

- идентификацию и аутентификацию субъектов логического доступа;
- организацию управления и организацию защиты идентификационных и аутентификационных данных;
- авторизацию (разграничение доступа) при осуществлении логического доступа;
- регистрацию событий защиты информации, связанных с идентификацией, аутентификацией и авторизацией при осуществлении логического доступа.

При реализации подпроцесса «Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа» рекомендуется использовать ГОСТ Р 50739.

7.2.2.2 Базовый состав мер по идентификации и аутентификации субъектов логического доступа применительно к уровням защиты информации приведен в таблице 4.

Таблица 4 — Базовый состав мер по идентификации и аутентификации субъектов логического доступа

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
РД.1	Идентификация и однофакторная аутентификация пользователей	Т	Т	Н
РД.2	Идентификация и многофакторная аутентификация пользователей	Н	Н	Т
РД.3	Идентификация и однофакторная аутентификация эксплуатационного персонала	Т	Н	Н
РД.4	Идентификация и многофакторная аутентификация эксплуатационного персонала	Н	Т	Т
РД.5	Аутентификация программных сервисов, осуществляющих логический доступ с использованием технических учетных записей	Т	Т	Т
РД.6	Аутентификация АРМ эксплуатационного персонала, используемых для осуществления логического доступа	Н	Т	Т
РД.7	Аутентификация АРМ пользователей, используемых для осуществления логического доступа	Н	Н	Т
РД.8	Сокрытие (неотображение) паролей при их вводе субъектами доступа	Т	Т	Т
РД.9	Запрет использования учетных записей субъектов логического доступа с незаданными аутентификационными данными или заданными по умолчанию разработчиком ресурса доступа, в том числе разработчиком АС	О	О	О
РД.10	Запрет на использование групповых, общих и стандартных учетных записей и паролей, а также прочих подобных методов идентификации и аутентификации, не позволяющих определить конкретного субъекта доступа	О	О	О
РД.11	Временная блокировка учетной записи пользователей после выполнения ряда неуспешных последовательных попыток аутентификации на период времени не менее 30 мин	Т	Т	Т
РД.12	Запрет множественной аутентификации субъектов логического доступа с использованием одной учетной записи путем открытия параллельных сессий логического доступа с использованием разных АРМ, в том числе виртуальных	Н	Т	Т
РД.13	Обеспечение возможности выполнения субъектом логического доступа — работниками финансовой организации процедуры принудительного прерывания сессии логического доступа и (или) приостановки осуществления логического доступа (с прекращением отображения на мониторе АРМ информации, доступ к которой получен в рамках сессии осуществления логического доступа)	Т	Т	Т

Окончание таблицы 4

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
РД.14	Автоматическое прерывание сессии логического доступа (приостановка осуществления логического доступа) по истечении установленного времени бездействия (неактивности) субъекта логического доступа, не превышающего 15 мин, с прекращением отображения на мониторе АРМ информации, доступ к которой получен в рамках сессии осуществления логического доступа	Т	Т	Т
РД.15	Выполнение процедуры повторной аутентификации для продолжения осуществления логического доступа после его принудительного или автоматического прерывания (приостановки осуществления логического доступа), предусмотренного мерами РД.13 и РД.14 настоящей таблицы	Т	Т	Т
РД.16	Использование на АРМ субъектов логического доступа встроенных механизмов контроля изменения базовой конфигурации оборудования (пароль на изменение параметров конфигурации системы, хранящихся в энергонезависимой памяти)	Т	Т	Т

7.2.2.3 Базовый состав мер по организации управления и организации защиты идентификационных и аутентификационных данных применительно к уровням защиты информации приведен в таблице 5.

Таблица 5 — Базовый состав мер по организации управления и организации защиты идентификационных и аутентификационных данных

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
РД.17	Запрет на использование технологии аутентификации с сохранением аутентификационных данных в открытом виде в СВТ	Т	Т	Т
РД.18	Запрет на передачу аутентификационных данных в открытом виде по каналам и линиям связи и их передачу куда-либо, кроме средств или систем аутентификации	Т	Т	Т
РД.19	Смена паролей пользователей не реже одного раза в год	Т	Т	Т
РД.20	Смена паролей эксплуатационного персонала не реже одного раза в квартал	Т	Т	Т
РД.21	Использование пользователями паролей длиной не менее восьми символов	Т	Т	Т
РД.22	Использование эксплуатационным персоналом паролей длиной не менее шестнадцати символов	Т	Т	Т
РД.23	Использование при формировании паролей субъектов логического доступа символов, включающих буквы (в верхнем и нижнем регистрах) и цифры	Т	Т	Т
РД.24	Запрет использования в качестве паролей субъектов логического доступа легко вычисляемых сочетаний букв и цифр (например, имена, фамилии, наименования, общепринятые сокращения)	Н	О	О
РД.25	Обеспечение возможности самостоятельной смены субъектами логического доступа своих паролей	Т	Т	Т
РД.26	Хранение копий аутентификационных данных эксплуатационного персонала на выделенных МНИ или на бумажных носителях	О	О	О
РД.27	Реализация защиты копий аутентификационных данных эксплуатационного персонала от НСД при их хранении на МНИ или бумажных носителях	О	О	О

Окончание таблицы 5

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
РД.28	Регистрация персонификации, выдачи (передачи) и уничтожения персональных технических устройств аутентификации, реализующих многофакторную аутентификацию	О	О	О
РД.29	Смена аутентификационных данных в случае их компрометации	О	О	О

7.2.2.4 Базовый состав мер по авторизации (разграничению доступа) при осуществлении логического доступа применительно к уровням защиты информации приведен в таблице 6.

Таблица 6 — Базовый состав мер по авторизации (разграничению доступа) при осуществлении логического доступа

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
РД.30	Авторизация логического доступа к ресурсам доступа, в том числе АС	Т	Т	Т
РД.31	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод) при разграничении логического доступа к ресурсам доступа	Т	Т	Т
РД.32	Реализация ролевого метода (с определением для каждой роли прав доступа) при разграничении логического доступа в АС	Н	Н	Т
РД.33	Реализация необходимых типов (чтение, запись, выполнение или иной тип) и правил разграничения логического доступа к ресурсам доступа, в том числе АС	Т	Т	Т
РД.34	Запрет реализации пользователями бизнес-процессов и технологических процессов финансовой организации с использования учетных записей эксплуатационного персонала, в том числе в АС	О	Т	Т
РД.35	Запрет выполнения пользователями бизнес-процессов с использованием привилегированных прав логического доступа, в том числе работы пользователей с правами локального администратора АРМ	Т	Т	Т
РД.36	Оповещение субъекта логического доступа после успешной авторизации о дате и времени его предыдущей авторизации в АС	Н	Н	Т
РД.37	Контроль состава разрешенных действий в АС до выполнения идентификации и аутентификации	Н	Т	Т
РД.38	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	О	О	О

7.2.2.5 Базовый состав мер по регистрации событий защиты информации, связанных с идентификацией, аутентификацией и авторизацией (разграничением доступа) при осуществлении логического доступа, применительно к уровням защиты информации приведен в таблице 7.

Таблица 7 — Базовый состав мер по регистрации событий защиты информации, связанных с идентификацией, аутентификацией и авторизацией (разграничением доступа) при осуществлении логического доступа

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
РД.39	Регистрация выполнения субъектами логического доступа ряда неуспешных последовательных попыток аутентификации	Н	Т	Т

Окончание таблицы 7

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
РД.40	Регистрация осуществления субъектами логического доступа идентификации и аутентификации	Т	Т	Т
РД.41	Регистрация авторизации, завершения и (или) прерывания (приостановки) осуществления эксплуатационным персоналом и пользователями логического доступа, в том числе в АС	Т	Т	Т
РД.42	Регистрация запуска программных сервисов, осуществляющих логический доступ	Н	Т	Т
РД.43	Регистрация изменений аутентификационных данных, используемых для осуществления логического доступа	Н	Т	Т
РД.44	Регистрация действий пользователей и эксплуатационного персонала, предусмотренных в случае компрометации их аутентификационных данных	Н	О	О

7.2.3 Подпроцесс «Защита информации при осуществлении физического доступа»

7.2.3.1 Применяемые финансовой организацией меры по защите информации при осуществлении физического доступа должны обеспечивать:

- организацию и контроль физического доступа в помещения, в которых расположены объекты доступа (далее — помещения);
- организацию и контроль физического доступа к объектам доступа, расположенным в публичных (общедоступных) местах (далее — общедоступные объекты доступа);
- регистрацию событий, связанных с физическим доступом.

7.2.3.2 Базовый состав мер по организации и контролю физического доступа в помещения применительно к уровням защиты информации приведен в таблице 8.

Таблица 8 — Базовый состав мер по организации и контролю физического доступа в помещения

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ФД.1	Документарное определение правил предоставления физического доступа	Н	О	О
ФД.2	Контроль перечня лиц, которым предоставлено право самостоятельного физического доступа в помещения	О	О	Т
ФД.3	Контроль самостоятельного физического доступа в помещения для лиц, не являющихся работниками финансовой организации	Н	О	Т
ФД.4	Контроль самостоятельного физического доступа в помещения для технического (вспомогательного) персонала	Н	О	Т
ФД.5	Осуществление физического доступа лицами, которым не предоставлено право самостоятельного доступа в помещения, только под контролем работников финансовой организации, которым предоставлено такое право	Н	О	О
ФД.6	Назначение для всех помещений распорядителя физического доступа	О	О	О
ФД.7	Предоставление права самостоятельного физического доступа в помещения по решению распорядителя физического доступа	О	О	О
ФД.8	Оборудование входных дверей помещения механическими замками, обеспечивающими надежное закрытие помещений в нерабочее время	О	О	О
ФД.9	Оборудование помещений средствами (системами) контроля и управления доступом	Н	Н	Т

Окончание таблицы 8

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ФД.10	Оборудование помещений средствами видеонаблюдения	Н	Н	Т
ФД.11	Оборудование помещений средствами охранной и пожарной сигнализации	Н	Н	Т
ФД.12	Расположение серверного и сетевого оборудования в запираемых серверных стоечных шкафах	Н	О	О
ФД.13	Контроль доступа к серверному и сетевому оборудованию, расположенному в запираемых серверных стоечных шкафах	Н	О	О
ФД.14	Хранение архивов информации средств (систем) контроля и управления доступом не менее трех лет	Н	Н	Т
ФД.15	Хранение архивов информации средств видеонаблюдения не менее 14 дней*	Н	Т	Н
ФД.16	Хранение архивов информации средств видеонаблюдения не менее 90 дней	Н	Н	Т
* В случае применения средств видеонаблюдения.				

7.2.3.3 Базовый состав мер по организации и контролю физического доступа к общедоступным объектам доступа применительно к уровням защиты информации приведен в таблице 9.

Таблица 9 — Базовый состав мер по организации и контролю физического доступа к общедоступным объектам доступа

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ФД.17	Регистрация доступа к общедоступным объектам доступа с использованием средств видеонаблюдения	Н	Т	Т
ФД.18	Хранение архивов информации средств видеонаблюдения, регистрирующих доступ к общедоступным объектам доступа, не менее 14 дней	Н	Т	Т
ФД.19	Контроль состояния общедоступных объектов доступа с целью выявлений несанкционированных изменений в их аппаратном обеспечении и (или) ПО	О	О	О
ФД.20	Приведение общедоступных объектов доступа, для которых были выявлены несанкционированные изменения в их аппаратном обеспечении и (или) ПО (до устранения указанных несанкционированных изменений), в состояние, при котором невозможно их использование для осуществления операции (транзакции), приводящей к финансовым последствиям для финансовой организации, клиентов и контрагентов	О	О	О

7.2.3.4 Базовый состав мер по регистрации событий, связанных с физическим доступом, применительно к уровням защиты информации приведен в таблице 10.

Таблица 10 — Базовый состав мер по регистрации событий, связанных с физическим доступом

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ФД.21	Регистрация событий защиты информации, связанных с входом (выходом) в помещения (из помещений), в которых расположены объекты доступа	Н	Н	Т

7.2.4 Подпроцесс «Идентификация и учет ресурсов и объектов доступа»

7.2.4.1 Применяемые финансовой организацией меры по идентификации и учету ресурсов и объектов доступа должны обеспечивать:

- организацию учета и контроль состава ресурсов и объектов доступа;
- регистрацию событий защиты информации, связанных с операциями по изменению состава ресурсов и объектов доступа.

При реализации подпроцесса «Идентификация и учет ресурсов и объектов доступа» рекомендуется использовать ГОСТ Р 50739.

7.2.4.2 Базовый состав мер по организации учета и контроля состава ресурсов и объектов доступа применительно к уровням защиты информации приведен в таблице 11.

Таблица 11 — Базовый состав мер по организации учета и контроля состава ресурсов и объектов доступа

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ИУ.1	Учет созданных, используемых и (или) эксплуатируемых ресурсов доступа	О	Т	Т
ИУ.2	Учет используемых и (или) эксплуатируемых объектов доступа	О	О	Т
ИУ.3	Учет эксплуатируемых общедоступных объектов доступа (в том числе банкоматов, платежных терминалов)	О	О	Т
ИУ.4	Контроль фактического состава созданных, используемых и (или) эксплуатируемых ресурсов доступа (баз данных, сетевых файловых ресурсов, виртуальных машин) и их корректного размещения в сегментах вычислительных сетей финансовой организации	О	Т	Т
ИУ.5	Контроль выполнения операций по созданию, удалению и резервному копированию ресурсов доступа (баз данных, сетевых файловых ресурсов, виртуальных машин)	Н	Т	Т
ИУ.6	Контроль фактического состава эксплуатируемых объектов доступа и их корректного размещения в сегментах вычислительных сетей финансовой организации	Н	О	Т

7.2.4.3 Базовый состав мер по регистрации событий защиты информации, связанных с операциями по изменению состава ресурсов и объектов доступа, применительно к уровням защиты информации приведен в таблице 12.

Таблица 12 — Базовый состав мер по регистрации событий защиты информации, связанных с операциями по изменению состава ресурсов и объектов доступа

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ИУ.7	Регистрация событий защиты информации, связанных с созданием, копированием, в том числе резервным, и (или) удалением ресурсов доступа (баз данных, сетевых файловых ресурсов, виртуальных машин)	Н	Т	Т
ИУ.8	Регистрация событий защиты информации, связанных с подключением (регистрацией) объектов доступа в вычислительных сетях финансовой организации	Н	Н	Т

7.3 Процесс 2 «Обеспечение защиты вычислительных сетей»

7.3.1 Подпроцесс «Сегментация и межсетевое экранирование вычислительных сетей»

7.3.1.1 Применяемые финансовой организацией меры по сегментации и межсетевому экранированию вычислительных сетей должны обеспечивать:

- сегментацию и межсетевое экранирование внутренних вычислительных сетей;

- защиту внутренних вычислительных сетей при взаимодействии с сетью Интернет;
- регистрацию событий защиты информации, связанных с операциями по изменению параметров защиты вычислительных сетей.

При реализации подпроцесса «Сегментация и межсетевое экранирование вычислительных сетей» рекомендуется использовать ГОСТ Р ИСО/МЭК 27033-1.

7.3.1.2 Базовый состав мер по сегментации и межсетевому экранированию внутренних вычислительных сетей применительно к уровням защиты информации приведен в таблице 13.

Таблица 13 — Базовый состав мер по сегментации и межсетевому экранированию внутренних вычислительных сетей

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
СМЭ.1	Выделение в вычислительных сетях финансовой организации отдельных сегментов (групп сегментов), предназначенных для размещения информационной инфраструктуры каждого из контуров безопасности (далее — сегменты контуров безопасности)	Н	Т	Т
СМЭ.2	Реализация сетевого взаимодействия и сетевой изоляции на уровне не выше третьего (сетевой) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1, сегментов контуров безопасности и внутренних вычислительных сетей финансовой организации, не предназначенных для размещения информационной инфраструктуры, входящей в контуры безопасности (далее — иные внутренние вычислительные сети финансовой организации)	Н	Т	Т
СМЭ.3	Межсетевое экранирование вычислительных сетей сегментов контуров безопасности, включая фильтрацию данных на сетевом и прикладном уровнях семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1	Н	Т	Т
СМЭ.4	Реализация и контроль информационного взаимодействия между сегментами контуров безопасности и иными внутренними вычислительными сетями финансовой организации в соответствии с установленными правилами и протоколами сетевого взаимодействия	Н	Т	Т
СМЭ.5	Реализация и контроль информационного взаимодействия с применением программных шлюзов между сегментами контуров безопасности и иными внутренними вычислительными сетями финансовой организации с целью обеспечения ограничения и контроля на передачу данных по инициативе субъектов логического доступа	Н	Н	Т
СМЭ.6	Выделение в вычислительных сетях финансовой организации отдельных сегментов (групп сегментов), предназначенных для размещения информационной инфраструктуры, используемой только на этапе создания и (или) модернизации АС, в том числе тестирования ПО и СВТ (далее — сегмент разработки и тестирования)	Н	Т	Т
СМЭ.7	Реализация запрета сетевого взаимодействия сегмента разработки и тестирования и иных внутренних вычислительных сетей финансовой организации по инициативе сегмента разработки и тестирования	Н	Т	Т
СМЭ.8	Выделение в составе сегментов контуров безопасности отдельных пользовательских сегментов, в которых располагаются только АРМ пользователей	Н	Н	Т
СМЭ.9	Выделение в составе сегментов контуров безопасности отдельных сегментов управления, в которых располагаются только АРМ эксплуатационного персонала, используемые для выполнения задач администрирования информационной инфраструктуры	Н	Н	Т
СМЭ.10	Выделение в составе сегментов контуров безопасности отдельных сегментов хранения и обработки данных, в которых располагаются ресурсы доступа, предназначенные для обработки и хранения данных, серверное оборудование и системы хранения данных	Н	Н	Т

Окончание таблицы 13

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
СМЭ.11	Выделение отдельных сегментов для размещения общедоступных объектов доступа (в том числе банкоматов, платежных терминалов)	Н	Т	Т
СМЭ.12	Реализация и контроль информационного взаимодействия между сегментами вычислительных сетей, определенных мерами СМЭ.8 — СМЭ.11 настоящей таблицы, и иными сегментами вычислительных сетей в соответствии с установленными правилами и протоколами сетевого взаимодействия	Н	Н	Т
СМЭ.13	Контроль содержимого информации при ее переносе из сегментов или в сегменты контуров безопасности с использованием переносных (отчуждаемых) носителей информации	Н	О	Т

7.3.1.3 Базовый состав мер по защите внутренних вычислительных сетей при взаимодействии с сетью Интернет применительно к уровням защиты информации приведен в таблице 14.

Таблица 14 — Базовый состав мер по защите внутренних вычислительных сетей при взаимодействии с сетью Интернет

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
СМЭ.14	Реализация сетевого взаимодействия и сетевой изоляции на уровне не выше второго (канальный) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1, внутренних вычислительных сетей финансовой организации и сети Интернет	Н	Т	Т
СМЭ.15	Реализация сетевого взаимодействия и сетевой изоляции на уровне не выше третьего (сетевой) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1, внутренних вычислительных сетей финансовой организации и сети Интернет	Т	Н	Н
СМЭ.16	Межсетевое экранирование внутренних вычислительных сетей финансовой организации, включая фильтрацию данных на сетевом и прикладном уровнях семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1	Т	Т	Т
СМЭ.17	Реализация и контроль информационного взаимодействия внутренних вычислительных сетей финансовой организации и сети Интернет в соответствии с установленными правилами и протоколами сетевого взаимодействия	Т	Т	Т
СМЭ.18	Сокрытие топологии внутренних вычислительных сетей финансовой организации	Т	Т	Т
СМЭ.19	Реализация сетевого взаимодействия внутренних вычислительных сетей финансовой организации и сети Интернет через ограниченное количество контролируемых точек доступа	Т	Т	Т
СМЭ.20	Реализация почтового обмена с сетью Интернет через ограниченное количество контролируемых точек информационного взаимодействия, состоящих из внешнего (подключенного к сети Интернет) и внутреннего (размещенного во внутренних сетях финансовой организации) почтовых серверов с безопасной репликацией почтовых сообщений между ними	Н	Т	Т

7.3.1.4 Базовый состав мер по регистрации событий защиты информации, связанных с операциями по изменению параметров защиты вычислительных сетей, применительно к уровням защиты информации приведен в таблице 15.

Таблица 15 — Базовый состав мер по регистрации событий защиты информации, связанных с операциями по изменению параметров защиты вычислительных сетей

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
СМЭ.21	Регистрация изменений параметров настроек средств и систем защиты информации, обеспечивающих реализацию сегментации, межсетевого экранирования и защиты вычислительных сетей финансовой организации	Т	Т	Т

7.3.2 Подпроцесс «Выявление вторжений и сетевых атак»

7.3.2.1 Применяемые финансовой организацией меры по выявлению вторжений и сетевых атак должны обеспечивать:

- мониторинг и контроль содержимого сетевого трафика;
- регистрацию событий защиты информации, связанных с результатами мониторинга и контроля содержимого сетевого трафика.

При реализации подпроцесса «Выявление вторжений и сетевых атак» рекомендуется использовать [12].

7.3.2.2 Базовый состав мер по мониторингу и контролю содержимого сетевого трафика применительно к уровням защиты информации приведен в таблице 16.

Таблица 16 — Базовый состав мер по мониторингу и контролю содержимого сетевого трафика

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ВСА.1	Контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным несанкционированным информационным взаимодействием между сегментами контуров безопасности и иными внутренними вычислительными сетями финансовой организации	Н	Н	Т
ВСА.2	Контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным несанкционированным информационным взаимодействием между вычислительными сетями финансовой организации и сетью Интернет	Н	Т	Т
ВСА.3	Контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным несанкционированным информационным взаимодействием между сегментами, предназначенными для размещения общедоступных объектов доступа (в том числе банкоматов, платежных терминалов), и сетью Интернет	Н	Н	Т
ВСА.4	Контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным несанкционированным логическим доступом к ресурсам доступа, размещенным в вычислительных сетях финансовой организации, подключенных к сети Интернет	Н	Т	Т
ВСА.5	Контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным несанкционированным удаленным доступом	Н	Т	Т
ВСА.6	Контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным несанкционированным логическим доступом к ресурсам доступа, размещенным во внутренних вычислительных сетях финансовой организации	Н	Н	Т
ВСА.7	Контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным несанкционированным доступом к аутентификационным данным легальных субъектов доступа	Н	Н	Т
ВСА.8	Контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным осуществлением атак типа «отказ в обслуживании», предпринимаемых в отношении ресурсов доступа, размещенных в вычислительных сетях финансовой организации, подключенных к сети Интернет	Н	Т	Т

Окончание таблицы 16

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ВСА.9	Блокирование атак типа «отказ в обслуживании» в масштабе времени, близком к реальному	Н	Т	Т
ВСА.10	Контроль и обеспечение возможности блокировки нежелательных сообщений электронной почты (SPAM)	Т	Т	Т
ВСА.11	Реализация контроля, предусмотренного мерами ВСА.1 — ВСА.9 настоящей таблицы, путем сканирования и анализа сетевого трафика между группами сегментов вычислительных сетей финансовой организации, входящих в разные контуры безопасности	Н	Т	Т
ВСА.12	Реализация контроля, предусмотренного мерами ВСА.1 — ВСА.9 настоящей таблицы, путем сканирования и анализа сетевого трафика в пределах сегмента контура безопасности	Н	Н	Т
ВСА.13	Реализация контроля, предусмотренного мерами ВСА.1 — ВСА.9 настоящей таблицы, путем сканирования и анализа сетевого трафика между вычислительными сетями финансовой организации и сетью Интернет	Н	Т	Т

7.3.2.3 Базовый состав мер по регистрации событий защиты информации, связанных с результатами мониторинга и контроля содержимого сетевого трафика, применительно к уровням защиты информации приведен в таблице 17.

Таблица 17 — Базовый состав мер по регистрации событий защиты информации, связанных с результатами мониторинга и контроля содержимого сетевого трафика

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ВСА.14	Регистрация фактов выявления аномальной сетевой активности в рамках контроля, предусмотренного мерами ВСА.1 — ВСА.8 таблицы 16	Н	Т	Т

7.3.3 Подпроцесс «Защита информации, передаваемой по вычислительным сетям»

7.3.3.1 Финансовая организация должна применять меры по защите информации, передаваемой по вычислительным сетям.

7.3.3.2 Базовый состав мер по защите информации, передаваемой по вычислительным сетям, применительно к уровням защиты информации приведен в таблице 18.

Таблица 18 — Базовый состав мер по защите информации, передаваемой по вычислительным сетям

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЗВС.1	Применение сетевых протоколов, обеспечивающих защиту подлинности сетевого соединения, контроль целостности сетевого взаимодействия и реализацию технологии двухсторонней аутентификации при осуществлении логического доступа с использованием телекоммуникационных каналов и (или) линий связи, не контролируемых финансовой организацией	Т	Т	Т
ЗВС.2	Реализация защиты информации от раскрытия и модификации, применение двухсторонней аутентификации при ее передаче с использованием сети Интернет, телекоммуникационных каналов и (или) линий связи, не контролируемых финансовой организацией	Т	Т	Т

7.3.4 Подпроцесс «Защита беспроводных сетей»

7.3.4.1 Применяемые финансовой организацией меры по защите беспроводных сетей должны обеспечивать:

- защиту информации от раскрытия и модификации при использовании беспроводных сетей;
- защиту внутренних вычислительных сетей при использовании беспроводных сетей;
- регистрацию событий защиты информации, связанных с использованием беспроводных сетей.

7.3.4.2 Базовый состав мер по защите информации от раскрытия и модификации при использовании беспроводных сетей применительно к уровням защиты информации приведен в таблице 19.

Таблица 19 — Базовый состав мер по защите информации от раскрытия и модификации при использовании беспроводных сетей

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЗБС.1	Аутентификация устройств доступа техническими средствами, реализующими функции беспроводного сетевого соединения (точками доступа по протоколу Wi-Fi)	Т	Т	Т
ЗБС.2	Защита информации от раскрытия и модификации при ее передаче с использованием протоколов беспроводного доступа	Т	Т	Т

7.3.4.3 Базовый состав мер по защите внутренних вычислительных сетей при использовании беспроводных сетей применительно к уровням защиты информации приведен в таблице 20.

Таблица 20 — Базовый состав мер по защите внутренних вычислительных сетей при использовании беспроводных сетей

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЗБС.3	Размещение технических средств, реализующих функции беспроводного соединения, в выделенных сегментах вычислительных сетей финансовой организации	Н	Т	Т
ЗБС.4	Реализация сетевого взаимодействия и сетевой изоляции на уровне не выше второго (канальный) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1, внутренних вычислительных сетей финансовой организации и сегментов вычисленных сетей, выделенных в соответствии с пунктом ЗБС.3 настоящей таблицы	Н	Н	Т
ЗБС.5	Реализация сетевого взаимодействия и сетевой изоляции на уровне не выше третьего (сетевой) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1, внутренних вычислительных сетей финансовой организации и сегментов вычисленных сетей, выделенных в соответствии с мерой ЗБС.3 настоящей таблицы	Н	Т	Н
ЗБС.6	Межсетевое экранирование внутренних вычислительных сетей финансовой организации и сегментов вычисленных сетей, выделенных в соответствии с мерой ЗБС.3 настоящей таблицы, включая фильтрацию данных на сетевом и прикладном уровнях семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1	Н	Т	Т
ЗБС.7	Реализация и контроль информационного взаимодействия внутренних вычислительных сетей финансовой организации и сегментов вычисленных сетей, выделенных в соответствии с мерой ЗБС.3 настоящей таблицы, в соответствии с установленными правилами и протоколами сетевого взаимодействия	Н	Т	Т
ЗБС.8	Блокирование попыток подключения к беспроводным точкам доступа с незарегистрированных устройств доступа, в том числе из-за пределов зданий и сооружений финансовой организации	Н	Н	Т

7.3.4.4 Базовый состав мер по регистрации событий защиты информации, связанных с использованием беспроводных сетей, применительно к уровням защиты информации приведен в таблице 21.

Таблица 21 — Базовый состав мер по регистрации событий защиты информации, связанных с использованием беспроводных сетей

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЗБС.9	Регистрация попыток подключения к беспроводным точкам доступа с незарегистрированных устройств доступа, в том числе из-за пределов финансовой организации	Н	Н	Т
ЗБС.10	Регистрация изменений параметров настроек средств и систем защиты информации, обеспечивающих реализацию сегментации, межсетевого экранирования и защиты внутренних вычислительных сетей финансовой организации и сегментов вычисленных сетей, выделенных в соответствии с мерой ЗБС.3 таблицы 20	Н	Т	Т

7.4 Процесс 3 «Контроль целостности и защищенности информационной инфраструктуры»

7.4.1 Применяемые финансовой организацией меры по контролю целостности и защищенности информационной инфраструктуры должны обеспечивать:

- контроль отсутствия известных (описанных) уязвимостей защиты информации объектов информатизации;
- организацию и контроль размещения, хранения и обновления ПО информационной инфраструктуры;
- контроль состава и целостности ПО информационной инфраструктуры;
- регистрацию событий защиты информации, связанных с результатами контроля целостности и защищенности информационной инфраструктуры.

7.4.2 Базовый состав мер по контролю отсутствия известных (описанных) уязвимостей защиты информации объектов информатизации применительно к уровням защиты информации приведен в таблице 22.

Таблица 22 — Базовый состав мер по контролю отсутствия известных (описанных) уязвимостей защиты информации объектов информатизации

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЦЗИ.1	Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированное (неконтролируемое) информационное взаимодействие между сегментами контуров безопасности и иными внутренними сетями финансовой организации	Н	Т	Т
ЦЗИ.2	Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированное (неконтролируемое) информационное взаимодействие между внутренними вычислительными сетями финансовой организации и сетью Интернет	О	Т	Т
ЦЗИ.3	Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированное (неконтролируемое) информационное взаимодействие между сегментами, предназначенными для размещения общедоступных объектов доступа (в том числе банкоматов, платежных терминалов), и сетью Интернет	О	Т	Т

Окончание таблицы 22

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЦЗИ.4	Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированный логический доступ к ресурсам доступа, размещенным в вычислительных сетях финансовой организации, подключенных к сети Интернет	О	Т	Т
ЦЗИ.5	Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированный удаленный доступ	О	Т	Т
ЦЗИ.6	Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированный логический доступ к ресурсам доступа, размещенным во внутренних вычислительных сетях финансовой организации	Н	Т	Т
ЦЗИ.7	Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей, предусмотренных мерами ЦЗИ.1 — ЦЗИ.6 настоящей таблицы, путем сканирования и анализа параметров настроек серверного и сетевого оборудования	Н	Т	Т
ЦЗИ.8	Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей, указанных в пунктах ЦЗИ.1 — ЦЗИ.6 настоящей таблицы, путем сканирования и анализа состава, версий и параметров настроек прикладного ПО, ПО АС и системного ПО, реализующего функции обеспечения защиты информации и (или) влияющего на обеспечение защиты информации (далее в настоящем разделе — системное ПО)*, установленного на серверном и сетевом оборудовании	Н	Т	Т
ЦЗИ.9	Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей, предусмотренных мерами ЦЗИ.1 — ЦЗИ.6 настоящей таблицы, путем сканирования и анализа состава, версий и параметров настроек прикладного ПО, ПО АС и (или) системного ПО, установленного на АРМ пользователей и эксплуатационного персонала	Н	Т	Т
ЦЗИ.10	Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей, предусмотренных мерами ЦЗИ.1 — ЦЗИ.6 настоящей таблицы, путем сканирования и анализа состава, версий и параметров настроек средств и систем защиты информации	Н	Т	Т
ЦЗИ.11	Ограничение (запрет) использования на АРМ пользователей и эксплуатационного персонала, задействованных в выполнении бизнес-процессов финансовой организации, ПО, реализующего функции по разработке, отладке и (или) тестированию ПО	Н	О	О
* В том числе ПО операционных систем, ПО СУБД, ПО серверов приложений, ПО систем виртуализации.				

7.4.3 Базовый состав мер по организации и контролю размещения, хранения и обновления ПО применительно к уровням защиты информации приведен в таблице 23.

Таблица 23 — Базовый состав мер по организации и контролю размещения, хранения и обновления ПО

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЦЗИ.12	Контроль размещения и своевременного обновления на серверном и сетевом оборудовании ПО средств и систем защиты информации, прикладного ПО, ПО АС, системного ПО и сигнатурных баз средств защиты информации, в том числе с целью устранения выявленных уязвимостей защиты информации	О	О	Т

Окончание таблицы 23

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЦЗИ.13	Контроль размещения и своевременного обновления на АРМ пользователей и эксплуатационного персонала ПО средств и систем защиты информации, прикладного ПО, ПО АС и системного ПО, в том числе с целью устранения выявленных уязвимостей защиты информации	О	О	Т
ЦЗИ.14	Контроль работоспособности (тестирование) и правильности функционирования АС после выполнения обновлений ПО, предусмотренного мерами ЦЗИ.12 и ЦЗИ.13 настоящей таблицы, выполняемого в сегментах разработки и тестирования	О	О	О
ЦЗИ.15	Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации после выполнения обновлений ПО, предусмотренного мерой ЦЗИ.12 настоящей таблицы	О	Т	Т
ЦЗИ.16	Обеспечение возможности восстановления эталонных копий ПО АС, ПО средств и систем защиты информации, системного ПО в случаях нештатных ситуаций	О	О	О
ЦЗИ.17	Наличие, учет и контроль целостности эталонных копий ПО АС, ПО средств и систем защиты информации, системного ПО	Н	Н	Т
ЦЗИ.18	Наличие, учет и контроль целостности эталонных значений параметров настроек ПО АС, системного ПО, ПО средств и систем защиты информации, возможность восстановления указанных настроек в случаях нештатных ситуаций	О	О	Т
ЦЗИ.19	Контроль целостности и достоверности источников получения при распространении и (или) обновлении ПО АС, ПО средств и систем защиты информации, системного ПО	О	О	Т

7.4.4 Базовый состав мер по контролю состава и целостности ПО информационной инфраструктуры применительно к уровням защиты информации приведен в таблице 24.

Таблица 24 — Базовый состав мер по контролю состава и целостности ПО информационной инфраструктуры

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЦЗИ.20	Контроль состава разрешенного для использования ПО АРМ пользователей и эксплуатационного персонала	О	Т	Т
ЦЗИ.21	Исключение возможности установки и (или) запуска неразрешенного для использования ПО АРМ пользователей и эксплуатационного персонала	О	Т	Т
ЦЗИ.22	Контроль состава ПО серверного оборудования	Н	О	Т
ЦЗИ.23	Контроль состава ПО АРМ пользователей и эксплуатационного персонала, запускаемого при загрузке операционной системы	Н	Т	Т
ЦЗИ.24	Контроль целостности запускаемых компонентов ПО АС на АРМ пользователей и эксплуатационного персонала	Н	Н	Т
ЦЗИ.25	Реализация доверенной загрузки операционных систем АРМ пользователей и эксплуатационного персонала	Н	Н	Т
ЦЗИ.26	Контроль (выявление) использования технологии мобильного кода*	Н	Т	Т
* В том числе Java, JavaScript, ActiveX, VBScript и иные аналогичные технологии.				

7.4.5 Базовый состав мер по регистрации событий защиты информации, связанных с результатами контроля целостности и защищенности информационной инфраструктуры, применительно к уровням защиты информации приведен в таблице 25.

Таблица 25 — Базовый состав мер по регистрации событий защиты информации, связанных с результатами контроля целостности и защищенности информационной инфраструктуры

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЦЗИ.27	Регистрация фактов выявления уязвимостей защиты информации	Н	Т	Т
ЦЗИ.28	Регистрация установки, обновления и (или) удаления ПО АС, ПО средств и систем защиты информации, системного ПО на серверном и сетевом оборудовании	Н	Т	Т
ЦЗИ.29	Регистрация установки, обновления и (или) удаления прикладного ПО, ПО АС, ПО средств и систем защиты информации, системного ПО на АРМ пользователей и эксплуатационного персонала	Н	Т	Т
ЦЗИ.30	Регистрация запуска программных сервисов	Н	Н	Т
ЦЗИ.31	Регистрация результатов выполнения операций по контролю состава ПО серверного оборудования, АРМ пользователей и эксплуатационного персонала	Н	Н	Т
ЦЗИ.32	Регистрация результатов выполнения операций по контролю состава ПО АРМ пользователей и эксплуатационного персонала	Н	Т	Т
ЦЗИ.33	Регистрация результатов выполнения операций по контролю состава ПО, запускаемого при загрузке операционной системы АРМ пользователей и эксплуатационного персонала	Н	Т	Т
ЦЗИ.34	Регистрация результатов выполнения операций контроля целостности запускаемых компонентов ПО АС	Н	Н	Т
ЦЗИ.35	Регистрация выявления использования технологии мобильного кода	Н	Т	Т
ЦЗИ.36	Регистрация результатов выполнения операций по контролю целостности и достоверности источников получения при распространении и (или) обновлении ПО АС, ПО средств и систем защиты информации, системного ПО	Н	Н	Т

7.5 Процесс 4 «Защита от вредоносного кода»

7.5.1 Применяемые финансовой организацией меры по защите от вредоносного кода должны обеспечивать:

- организацию эшелонированной защиты от вредоносного кода на разных уровнях информационной инфраструктуры;
- организацию и контроль применения средств защиты от вредоносного кода;
- регистрацию событий защиты информации, связанных с реализацией защиты от вредоносного кода.

При реализации процесса «Защита от вредоносного кода» рекомендуется использовать [13].

7.5.2 Базовый состав мер по организации эшелонированной защиты от вредоносного кода на разных уровнях информационной инфраструктуры применительно к уровням защиты информации приведен в таблице 26.

Таблица 26 — Базовый состав мер по организации эшелонированной защиты от вредоносного кода на разных уровнях информационной инфраструктуры

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЗВК.1	Реализация защиты от вредоносного кода на уровне физических АРМ пользователей и эксплуатационного персонала	Т	Т	Т

Окончание таблицы 26

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЗВК.2	Реализация защиты от вредоносного кода на уровне виртуальной информационной инфраструктуры	Т	Т	Т
ЗВК.3	Реализация защиты от вредоносного кода на уровне серверного оборудования	Т	Т	Т
ЗВК.4	Реализация защиты от вредоносного кода на уровне контроля межсетевого трафика	Н	Т	Т
ЗВК.5	Реализация защиты от вредоносного кода на уровне контроля почтового трафика	Т	Т	Т
ЗВК.6	Реализация защиты от вредоносного кода на уровне входного контроля устройств и переносных (отчуждаемых) носителей информации	Т	Т	Т
ЗВК.7	Реализация защиты от вредоносного кода на уровне контроля общедоступных объектов доступа (в том числе банкоматов, платежных терминалов)	Т	Т	Т

7.5.3 Базовый состав мер по организации и контролю применения средств защиты от вредоносного кода применительно к уровням защиты информации приведен в таблице 27.

Таблица 27 — Базовый состав мер по организации и контролю применения средств защиты от вредоносного кода

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЗВК.8	Функционирование средств защиты от вредоносного кода в постоянном, автоматическом режиме, в том числе в части установки их обновлений и сигнатурных баз данных	Т	Т	Т
ЗВК.9	Функционирование средств защиты от вредоносного кода на АРМ пользователей и эксплуатационного персонала в резидентном режиме (в режиме service — для операционной системы Windows, в режиме daemon — для операционной системы Unix), их автоматический запуск при загрузке операционной системы	Т	Т	Т
ЗВК.10	Применение средств защиты от вредоносного кода, реализующих функцию контроля целостности их программных компонентов	Т	Т	Т
ЗВК.11	Контроль отключения и своевременного обновления средств защиты от вредоносного кода	Т	Т	Т
ЗВК.12	Выполнение еженедельных операций по проведению проверок на отсутствие вредоносного кода	Т	Т	Т
ЗВК.13	Использование средств защиты от вредоносного кода различных производителей, как минимум для уровней: - физические АРМ пользователей и эксплуатационного персонала; - серверное оборудование	Т	Н	Н
ЗВК.14	Использование средств защиты от вредоносного кода различных производителей, как минимум для уровней: - физические АРМ пользователей и эксплуатационного персонала; - серверное оборудование; - контроль межсетевого трафика	Н	Т	Т
ЗВК.15	Выполнение проверок на отсутствие вредоносного кода путем анализа информационных потоков между сегментами контуров безопасности и иными внутренними вычислительными сетями финансовой организации	Н	Т	Т

Окончание таблицы 27

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЗВК.16	Выполнение проверок на отсутствие вредоносного кода путем анализа информационных потоков между внутренними вычислительными сетями финансовой организации и сетью Интернет	Н	Т	Т
ЗВК.17	Выполнение проверок на отсутствие вредоносного кода путем анализа информационных потоков между сегментами, предназначенными для размещения общедоступных объектов доступа (в том числе банкоматов, платежных терминалов), и сетью Интернет	Н	Т	Т
ЗВК.18	Входной контроль всех устройств и переносных (отчуждаемых) носителей информации (включая мобильные компьютеры и флеш-накопители) перед их использованием в вычислительных сетях финансовой организации	Т	Т	Т
ЗВК.19	Входной контроль устройств и переносных (отчуждаемых) носителей информации перед их использованием в вычислительных сетях финансовой организации, в выделенном сегменте вычислительной сети, с исключением возможности информационного взаимодействия указанного сегмента и иных сегментов вычислительных сетей финансовой организации (кроме управляющего информационного взаимодействия по установленным правилам и протоколам)	Н	Т	Т
ЗВК.20	Выполнение предварительных проверок на отсутствие вредоносного кода устанавливаемого или изменяемого ПО, а также выполнение проверки после установки и (или) изменения ПО	Н	О	О
ЗВК.21	Запрет неконтролируемого открытия самораспаковывающихся архивов и исполняемых файлов, полученных из сети Интернет	О	Т	Т

7.5.4 Базовый состав мер по регистрации событий защиты информации, связанных с реализацией защиты от вредоносного кода, применительно к уровням защиты информации приведен в таблице 28.

Таблица 28 — Базовый состав мер по регистрации событий защиты информации, связанных с реализацией защиты от вредоносного кода

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЗВК.22	Регистрация операций по проведению проверок на отсутствие вредоносного кода	Т	Т	Т
ЗВК.23	Регистрация фактов выявления вредоносного кода	Т	Т	Т
ЗВК.24	Регистрация неконтролируемого использования технологии мобильного кода*	Т	Т	Т
ЗВК.25	Регистрация сбоев в функционировании средств защиты от вредоносного кода	Т	Т	Т
ЗВК.26	Регистрация сбоев в выполнении контроля (проверок) на отсутствие вредоносного кода	Т	Т	Т
ЗВК.27	Регистрация отключения средств защиты от вредоносного кода	Т	Т	Т
ЗВК.28	Регистрация нарушений целостности программных компонентов средств защиты от вредоносного кода	Т	Т	Т
* В том числе Java, JavaScript, ActiveX, VBScript и иные аналогичные технологии.				

7.6 Процесс 5 «Предотвращение утечек информации»

7.6.1 Применяемые финансовой организацией меры по предотвращению утечек информации должны обеспечивать:

- блокирование неразрешенных к использованию и контроль разрешенных к использованию потенциальных каналов утечки информации;
- контроль (анализ) информации, передаваемой по разрешенным к использованию потенциальным каналам утечки информации;
- организацию защиты машинных носителей информации (МНИ);
- регистрацию событий защиты информации, связанных с реализацией защиты по предотвращению утечки информации.

Примечание — Рекомендации, обеспечивающие снижение рисков утечки информации путем мониторинга и контроля информационных потоков, приведены в [14].

7.6.2 Базовый состав мер по блокированию неразрешенных к использованию и контролю разрешенных к использованию потенциальных каналов утечки информации применительно к уровням защиты информации приведен в таблице 29.

Таблица 29 — Базовый состав мер по блокированию неразрешенных к использованию и контролю разрешенных к использованию потенциальных каналов утечки информации

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ПУИ.1	Блокирование неразрешенной и контроль (анализ) разрешенной передачи информации конфиденциального характера на внешние адреса электронной почты	Н	Т	Т
ПУИ.2	Блокирование неразрешенной и контроль (анализ) разрешенной передачи информации конфиденциального характера в сеть Интернет с использованием информационной инфраструктуры финансовой организации	Н	Т	Т
ПУИ.3	Блокирование неразрешенной и контроль (анализ) разрешенной печати информации конфиденциального характера	Н	Т	Т
ПУИ.4	Блокирование неразрешенного и контроль (анализ) разрешенного копирования информации конфиденциального характера на переносные (отчуждаемые) носители информации	Н	Т	Т

7.6.3 Базовый состав мер по контролю (анализу) информации, передаваемой по разрешенным к использованию потенциальным каналам утечки информации, применительно к уровням защиты информации приведен в таблице 30.

Таблица 30 — Базовый состав мер по контролю (анализу) информации, передаваемой по разрешенным к использованию потенциальным каналам утечки информации

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ПУИ.5	Контентный анализ передаваемой информации по протоколам исходящего почтового обмена	Н	Т	Т
ПУИ.6	Ведение единого архива электронных сообщений с архивным доступом на срок не менее 6 мес и оперативным доступом на срок не менее 1 мес	Н	Т	Н
ПУИ.7	Ведение единого архива электронных сообщений с архивным доступом на срок не менее одного года и оперативным доступом на срок не менее 3 мес	Н	Н	Т
ПУИ.8	Ограничение на перечень протоколов сетевого взаимодействия, используемых для осуществления передачи сообщений электронной почты	Н	Т	Т

Окончание таблицы 30

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ПУИ.9	Ограничение на перечень форматов файлов данных, разрешенных к передаче в качестве вложений в сообщения электронной почты	Н	Т	Т
ПУИ.10	Ограничение на размеры файлов данных, передаваемых в качестве вложений в сообщения электронной почты	Н	Т	Т
ПУИ.11	Контентный анализ информации, передаваемой в сеть Интернет с использованием информационной инфраструктуры финансовой организации	Н	Т	Т
ПУИ.12	Классификация ресурсов сети Интернет с целью блокировки доступа к сайтам или типам сайтов, запрещенных к использованию в соответствии с установленными правилами	Н	Т	Т
ПУИ.13	Ограничение на перечень протоколов сетевого взаимодействия и сетевых портов, используемых при осуществлении взаимодействия с сетью Интернет	Н	Т	Т
ПУИ.14	Запрет хранения и обработки информации конфиденциального характера на объектах доступа, размещенных в вычислительных сетях финансовой организации, подключенных к сети Интернет	Н	О	О
ПУИ.15	Контентный анализ информации, выводимой на печать	Н	Т	Т
ПУИ.16	Использование многофункциональных устройств печати с возможностью получения результатов выполнения задания на печать по паролю и (или) персональной карточке доступа	Н	Н	Т
ПУИ.17	Контентный анализ информации, копируемой на переносные (отчуждаемые) носители информации	Н	Т	Т
ПУИ.18	Блокирование неразрешенных к использованию портов ввода-вывода информации СВТ	Н	Т	Т
ПУИ.19	Блокирование возможности использования незарегистрированных (неразрешенных к использованию) переносных (отчуждаемых) носителей информации в информационной инфраструктуре финансовой организации	Н	Т	Т

7.6.4 Базовый состав мер по организации защиты машинных носителей информации применительно к уровням защиты информации приведен в таблице 31.

Таблица 31 — Базовый состав мер по организации защиты машинных носителей информации

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ПУИ.20	Учет и контроль использования МНИ, предназначенных для хранения информации конфиденциального характера	О	О	О
ПУИ.21	Документарное определение порядка использования и доступа к МНИ, предназначенным для хранения информации конфиденциального характера	О	О	О
ПУИ.22	Маркирование учтенных МНИ	О	О	О
ПУИ.23	Стирание информации конфиденциального характера с МНИ средствами, обеспечивающими полную перезапись данных, при осуществлении вывода МНИ из эксплуатации или вывода из эксплуатации СВТ, в состав которых входят указанные МНИ, а также при необходимости их передачи в сторонние организации	Т	Н	Н

Окончание таблицы 31

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ПУИ.24	Стирание информации конфиденциального характера с МНИ средствами гарантированного стирания или способом (средством), обеспечивающим невозможность их восстановления, при осуществлении вывода МНИ из эксплуатации или вывода из эксплуатации СВТ, в состав которых входят указанные МНИ, а также при необходимости их передачи в сторонние организации	Н	Т	Т
ПУИ.25	Стирание информации конфиденциального характера с МНИ средствами, обеспечивающими полную перезапись данных, при передаче (перезакреплении) МНИ между работниками и (или) структурными подразделениями финансовой организации	Т	Н	Н
ПУИ.26	Стирание информации конфиденциального характера с МНИ средствами гарантированного стирания или способом (средством), обеспечивающим невозможность их восстановления, при передаче (перезакреплении) МНИ между работниками и (или) структурными подразделениями финансовой организации	Н	Т	Т
ПУИ.27	Шифрование информации конфиденциального характера при ее хранении на МНИ, выносимых за пределы финансовой организации	Н	Н	Т

7.6.5 Базовый состав мер по регистрации событий защиты информации, связанных с реализацией защиты по предотвращению утечки информации, применительно к уровням защиты информации приведен в таблице 32.

Таблица 32 — Базовый состав мер по регистрации событий защиты информации, связанных с реализацией защиты по предотвращению утечки информации

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ПУИ.28	Регистрация использования разблокированных портов ввода-вывода информации СВТ	Н	Т	Т
ПУИ.29	Регистрация операций, связанных с осуществлением доступа работниками финансовой организации к ресурсам сети Интернет	Н	Т	Т
ПУИ.30	Регистрация фактов вывода информации на печать	Н	Т	Т
ПУИ.31	Регистрация результатов выполнения контентного анализа информации, предусмотренного мерами ПУИ.5, ПУИ.11, ПУИ.15, ПУИ.17 таблицы 30	Н	Т	Т
ПУИ.32	Регистрация действий по учету и снятию с учета МНИ, предназначенных для хранения информации конфиденциального характера	О	О	О
ПУИ.33	Регистрация фактов стирания информации с МНИ	О	О	О

7.7 Процесс 6 «Управление инцидентами защиты информации»

7.7.1 Подпроцесс «Мониторинг и анализ событий защиты информации»

7.7.1.1 Применяемые финансовой организацией меры по мониторингу и анализу событий защиты информации должны обеспечивать:

- организацию мониторинга данных регистрации о событиях защиты информации, формируемых средствами и системами защиты информации, объектами информатизации, в том числе в соответствии с требованиями к содержанию базового состава мер защиты информации настоящего стандарта;
- сбор, защиту и хранение данных регистрации о событиях защиты информации;

- анализ данных регистрации о событиях защиты информации;
- регистрацию событий защиты информации, связанных с операциями по обработке данных регистрации о событиях защиты информации.

При реализации подпроцесса «Мониторинг и анализ событий защиты информации» рекомендуется использовать ГОСТ Р ИСО/МЭК ТО 18044.

Примечание — Рекомендации по обнаружению инцидентов информационной безопасности и реагированию на инциденты информационной безопасности приведены в [15].

7.7.1.2 Базовый состав мер по организации мониторинга данных регистрации о событиях защиты информации, формируемых объектами информатизации, применительно к уровням защиты информации приведен в таблице 33.

Таблица 33 — Базовый состав мер по организации мониторинга данных регистрации о событиях защиты информации, формируемых объектами информатизации

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
МАС.1	Организация мониторинга данных регистрации о событиях защиты информации, формируемых техническими мерами, входящими в состав системы защиты информации	Т	Т	Т
МАС.2	Организация мониторинга данных регистрации о событиях защиты информации, формируемых сетевым оборудованием, в том числе активным сетевым оборудованием, маршрутизаторами, коммутаторами	Н	Т	Т
МАС.3	Организация мониторинга данных регистрации о событиях защиты информации, формируемых сетевыми приложениями и сервисами	Н	Т	Т
МАС.4	Организация мониторинга данных регистрации о событиях защиты информации, формируемых системным ПО, операционными системами, СУБД	Н	Т	Т
МАС.5	Организация мониторинга данных регистрации о событиях защиты информации, формируемых АС и приложениями	Т	Т	Т
МАС.6	Организация мониторинга данных регистрации о событиях защиты информации, формируемых контроллерами доменов	Т	Т	Т
МАС.7	Организация мониторинга данных регистрации о событиях защиты информации, формируемых средствами (системами) контроля и управления доступом	Н	Н	Т

7.7.1.3 Базовый состав мер по сбору, защите и хранению данных регистрации о событиях защиты информации применительно к уровням защиты информации приведен в таблице 34.

Таблица 34 — Базовый состав мер по сбору, защите и хранению данных регистрации о событиях защиты информации

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
МАС.8	Централизованный сбор данных регистрации о событиях защиты информации, формируемых объектами информатизации, определенных мерами МАС.1 — МАС.7 таблицы 33	Н	Т	Т
МАС.9	Генерация временных меток для данных регистрации о событиях защиты информации и синхронизации системного времени объектов информатизации, используемых для формирования, сбора и анализа данных регистрации	Т	Т	Т

Окончание таблицы 34

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
МАС.10	Контроль формирования данных регистрации о событиях защиты информации объектов информатизации, определенных мерами МАС.1 — МАС.7 таблицы 33	О	Т	Т
МАС.11	Реализация защиты данных регистрации о событиях защиты информации от раскрытия и модификации, двухсторонней аутентификации при передаче данных регистрации с использованием сети Интернет	Н	Т	Т
МАС.12	Обеспечение гарантированной доставки данных регистрации о событиях защиты информации при их централизованном сборе	Н	Т	Т
МАС.13	Резервирование необходимого объема памяти для хранения данных регистрации о событиях защиты информации	Т	Т	Т
МАС.14	Реализация защиты данных регистрации о событиях защиты информации от НСД при их хранении, обеспечение целостности и доступности хранимых данных регистрации	Т	Т	Т
МАС.15	Обеспечение возможности доступа к данным регистрации о событиях защиты информации в течение трех лет	Т	Т	Н
МАС.16	Обеспечение возможности доступа к данным регистрации о событиях защиты информации в течение пяти лет	Н	Н	Т

7.7.1.4 Базовый состав мер по анализу данных регистрации о событиях защиты информации применительно к уровням защиты информации приведен в таблице 35.

Таблица 35 — Базовый состав мер по анализу данных регистрации о событиях защиты информации

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
МАС.17	Обеспечение возможности выполнения операции нормализации (приведения к единому формату), фильтрации, агрегации и классификации данных регистрации о событиях защиты информации	Н	Т	Т
МАС.18	Обеспечение возможности выявления и анализа событий защиты информации, потенциально связанных с инцидентами защиты информации, в том числе НСД*	Т	Т	Т
МАС.19	Обеспечение возможности определения состава действий и (или) операций конкретного субъекта доступа	Т	Т	Т
МАС.20	Обеспечение возможности определения состава действий и (или) операций субъектов доступа при осуществлении логического доступа к конкретному ресурсу доступа	Т	Т	Т
* Перечень событий, потенциально связанных с НСД, рекомендуемых для выявления, регистрации и анализа, приведен в приложении В к настоящему стандарту.				

7.7.1.5 Базовый состав мер по регистрации событий защиты информации, связанных с операциями по обработке данных регистрации о событиях защиты информации, применительно к уровням защиты информации приведен в таблице 36.

Таблица 36 — Базовый состав мер по регистрации событий защиты информации, связанных с операциями по обработке данных регистрации о событиях защиты информации

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
МАС.21	Регистрация нарушений и сбоев в формировании и сборе данных о событиях защиты информации	Н	Т	Т
МАС.22	Регистрация доступа к хранимым данным о событиях защиты информации	Т	Т	Т
МАС.23	Регистрация операций, связанных с изменением правил нормализации (приведения к единому формату), фильтрации, агрегации и классификации данных регистрации о событиях защиты информации	Н	Т	Т

7.7.2 Подпроцесс «Обнаружение инцидентов защиты информации и реагирование на них»

7.7.2.1 Применяемые финансовой организацией меры по обнаружению инцидентов защиты информации и реагирование на них должны обеспечивать:

- обнаружение и регистрацию инцидентов защиты информации;
- организацию реагирования на инциденты защиты информации;
- организацию хранения и защиту информации об инцидентах защиты информации;
- регистрацию событий защиты информации, связанных с результатами обнаружения инцидентов защиты информации и реагирования на них.

При реализации подпроцесса «Обнаружение инцидентов защиты информации и реагирование на них» рекомендуется использовать ГОСТ Р ИСО/МЭК ТО 18044.

Примечание — Рекомендации по обнаружению инцидентов информационной безопасности и реагированию на инциденты информационной безопасности приведены в [15].

7.7.2.2 Базовый состав мер по обнаружению и регистрации инцидентов защиты информации применительно к уровням защиты информации приведен в таблице 37.

Таблица 37 — Базовый состав мер по обнаружению и регистрации инцидентов защиты информации

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
РИ.1	Регистрация информации о событиях защиты информации, потенциально связанных с инцидентами защиты информации, в том числе НСД, выявленными в рамках мониторинга и анализа событий защиты информации	О	Т	Т
РИ.2	Регистрация информации, потенциально связанной с инцидентами защиты информации, в том числе НСД, полученной от работников, клиентов и (или) контрагентов финансовой организации	О	Т	Т
РИ.3	Классификация инцидентов защиты информации с учетом степени их влияния (критичности) на предоставление финансовых услуг, реализацию бизнес-процессов и (или) технологических процессов финансовой организации	О	О	Т
РИ.4	Установление и применение единых правил получения от работников, клиентов и (или) контрагентов финансовой организации информации, потенциально связанной с инцидентами защиты информации	О	О	О
РИ.5	Установление и применение единых правил регистрации и классификации инцидентов защиты информации в части состава и содержания атрибутов, описывающих инцидент защиты информации, и их возможных значений	О	Т	Т

7.7.2.3 Базовый состав мер по организации реагирования на инциденты защиты информации применительно к уровням защиты информации приведен в таблице 38.

Таблица 38 — Базовый состав мер по организации реагирования на инциденты защиты информации

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
РИ.6	Установление и применение единых правил реагирования на инциденты защиты информации	О	О	О
РИ.7	Определение и назначение ролей, связанных с реагированием на инциденты защиты информации	О	Н	Н
РИ.8	Определение и назначение ролей, связанных с реагированием на инциденты защиты информации — ролей группы реагирования на инциденты защиты информации (ГРИЗИ)	Н	О	О
РИ.9	Выделение в составе ГРИЗИ следующих основных ролей: - руководитель ГРИЗИ, в основные функциональные обязанности которого входит обеспечение оперативного руководства реагированием на инциденты защиты информации; - оператор-диспетчер ГРИЗИ, в основные функциональные обязанности которого входит обеспечение сбора и регистрации информации об инцидентах защиты информации; - аналитик ГРИЗИ, в основные функциональные обязанности которого входит выполнение непосредственных действий по реагированию на инцидент защиты информации; - секретарь ГРИЗИ, в основные функциональные обязанности которого входит документирование результатов реагирования на инциденты защиты информации, формирование аналитических отчетов материалов	Н	О	О
РИ.10	Своевременное (оперативное) оповещение членов ГРИЗИ о выявленных инцидентах защиты информации	Н	Т	Т
РИ.11	Предоставление членам ГРИЗИ прав логического и физического доступа и административных полномочий, необходимых для проведения реагирования на инциденты защиты информации	Н	О	О
РИ.12	Проведение реагирования на каждый обнаруженный инцидент защиты информации, включающего: - анализ инцидента; - определение источников и причин возникновения инцидента; - оценку последствий инцидента на предоставление финансовых услуг, реализацию бизнес-процессов или технологических процессов финансовой организации; - принятие мер по устранению последствий инцидента; - планирование и принятие мер по предотвращению повторного возникновения инцидента	О	О	О
РИ.13	Установление и применение единых правил сбора, фиксации и распространения информации об инцидентах защиты информации	О	О	О
РИ.14	Установление и применение единых правил закрытия инцидентов защиты информации	О	О	О

7.7.2.4 Базовый состав мер по организации хранения и защите информации об инцидентах защиты информации применительно к уровням защиты информации приведен в таблице 39.

Таблица 39 — Базовый состав мер по организации хранения и защите информации об инцидентах защиты информации

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
РИ.15	Реализация защиты информации об инцидентах защиты информации от НСД, обеспечение целостности и доступности указанной информации	Т	Т	Т

Окончание таблицы 39

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
РИ.16	Разграничение доступа членов ГРИЗИ к информации об инцидентах защиты информации в соответствии с определенным распределением ролей, связанных с реагированием на инциденты защиты информации	Н	Т	Т
РИ.17	Обеспечение возможности доступа к информации об инцидентах защиты информации в течение трех лет	Т	Т	Н
РИ.18	Обеспечение возможности доступа к информации об инцидентах защиты информации в течение пяти лет	Н	Н	Т

7.7.2.5 Базовый состав мер по регистрации событий защиты информации, связанных с результатами обнаружения инцидентов защиты информации и реагирования на них, применительно к уровням защиты информации приведен в таблице 40.

Таблица 40 — Базовый состав мер по регистрации событий защиты информации, связанных с результатами обнаружения инцидентов защиты информации и реагирования на них

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
РИ.19	Регистрация доступа к информации об инцидентах защиты информации	Т	Т	Т

7.8 Процесс 7 «Защита среды виртуализации»

7.8.1 Для обеспечения должного уровня защиты информации при использовании технологии виртуализации, организационные и технические меры, применяемые для защиты среды виртуализации, являются дополнительными и применяются в совокупности с иными мерами защиты информации, установленными настоящим стандартом.

Дополнительные организационные и технические меры, применяемые для защиты среды виртуализации, определяются для следующих процессов (подпроцессов) защиты информации, перечисленных в 7.1.1 настоящего стандарта:

- идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа;
- сегментация и межсетевое экранирование вычислительных сетей.

7.8.2 Применяемые финансовой организацией меры по защите среды виртуализации должны обеспечивать:

- организацию идентификации, аутентификации, авторизации (разграничения доступа) при осуществлении логического доступа к виртуальным машинам и серверным компонентам виртуализации;
- организацию и контроль информационного взаимодействия и изоляции виртуальных машин;
- организацию защиты образов виртуальных машин;
- регистрацию событий защиты информации, связанных с доступом к виртуальным машинам и серверным компонентам виртуализации.

Примечание — Рекомендации по обеспечению информационной безопасности при использовании технологии виртуализации в рамках реализации банковских технологических процессов приведены в [16] и ГОСТ Р 56938.

7.8.3 Базовый состав мер по организации идентификации, аутентификации, авторизации (разграничения доступа) при осуществлении логического доступа к виртуальным машинам и серверным компонентам виртуализации применительно к уровням защиты информации приведен в таблице 41.

Таблица 41 — Базовый состав мер по организации идентификации, аутентификации, авторизации (разграничения доступа) при осуществлении логического доступа к виртуальным машинам и серверным компонентам виртуализации

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЗСВ.1	Разграничение и контроль осуществления одновременного доступа к виртуальным машинам с АРМ пользователей и эксплуатационного персонала только в пределах одного контура безопасности	Н	Т	Н
ЗСВ.2	Разграничение и контроль осуществления одновременного доступа к виртуальным машинам с АРМ пользователей и эксплуатационного персонала только в пределах одного контура безопасности на уровне не выше третьего (сетевой) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1	Н	Н	Т
ЗСВ.3	Разграничение и контроль осуществления одновременного доступа виртуальных машин к системе хранения данных в пределах контура безопасности	Н	Т	Н
ЗСВ.4	Разграничение и контроль осуществления одновременного доступа виртуальных машин к системе хранения данных в пределах контура безопасности на уровне не выше третьего (сетевой) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1	Н	Н	Т
ЗСВ.5	Идентификация и аутентификация пользователей серверными компонентами виртуализации и (или) средствами централизованных сервисов аутентификации при предоставлении доступа к виртуальным машинам	Т	Т	Т
ЗСВ.6	Реализация необходимых методов предоставления доступа к виртуальным машинам, обеспечивающих возможность доступа с использованием одних аутентификационных данных только к одной виртуальной машине	Н	Т	Н
ЗСВ.7	Реализация необходимых методов предоставления доступа к виртуальным машинам, обеспечивающих возможность доступа с использованием одних аутентификационных данных только к одной виртуальной машине с одного АРМ пользователя или эксплуатационного персонала	Н	Н	Т
ЗСВ.8	Обеспечение возможности принудительной блокировки (выключения) установленной сессии работы пользователя с виртуальной машиной	Т	Т	Т
ЗСВ.9	Контроль и протоколирование доступа эксплуатационного персонала к серверным компонентам виртуализации и системе хранения данных с реализацией двухфакторной аутентификации	Н	Т	Т
ЗСВ.10	Размещение средств защиты информации, используемых для организации контроля и протоколирования доступа эксплуатационного персонала к серверным компонентам виртуализации и системе хранения данных на физических СВТ	Н	Т	Т
ЗСВ.11	Реализация правил управления правами логического доступа, обеспечивающая запрет одновременного совмещения одним субъектом логического доступа следующих функций: - создание виртуальных машин, управление образами виртуальных машин на этапах их жизненного цикла; - предоставление доступа к виртуальным машинам, включая настройку виртуальных сегментов вычислительных сетей и применяемых средств защиты информации на уровне серверных компонентов виртуализации; - управление системы хранения данных; - управление настройками гипервизоров; - конфигурирование виртуальных сетей в рамках своего контура безопасности	Н	Н	Т
ЗСВ.12	Размещение серверных и пользовательских компонентов АС на разных виртуальных машинах	Н	О	О

7.8.4 Базовый состав мер по организации сегментации и межсетевого экранирования вычислительных сетей, предназначенных для размещения виртуальных машин и серверных компонент виртуализации, применительно к уровням защиты информации приведен в таблице 42.

Таблица 42 — Базовый состав мер по организации и контролю информационного взаимодействия и изоляции виртуальных машин[1)]

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЗСВ.13	Выделение в вычислительных сетях финансовой организации отдельных сегментов (групп сегментов), в том числе виртуальных, используемых для размещения совокупности виртуальных машин, предназначенных для размещения серверных компонент АС, включенных в разные контуры безопасности	Н	Т	Т
ЗСВ.14	Выделение в вычислительных сетях финансовой организации отдельных сегментов (групп сегментов), в том числе виртуальных, используемых для размещения совокупности виртуальных машин, предназначенных для размещения АРМ пользователей и эксплуатационного персонала, включенных в разные контуры безопасности	Н	Т	Т
ЗСВ.15	Организация информационного обмена между сегментами (группами сегментов) вычислительных сетей, определенных мерами ЗСВ.13 и ЗСВ.14 настоящей таблицы, физическим оборудованием (программно-аппаратным комплексом) и (или) программными средствами межсетевого экранирования, функционирующими на уровне гипервизора среды виртуализации	Н	Н	Т
ЗСВ.16	Межсетевое экранирование сегментов (групп сегментов) вычислительных сетей, определенных мерами ЗСВ.13 и ЗСВ.14 настоящей таблицы, включая фильтрацию данных на сетевом и прикладном уровнях семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1	Н	Т	Т
ЗСВ.17	Реализация и контроль информационного взаимодействия между сегментами (группами сегментов) вычислительных сетей мерами, указанными в пунктах ЗСВ.13 и ЗСВ.14 настоящей таблицы, в соответствии с установленными правилами и протоколами сетевого взаимодействия	Н	Т	Т
ЗСВ.18	Реализация мер защиты информации ЗСВ.15 — ЗСВ.17 настоящей таблицы физическим оборудованием (программно-аппаратным комплексом) и (или) программными средствами межсетевого экранирования, функционирующих на уровне гипервизора среды виртуализации	Н	Н	Т
ЗСВ.19	Организация и контроль информационного взаимодействия между виртуальными машинами разных АС в соответствии с установленными правилами и протоколами сетевого взаимодействия	Н	Н	Т
ЗСВ.20	Исключение возможности информационного взаимодействия и переноса информации между сегментами вычислительных сетей, входящими в разные контуры безопасности, с использованием АРМ пользователей и эксплуатационного персонала, эксплуатируемых для осуществления доступа к виртуальным машинам разных контуров безопасности	Н	Т	Т
ЗСВ.21	Выделение отдельных логических разделов системы хранения данных для каждого из контуров безопасности	Н	Т	Т
ЗСВ.22	Выделение отдельных сегментов управления, в которых располагаются АРМ эксплуатационного персонала, используемые для выполнения задач администрирования серверных компонент виртуализации и системы хранения данных*	Н	Н	Т
* Допускается использование единых сегментов управления, выделяемых в рамках выполнения меры ЗСВ.22 и меры СМЭ.9 таблицы 13.				

[1)] Меры по организации и контролю информационного взаимодействия и изоляции виртуальных машин применяются в совокупности с мерами по сегментации и межсетевому экранированию внутренних вычислительных сетей (см. меры СМЭ.1 — СМЭ.13 таблицы 13).

7.8.5 Базовый состав мер по организации защиты образов виртуальных машин применительно к уровням защиты информации приведен в таблице 43.

Таблица 43 — Базовый состав мер по организации защиты образов виртуальных машин

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЗСВ.23	Регламентация и контроль выполнения: - операций в рамках жизненного цикла базовых образов виртуальных машин; - операций по копированию образов виртуальных машин	Н	О	О
ЗСВ.24	Включение только в базовые образы виртуальных машин следующего ПО: - ПО технических мер защиты информации, применяемых в пределах виртуальных машин; - ПО АС	Н	О	О
ЗСВ.25	Отнесение каждой из виртуальных машин только к одному из контуров безопасности	Н	О	О
ЗСВ.26	Контроль целостности, выполняемый при запуске (загрузке) виртуальной машины: - базового образа виртуальной машины; - ПО, включенного в пользовательский профиль виртуальной машины; - параметров настроек ПО технических мер защиты информации, применяемых в пределах виртуальных машин	Н	Н	Т
ЗСВ.27	Запрет на копирование текущих образов виртуальных машин, использующих СКЗИ, с загруженными криптографическими ключами	О	О	О
ЗСВ.28	Запрет на копирование текущих образов виртуальных машин, используемых для реализации технологии виртуализации АРМ пользователей	О	О	О
ЗСВ.29	Запрет сохранения изменений, произведенных пользователями в процессе работы их виртуальных машин, в базовом образе виртуальных машин	Н	Н	Т
ЗСВ.30	Контроль завершения сеанса работы пользователей с виртуальными машинами	Н	Т	Н
ЗСВ.31	Контроль завершения сеанса работы пользователей с виртуальными машинами и обеспечение последующей работы виртуальной машины с использованием базового образа	Н	Н	Т

7.8.6 Базовый состав мер по регистрации событий защиты информации, связанных с доступом к виртуальным машинам и серверным компонентам виртуализации, применительно к уровням защиты информации приведен в таблице 44.

Таблица 44 — Базовый состав мер по регистрации событий защиты информации, связанных с доступом к виртуальным машинам и серверным компонентам виртуализации

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЗСВ.32	Регистрация операций, связанных с запуском (остановкой) виртуальных машин	Т	Т	Т
ЗСВ.33	Регистрация операций, связанных с изменением параметров настроек виртуальных сетевых сегментов, реализованных средствами гипервизора	Н	Т	Т
ЗСВ.34	Регистрация операций, связанных с созданием и удалением виртуальных машин	Т	Т	Т

Окончание таблицы 44

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЗСВ.35	Регистрация операций, связанных с созданием, изменением, копированием, удалением базовых образов виртуальных машин	Т	Т	Т
ЗСВ.36	Регистрация операций, связанных с копированием текущих образов виртуальных машин	Т	Т	Т
ЗСВ.37	Регистрация операций, связанных с изменением прав логического доступа к серверным компонентам виртуализации	Т	Т	Т
ЗСВ.38	Регистрация операций, связанных с изменением параметров настроек серверных компонентов виртуализации	Т	Т	Т
ЗСВ.39	Регистрация операций, связанных с аутентификацией и авторизацией эксплуатационного персонала при осуществлении доступа к серверным компонентам виртуализации	Т	Т	Т
ЗСВ.40	Регистрация операций, связанных с аутентификацией и авторизацией пользователей при осуществлении доступа к виртуальным машинам	Т	Т	Т
ЗСВ.41	Регистрация операций, связанных с запуском (остановкой) ПО серверных компонент виртуализации	Н	Н	Т
ЗСВ.42	Регистрация операций, связанных с изменением параметров настроек технических мер защиты информации, используемых для реализации контроля доступа к серверным компонентам виртуализации	Т	Т	Т
ЗСВ.43	Регистрация операций, связанных с изменением настроек технических мер защиты информации, используемых для обеспечения защиты виртуальных машин	Т	Т	Т

7.9 Процесс 8 «Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств»

7.9.1 Применяемые финансовой организацией меры по защите информации при осуществлении удаленного логического доступа работников финансовой организации с использованием мобильных (переносных) устройств должны обеспечивать:

- защиту информации от раскрытия и модификации при осуществлении удаленного доступа;
- защиту внутренних вычислительных сетей при осуществлении удаленного доступа;
- защиту информации от раскрытия и модификации при ее обработке и хранении на мобильных (переносных) устройствах.

7.9.2 Базовый состав мер по защите информации от раскрытия и модификации при осуществлении удаленного доступа применительно к уровням защиты информации приведен в таблице 45.

Таблица 45 — Базовый состав мер по защите информации от раскрытия и модификации при осуществлении удаленного доступа

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЗУД.1	Определение правил удаленного доступа и перечня ресурсов доступа, к которым предоставляется удаленный доступ	О	О	О
ЗУД.2	Аутентификация мобильных (переносных) устройств удаленного доступа	Т	Т	Т
ЗУД.3	Предоставление удаленного доступа только с использованием мобильных (переносных) устройств доступа, находящихся под контролем системы централизованного управления и мониторинга (системы Mobile Device Management, MDM)	Н	Т	Т

Окончание таблицы 45

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЗУД.4	Реализация защиты информации от раскрытия и модификации, применение двухсторонней взаимной аутентификации участников информационного обмена при ее передаче при осуществлении удаленного логического доступа	Т	Т	Т

7.9.3 Базовый состав мер по защите внутренних вычислительных сетей при осуществлении удаленного доступа применительно к уровням защиты информации приведен в таблице 46.

Таблица 46 — Базовый состав мер по защите внутренних вычислительных сетей при осуществлении удаленного доступа

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЗУД.5	Идентификация, двухфакторная аутентификация и авторизация субъектов доступа после установления защищенного сетевого взаимодействия, выполнения аутентификации, предусмотренной мерами ЗУД.2 и ЗУД.4 таблицы 45	Т	Т	Т
ЗУД.6	Запрет прямого сетевого взаимодействия мобильных (переносных) устройств доступа и внутренних сетей финансовой организации на уровне выше второго (канальный) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1	Н	Т	Т
ЗУД.7	Реализация доступа к ресурсам сети Интернет только через информационную инфраструктуру финансовой организации после установления защищенного сетевого взаимодействия, выполнения аутентификации, предусмотренной мерами ЗУД.2 и ЗУД.4 таблицы 45	Н	Т	Т
ЗУД.8	Контентный анализ информации, передаваемой мобильными (переносными) устройствами в сеть Интернет с использованием информационной инфраструктуры финансовой организации	Н	Т	Т
ЗУД.9	Реализация и контроль информационного взаимодействия внутренних вычислительных сетей финансовой организации и мобильных (переносных) устройств в соответствии с установленными правилами и протоколами сетевого взаимодействия	Т	Т	Т

7.9.4 Базовый состав мер по защите информации от раскрытия и модификации при ее обработке и хранении на мобильных (переносных) устройствах применительно к уровням защиты информации приведен в таблице 47.

Таблица 47 — Базовый состав мер по защите информации от раскрытия и модификации при ее обработке и хранении на мобильных (переносных) устройствах

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЗУД.10	Применение системы централизованного управления и мониторинга (MDM-системы), реализующей: - шифрование и возможность удаленного удаления информации, полученной в результате взаимодействия с информационными ресурсами финансовой организации; - аутентификацию пользователей на устройстве доступа;	Н	Т	Т

Окончание таблицы 47

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЗУД.10	- блокировку устройства по истечении определенного промежутка времени неактивности пользователя, требующую выполнения повторной аутентификации пользователя на устройстве доступа; - управление обновлениями системного ПО устройств доступа; - управление параметрами настроек безопасности системного ПО устройств доступа; - управление составом и обновлениями прикладного ПО; - невозможность использования мобильного (переносного) устройства в режиме USB-накопителя, а также в режиме отладки; - управление ключевой информацией, используемой для организации защищенного сетевого взаимодействия; - возможность определения местонахождения устройства доступа; - регистрацию смены SIM-карты; - запрет переноса информации в облачные хранилища данных, расположенные в общедоступных сетях (например, iCloud); - обеспечение возможности централизованного управления и мониторинга при смене SIM-карты	Н	Т	Т
ЗУД.11	Обеспечение защиты мобильных (переносных) устройств от воздействий вредоносного кода	Т	Т	Т
ЗУД.12	Стирание информации конфиденциального характера с мобильных (переносных) устройств средствами, обеспечивающими полную перезапись данных, при осуществлении вывода мобильных (переносных) устройств из эксплуатации, а также при необходимости их передачи в сторонние организации, между работниками и (или) структурными подразделениями финансовой организации	Т	Т	Т

8 Требования к организации и управлению защитой информации

8.1 Общие положения

8.1.1 Разделы 8 и 9 настоящего стандарта устанавливают требования к содержанию базового состава мер защиты информации, входящих в состав системы организации и управления защитой информации, направленных на обеспечение должной полноты и качества реализации системы защиты информации.

8.1.2 Меры системы организации и управления защитой информации применяются:

- на системных уровнях информационной инфраструктуры (определенных в 6.2 настоящего стандарта). Требования к содержанию базового состава мер системы организации и управления защитой информации, применяемых на системных уровнях, установлены в настоящем разделе;

- на этапах жизненного цикла АС и приложений, используемых для обработки, передачи и (или) хранения защищаемой информации в рамках выполнения и (или) обеспечения выполнения бизнес-процессов или технологических процессов финансовой организации. Требования к содержанию базового состава мер системы организации и управления защитой информации, применяемых на этапах жизненного цикла АС и приложений, установлены в разделе 9 настоящего стандарта.

8.1.3 Меры системы организации и управления защитой информации на системных уровнях применяются для каждого отдельного процесса (направления) защиты информации из числа мер, определенных в разделе 7 настоящего стандарта.

8.1.4 Меры системы организации и управления защитой информации на системных уровнях применяются в рамках следующих направлений защиты информации:

- направление 1 «Планирование процесса системы защиты информации» («Планирование»);
- направление 2 «Реализация процесса системы защиты информации» («Реализация»);
- направление 3 «Контроль процесса системы защиты информации» («Контроль»);
- направление 4 «Совершенствование процесса системы защиты информации» («Совершенствование»).

8.1.5 Способы реализации мер системы организации и управления защитой информации, установленные в таблицах раздела 8 настоящего стандарта, обозначены как в 7.1.6.

8.2 Направление 1 «Планирование процесса системы защиты информации»

8.2.1 В рамках направления «Планирование» финансовая организация обеспечивает определение (пересмотр):

- области применения процесса системы защиты информации;
- состава применяемых (а также не применяемых) мер защиты информации из числа мер, определенных в разделах 7, 8 и 9 настоящего стандарта;
- состава и содержания мер защиты информации, являющихся дополнительными к базовому составу мер, определенных в разделах 7, 8 и 9 настоящего стандарта, определяемых на основе актуальных угроз защиты информации, требований к защите информации, установленных нормативными правовыми актами в области обеспечения безопасности и защиты информации;
- порядка применения мер защиты информации в рамках процесса системы защиты информации.

Реализация деятельности в рамках направления «Планирование» осуществляется на основе политики финансовой организации в отношении целевых показателей величины допустимого остаточного операционного риска (риск-аппетита), связанного с обеспечением безопасности информации, а также при необходимости на основе результатов деятельности в рамках направления «Совершенствование».

Примечание — Рекомендации по документированию деятельности в области обеспечения информационной безопасности приведены в [17].

8.2.2 Базовый состав мер планирования процесса системы защиты информации приведен в таблице 48.

Таблица 48 — Базовый состав мер планирования процесса системы защиты информации

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ПЗИ.1	Документарное определение области применения процесса системы защиты информации* для уровней информационной инфраструктуры, определенных в 6.2 настоящего стандарта	О	О	О
ПЗИ.2	Документарное определение состава (с указанием соответствия настоящему стандарту) и содержания организационных мер защиты информации, выбранных финансовой организацией и реализуемых в рамках процесса системы защиты информации	О	О	О
ПЗИ.3	Документарное определение порядка применения организационных мер защиты информации, реализуемых в рамках процесса системы защиты информации	О	О	О
ПЗИ.4	Документарное определение состава (с указанием соответствия настоящему стандарту) и содержания технических мер защиты информации, выбранных финансовой организацией и реализуемых в рамках процесса системы защиты информации	О	О	О
ПЗИ.5	Документарное определение порядка применения технических мер защиты информации, реализуемых в рамках процесса системы защиты информации, включающего: - правила размещения технических мер защиты информации в информационной инфраструктуре; - параметры настроек технических мер защиты информации и информационной инфраструктуры, предназначенных для размещения технических мер защиты информации**; - руководства по применению технических мер защиты информации (включающие руководства по эксплуатации, контролю эксплуатации и использованию по назначению технических мер защиты информации); - состав ролей и права субъектов доступа, необходимых для обеспечения применения технических мер защиты информации (включающего эксплуатацию, контроль эксплуатации и использование по назначению мер защиты информации)	О	О	О

* Область применения процесса системы защиты информации определяется в соответствии с положениями нормативных актов Банка России.

** Параметры настроек компонентов информационной инфраструктуры, предназначенных для размещения технических мер защиты информации, определяются в случае необходимости.

8.3 Направление 2 «Реализация процесса системы защиты информации»

8.3.1 Деятельность в рамках направления «Реализация» выполняется по результатам выполнения направлений «Планирование» и (или) «Совершенствование» (см. 8.2 и 8.5 настоящего стандарта соответственно).

В рамках направления «Реализация» финансовая организация обеспечивает:

- должное применение мер защиты информации;
- определение ролей защиты информации, связанных с применением мер защиты информации;
- назначение ответственных лиц за выполнение ролей защиты информации;
- доступность реализации технических мер защиты информации;
- применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия [в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности], в случаях, когда применение таких средств необходимо для нейтрализации угроз безопасности, определенных в модели угроз и нарушителей безопасности информации финансовой организации;
- обучение, практическую подготовку (переподготовку) работников финансовой организации, ответственных за применение мер защиты информации;
- повышение осведомленности (инструктаж) работников финансовой организации в области защиты информации.

Примечание — Рекомендации по определению потребностей организации банковской системы Российской Федерации в ресурсах, необходимых для реализации процессов информационной безопасности, и по проведению контроля эффективности использования этих ресурсов приведены в [6].

8.3.2 Базовый состав мер по реализации процесса системы защиты информации приведен в таблице 49.

Таблица 49 — Базовый состав мер по реализации процесса системы защиты информации

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
РЗИ.1	Реализация учета объектов и ресурсов доступа, входящих в область применения процесса системы защиты информации, для уровней информационной инфраструктуры, определенных в 6.2 настоящего стандарта, в том числе объектов доступа, расположенных в публичных (общедоступных) местах (в том числе банкоматах, платежных терминалах)	О	О	Т
РЗИ.2	Размещение и настройка (конфигурирование) технических мер защиты информации в информационной инфраструктуре финансовой организации	О	О	Т
РЗИ.3	Контроль (тестирование) полноты реализации технических мер защиты информации	О	О	О
РЗИ.4	Назначение работникам финансовой организации ролей, связанных с применением мер защиты информации, и установление обязанности и ответственности за их выполнение	О	О	О
РЗИ.5	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной инфраструктуры	О	О	О
РЗИ.6	Реализация эксплуатации, использования по назначению технических мер защиты информации	О	О	О
РЗИ.7	Реализация применения организационных мер защиты информации	О	О	О
РЗИ.8	Реализация централизованного управления техническими мерами защиты информации*	Н	Н	Т
РЗИ.9	Обеспечение доступности технических мер защиты информации: - применение отказоустойчивых технических решений; - резервирование информационной инфраструктуры, необходимой для функционирования технических мер защиты информации; - осуществление контроля безотказного функционирования технических мер защиты информации;	Н	Н	Т

Окончание таблицы 49

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
РЗИ.9	- принятие регламентированных мер по восстановлению отказавших технических мер защиты информации информационной инфраструктуры, необходимых для их функционирования	Н	Н	Т
РЗИ.10	Обеспечение возможности сопровождения технических мер защиты информации в течение всего срока их использования	Н	О	О
РЗИ.11	Применение сертифицированных по требованиям безопасности информации средств защиты информации не ниже 4 класса**	Н	Н	Т
РЗИ.12	Применение сертифицированных по требованиям безопасности информации средств защиты информации не ниже 5 класса**	Н	Т	Н
РЗИ.13	Применение сертифицированных по требованиям безопасности информации средств защиты информации не ниже 6 класса**	Т	Н	Н
РЗИ.14	Применение СКЗИ, имеющих класс не ниже КС2**	Н	Н	Т
РЗИ.15	Обучение, практическая подготовка (переподготовка) работников финансовой организации, ответственных за применение мер защиты информации в рамках процесса защиты информации	О	О	О
РЗИ.16	Повышение осведомленности (инструктаж) работников финансовой организации в области реализации процесса защиты информации, применения организационных мер защиты информации, использования по назначению технических мер защиты информации	О	О	О
* Централизованное управление реализуется для технических мер защиты информации, множественно размещаемых на АРМ пользователей и эксплуатационного персонала. ** В случаях, когда применение таких средств необходимо для нейтрализации угроз безопасности, определенных в модели угроз и нарушителей безопасности информации финансовой организации.				

8.4 Направление 3 «Контроль процесса системы защиты информации»

8.4.1 Деятельность в рамках направления «Контроль» должна обеспечивать достаточную уверенность в том, что применение мер защиты информации осуществляется надлежащим образом и соответствует политике финансовой организации в отношении целевых показателей величины допустимого остаточного операционного риска (риск-аппетита), связанного с обеспечением безопасности информации.

Применяемые финансовой организацией меры защиты информации должны обеспечивать контроль:

- области применения процесса системы защиты информации;
- должного применения мер защиты информации в рамках процесса системы защиты информации;
- знаний работников финансовой организации в части применения мер защиты информации.

8.4.2 Базовый состав мер контроля процесса системы защиты информации приведен в таблице 50.

Таблица 50 — Базовый состав мер контроля процесса системы защиты информации

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
КЗИ.1	Контроль фактического состава объектов и ресурсов доступа, входящих в область применения процесса системы защиты информации, на соответствие учетным данным, формируемым в рамках выполнения меры РЗИ.1 таблицы 49	О	О	Т

Окончание таблицы 50

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
КЗИ.2	Контроль эксплуатации и использования по назначению технических мер защиты информации, включающий: - контроль фактического размещения технических мер защиты информации в информационной инфраструктуре финансовой организации; - контроль фактических параметров настроек технических мер защиты информации и компонентов информационной инфраструктуры, предназначенных для размещения технических мер защиты информации	О	О	Т
КЗИ.3	Контроль эксплуатации и использования по назначению технических мер защиты информации, включающий: - контроль назначения ролей, связанных с эксплуатацией и использованием по назначению технических мер защиты информации; - контроль выполнения руководств по эксплуатации и использованию по назначению технических мер защиты информации	О	О	О
КЗИ.4	Периодический контроль (тестирование) полноты реализации технических мер защиты информации	О	Т	Т
КЗИ.5	Контроль применения организационных мер защиты информации	О	О	О
КЗИ.6	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование	О	Т	Т
КЗИ.7	Проведение проверок знаний работников финансовой организации в части применения мер защиты информации в рамках процесса системы защиты информации	О	О	О
КЗИ.8	Фиксация результатов (свидетельств) проведения мероприятий по контролю реализации процесса системы защиты информации, проводимых в соответствии с мерами КЗИ.1 — КЗИ.7 настоящей таблицы	О	О	О

8.4.3 Базовый состав мер контроля процесса системы защиты информации в части регистрации событий защиты информации приведен в таблице 51.

Таблица 51 — Базовый состав мер контроля процесса системы защиты информации в части регистрации событий защиты информации

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
КЗИ.9	Регистрация операций по установке и (или) обновлению ПО технических средств защиты информации	Н	Т	Т
КЗИ.10	Регистрация операций по обновлению сигнатурных баз технических средств защиты информации (в случае их использования)	Н	Т	Т
КЗИ.11	Регистрация операций по изменению параметров настроек технических мер защиты информации и информационной инфраструктуры, предназначенных для размещения технических мер защиты информации	Н	Т	Т
КЗИ.12	Регистрация сбоев (отказов) технических мер защиты информации	Н	Т	Т

8.5 Направление 4 «Совершенствование процесса системы защиты информации»

8.5.1 Деятельность в рамках направления «Совершенствование» выполняется на основе результатов проведения мероприятий по обнаружению инцидентов защиты информации и реагированию на них, обнаружению недостатков в обеспечении защиты информации в рамках направления «Контроль», а также в случаях изменения политики финансовой организации в отношении принципов и приоритетов

в реализации системы защиты информации, целевых показателей величины допустимого остаточного операционного риска (риск-аппетита).

Применяемые финансовой организацией меры в рамках направления «Совершенствование» должны обеспечивать формирование и фиксацию решений о необходимости выполнения корректирующих или превентивных действий, в частности пересмотр применяемых мер защиты информации. При этом непосредственная деятельность по совершенствованию процесса защиты информации выполняется в рамках направления «Реализация» и при необходимости направления «Планирование».

8.5.2 Базовый состав мер по совершенствованию процесса системы защиты информации приведен в таблице 52.

Таблица 52 — Базовый состав мер по совершенствованию процесса системы защиты информации

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
СЗИ.1	Проведение и фиксация результатов (свидетельств) анализа необходимости совершенствования процесса системы защиты информации в случаях: - обнаружения инцидентов защиты информации; - обнаружения недостатков в рамках контроля системы защиты информации	О	О	О
СЗИ.2	Проведение и фиксация результатов (свидетельств) анализа необходимости совершенствования процесса системы защиты информации в случаях изменения политики финансовой организации в отношении: - области применения процесса системы защиты информации; - основных принципов и приоритетов в реализации процесса системы защиты информации; - целевых показателей величины допустимого остаточного операционного риска (риск-аппетита), связанного с обеспечением безопасности информации	О	О	О
СЗИ.3	Проведение и фиксация результатов (свидетельств) анализа необходимости совершенствования процесса системы защиты информации в случаях: - изменений требований к защите информации, определенных правилами платежной системы*; - изменений, внесенных в законодательство Российской Федерации, в том числе нормативные акты Банка России	О	О	О
СЗИ.4	Фиксация решений о проведении совершенствования процесса системы защиты информации в виде корректирующих или превентивных действий, например: - пересмотр области применения процесса системы защиты информации; - пересмотр состава и содержания организационных мер защиты информации, применяемых в рамках процесса системы защиты информации; - пересмотр состава технических мер защиты информации, применяемых в рамках процесса системы защиты информации	О	О	О
* Применяется только для участников платежных систем.				

9 Требования к защите информации на этапах жизненного цикла автоматизированных систем и приложений

9.1 Настоящий раздел устанавливает требования к содержанию базового состава мер защиты информации на этапах жизненного цикла АС и приложений, эксплуатируемых в рамках предоставления бизнес-процессов и (или) технологических процессов финансовой организации (далее при совместном упоминании — АС).

9.2 Деятельность по защите информации на стадиях жизненного цикла АС должна реализовываться путем:

- размещения компонентов АС в защищенной информационной инфраструктуре, для которой на системных уровнях реализованы процессы системы защиты информации, определенные в разделе 7 настоящего стандарта;

- создания и обеспечения применения системы защиты информации для конкретной АС, реализующей отдельные дополнительные (по отношению к требованиям раздела 8 настоящего стандарта) функции защиты информации для АС, не реализованные на системных уровнях.

9.3 Применяемые финансовой организацией меры на этапах жизненного цикла АС должны обеспечивать:

- определение состава мер защиты информации, реализуемых в АС (мер системы защиты информации АС);
- должное применение и контроль применения мер системы защиты информации АС;
- контроль отсутствия уязвимостей защиты информации в прикладном ПО АС и информационной инфраструктуре, предназначенной для размещения АС;
- конфиденциальность защищаемой информации.

Примечание — Рекомендации по обеспечению информационной безопасности на стадиях жизненного цикла АС приведены в [18].

9.4 Способы реализации мер защиты информации на этапах жизненного цикла АС в таблицах раздела 9 настоящего стандарта обозначены, как в 7.1.6.

9.5 Базовый состав мер защиты информации на этапе «Создание (модернизация) АС» приведен в таблице 53.

Таблица 53 — Базовый состав мер защиты информации на этапе «Создание (модернизация) АС»

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЖЦ.1	Документарное определение перечня защищаемой информации, планируемой к обработке в АС	О	О	О
ЖЦ.2	Документарное определение состава (с указанием соответствия настоящему стандарту) и содержания мер системы защиты информации АС (функционально-технических требований к системе защиты информации АС)	О	О	О
ЖЦ.3	Документарное определение в проектной и эксплуатационной документации на систему защиты информации АС: - состава и порядка применения технических и (или) организационных мер системы защиты информации АС; - параметров настроек технических мер системы защиты информации АС и компонентов информационной инфраструктуры, предназначенных для размещения указанных технических мер*	О	О	О
ЖЦ.4	Реализация управления версиями (сборками) и изменениями создаваемого (модернизируемого), в том числе тестируемого, прикладного ПО АС, осуществляемого для цели: - контроля реализации функций защиты информации в определенной версии (сборке) прикладного ПО; - принятия мер, препятствующих несанкционированному внесению изменений в версии (сборки) прикладного ПО	Н	О	О
ЖЦ.5	Использование (контроль использования) сегментов разработки и тестирования, выделенных в соответствии с мерой СМЭ.6 таблицы 13, при создании (модернизации), включая тестирование, АС	Н	О	О
ЖЦ.6	Контроль предоставления и обеспечение разграничения доступа в сегментах разработки и тестирования	О	О	О
ЖЦ.7	Реализация запрета использования защищаемой информации в сегментах разработки и тестирования**	О	О	О
ЖЦ.8	Применение прикладного ПО АС, сертифицированного на соответствие требованиям по безопасности информации, включая требования по анализу уязвимостей и контролю отсутствия недекларированных возможностей, в соответствии с законодательством Российской Федерации или в отноше-	Н	О	О

Окончание таблицы 53

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЖЦ.8	нии которых проведен анализ уязвимостей по требованиям к оценочному уровню доверия не ниже чем ОУД 4 в соответствии с требованиями ГОСТ Р ИСО/МЭК 15408-3***	Н	О	О
ЖЦ.9	Контроль (тестирование) полноты реализации мер системы защиты информации АС (функционально-технических требований к системе защиты информации АС)	О	О	О
ЖЦ.10	Проведение модернизации АС при изменении требований к составу и содержанию мер системы защиты информации АС (функционально-технические требований к системе защиты информации АС)	О	О	О
ЖЦ.11	Документарное определение в проектной и эксплуатационной документации на систему защиты информации АС*4 - состава и порядка применения клиентами финансовой организации прикладного ПО и (или) технических и (или) организационных мер защиты информации (далее при совместном упоминании — клиентские компоненты); - параметров настроек клиентских компонентов и информационной инфраструктуры клиентов финансовой организации, предназначенной для размещения клиентских компонентов; - описания мер по обеспечению использования клиентом определенных доверенных версий (сборок) прикладного ПО	О	О	О

* Параметры настроек компонентов информационной инфраструктуры, предназначенных для размещения технических мер защиты информации, определяются в случае необходимости.

** За исключением конфигурационной информации, определяющей параметры работы АС.

*** В случаях, предусмотренных нормативными актами Банка России, и (или) если в соответствии с моделью угроз и нарушителей безопасности информации финансовой организации, угрозы, связанные с наличием уязвимостей и недеклалированных возможностей в прикладном ПО АС, признаны актуальными.

*4 Документарное определение в соответствии с мерой ЖЦ.11 выполняется в случае необходимости.

9.6 Базовый состав мер защиты информации на этапе «Ввод в эксплуатацию АС» приведен в таблице 54.

Таблица 54 — Базовый состав мер защиты информации на этапе «Ввод в эксплуатацию АС»

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЖЦ.12	Размещение и настройка (конфигурирование) технических мер системы защиты информации АС в информационной инфраструктуре, используемой для непосредственной реализации бизнес-процессов или технологических процессов финансовой организации (далее — промышленная среда), в соответствии с положениями проектной и эксплуатационной документации	О	О	О
ЖЦ.13	Контроль (тестирование) полноты реализации мер системы защиты информации АС (функционально-технических требований к системе защиты информации АС) в промышленной среде	О	О	О
ЖЦ.14	Реализация контроля защищенности АС, включающего*: - тестирование на проникновение; - анализ уязвимостей системы защиты информации АС и информационной инфраструктуры промышленной среды	Н	О	О

* По решению финансовой организации при модернизации АС проводится контроль защищенности только элементов информационной инфраструктуры, подвергнутых модернизации.

9.7 Базовый состав мер защиты информации на этапе «Эксплуатация (сопровождение) АС» приведен в таблице 55.

Таблица 55 — Базовый состав мер защиты информации на этапе «Эксплуатация (сопровождение) АС»

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЖЦ.15	Реализация контроля эксплуатации технических мер системы защиты информации АС в соответствии с положениями проектной и эксплуатационной документации, включающего: - контроль фактического размещения технических мер защиты в промышленной среде; - контроль фактических параметров настроек технических мер защиты информации и информационной инфраструктуры, предназначенной для размещения технических мер защиты информации	О	О	О
ЖЦ.16	Реализация контроля применения мер системы защиты информации АС	О	О	О
ЖЦ.17	Назначение и реализация контроля деятельности лиц, ответственных за эксплуатацию (сопровождение) системы защиты информации АС	О	О	О
ЖЦ.18	Обеспечение возможности сопровождения технических мер системы защиты информации АС в течение всего срока их использования	Н	О	О
ЖЦ.19	Обеспечение доступности технических мер системы защиты информации АС: - применение отказоустойчивых технических мер; - резервирование технических средств АС, необходимых для функционирования технических мер; - осуществление контроля безотказного функционирования технических мер; - принятие регламентированных мер по восстановлению отказавших технических мер и технических средств АС, необходимых для их функционирования	Н	Н	Т
ЖЦ.20	Реализация проведения ежегодного контроля защищенности АС, включающего: - тестирование на проникновение; - анализ уязвимостей системы защиты информации АС и информационной инфраструктуры промышленной среды	Н	О	О
ЖЦ.21	Обеспечение оперативного устранения выявленных уязвимостей защиты информации АС, включая уязвимости прикладного ПО	О	О	О
ЖЦ.22	Регистрация внесения изменений в АС, включая обновление прикладного ПО	Н	О	О
ЖЦ.23	Регистрация операций по изменению параметров настроек технических мер системы защиты информации АС	О	Т	Т
ЖЦ.24	Реализация контроля в сегментах разработки и тестирования корректности функционирования систем защиты информации АС после внесения изменений в АС, включая обновления прикладного ПО	Н	О	О
ЖЦ.25	Реализация управления версиями (сборками) и изменениями прикладного ПО при его обновлении (модификации)	Н	О	О

9.8 Базовый состав мер защиты информации на этапе «Эксплуатация (сопровождение) и снятие с эксплуатации АС» приведен в таблице 56.

Таблица 56 — Базовый состав мер защиты информации на этапе «Эксплуатация (сопровождение) и снятие с эксплуатации АС»

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЖЦ.26	Принятие мер по обеспечению защиты информации от несанкционированного копирования и распространения	О	О	О
ЖЦ.27	Обеспечение защиты резервных копий защищаемой информации	Н	О	О
ЖЦ.28	Реализация контроля уничтожения защищаемой информации в случаях, когда указанная информация больше не используется, в том числе содержащейся в архивах, с применением мер ПУИ.23 — ПУИ.26 таблицы 31	Н	О	О

Приложение А
(справочное)

Основные положения базовой модели угроз и нарушителей безопасности информации

А.1 Основой для реализации финансовой организацией системы защиты информации являются разработанные и утвержденные модели угроз и нарушителей безопасности информации.

Степень детализации содержимого моделей угроз и нарушителей безопасности информации может быть различна и определяется реальными потребностями финансовой организации.

А.2 Модели угроз и нарушителей безопасности информации носят прогнозный характер и разрабатываются на основе опыта, знаний и практики финансовой организации. Чем точнее сделан прогноз в отношении актуальных для финансовой организации угроз безопасности информации, тем адекватнее и эффективнее будут планируемые и предпринимаемые усилия по обеспечению требуемого уровня защиты информации. При этом следует учитывать, что со временем угрозы, их источники и сопутствующие риски могут изменяться. Поэтому модели угроз и нарушителей безопасности информации следует периодически пересматривать, для чего в финансовой организации должны быть установлены и выполняться процедуры регулярного анализа необходимости их пересмотра.

А.3 В случае отсутствия у финансовой организации потенциала, необходимого для самостоятельной разработки моделей угроз и нарушителей безопасности информации, указанные модели рекомендуется составлять с привлечением сторонних организаций, обладающих необходимым опытом, знаниями и компетенцией.

При разработке моделей угроз и нарушителей безопасности информации необходимо учитывать, что из всех возможных объектов атак с наибольшей вероятностью нарушитель выберет наиболее слабо контролируемый, где его деятельность будет оставаться необнаруженной максимально долго. Поэтому все критические операции в рамках бизнес-процессов и технологических процессов финансовой организации, где осуществляется любое взаимодействие субъектов доступа с объектами информатизации, должны особенно тщательно контролироваться.

А.4 На каждом из уровней информационной инфраструктуры, определенных в 6.2 настоящего стандарта, актуальные угрозы безопасности информации и их источники являются различными.

Одной из основных целей злоумышленника является осуществление НСД к информационным ресурсам на уровне АС и приложений, эксплуатируемых в рамках бизнес-процессов или технологических процессов финансовой организации, что более эффективно для злоумышленника и опаснее для финансовой организации, чем осуществление НСД через иные уровни, требующего специфических знаний, ресурсов и времени.

Целью злоумышленника также может являться нарушение непрерывности предоставления финансовых услуг, осуществления бизнес-процессов или технологических процессов финансовой организации, например посредством распространения вредоносного кода, целенаправленных компьютерных атак или нарушения правил эксплуатации на уровне аппаратного обеспечения.

А.5 Основными типами источников угроз безопасности информации являются:

- неблагоприятные события техногенного характера;
- сбои и отказы в работе объектов и (или) ресурсов доступа;
- зависимость процессов эксплуатации объектов информатизации от иностранных поставщиков или провайдеров услуг;
- внутренние нарушители безопасности информации — лица, в том числе работники финансовой организации и работники подрядных организаций, реализующие угрозы безопасности информации с использованием легально предоставленных им прав логического или физического доступа;
- внешние нарушители безопасности информации — лица, в том числе работники финансовой организации, реализующие угрозы безопасности информации без использования легально предоставленных прав логического или физического доступа, а также субъекты, не являющиеся работниками финансовой организации, реализующие целенаправленные компьютерные атаки, в том числе с целью личного обогащения или блокирования штатного функционирования бизнес-процессов или технологических процессов финансовой организации.

А.6 К числу наиболее актуальных источников угроз на уровне аппаратного обеспечения, уровне сетевого оборудования и уровне сетевых приложений и сервисов относятся следующие:

- сбои и отказы в работе объектов доступа;
- внутренние нарушители безопасности информации [эксплуатационный, вспомогательный (технический) персонал], осуществляющие целенаправленное деструктивное воздействие на объекты доступа;
- зависимость процессов эксплуатации объектов доступа от иностранных поставщиков или провайдеров услуг;
- внешние нарушители безопасности информации, обладающие знаниями о возможных уязвимостях защиты информации;
- внешние нарушители безопасности информации, организующие DoS, DDoS и иные виды компьютерных атак;

- комбинированные источники угроз: внешние и внутренние нарушители безопасности информации, действующие совместно и (или) согласованно.

А.7 К числу наиболее актуальных источников угроз на уровне серверных компонентов виртуализации, программных инфраструктурных сервисов, операционных систем, систем управления базами данных и серверов приложений относятся следующие:

- внутренние нарушители безопасности информации (эксплуатационный персонал), осуществляющие целенаправленные деструктивные воздействия на ресурсы доступа;
- внутренние нарушители безопасности информации (эксплуатационный персонал), реализующие угрозы безопасности информации с использованием легально предоставленных прав логического доступа;
- сбои и отказы в работе ПО;
- зависимость процессов эксплуатации ресурсов доступа, ПО от иностранных поставщиков или провайдеров услуг;
- внешние нарушители безопасности информации, обладающие знаниями о возможных уязвимостях защиты информации;
- комбинированные источники угроз: внешние и внутренние нарушители безопасности информации, действующие в сговоре.

А.8 К числу наиболее актуальных источников угроз на уровне АС и приложений, эксплуатируемых в рамках бизнес-процессов и технологических процессов финансовой организации, относятся следующие:

- внутренние нарушители безопасности информации (пользователи и эксплуатационный персонал АС и приложений), реализующие угрозы безопасности информации с использованием легально предоставленных прав логического доступа;
- внешние нарушители безопасности информации, обладающие знаниями о возможных уязвимостях защиты информации;
- зависимость процессов эксплуатации АС и приложений от иностранных поставщиков или провайдеров услуг;
- комбинированные источники угроз: внешние и внутренние нарушители безопасности информации, действующие в сговоре.

А.9 Наибольшими возможностями для нанесения ущерба финансовой организации обладают ее собственные работники. В этом случае содержанием деятельности нарушителя является прямое нецелевое использование предоставленных прав физического и (или) логического доступа. При этом он будет стремиться к сокрытию следов своей деятельности.

Внешний нарушитель безопасности информации, как правило, имеет сообщника (сообщников) внутри финансовой организации. При условии должного соблюдения требований к защите информации, в том числе требований к содержанию базового состава, составу мер защиты информации, установленных настоящим стандартом, соблюдения принципа «знать своего работника», реализация угроз внешними нарушителями безопасности информации, действующими самостоятельно, без соучастников внутри финансовой организации, значительно затруднена.

Приложение Б
(справочное)

Состав и содержание организационных мер, связанных с обработкой финансовой организацией персональных данных

Б.1 Цели обработки ПДн должны быть документально установлены и утверждены руководством финансовой организации.

Б.2 В финансовой организации должна быть установлена необходимость осуществления уведомления уполномоченного органа по защите прав субъектов ПДн об обработке ПДн и организована деятельность по своевременному направлению указанного уведомления в соответствии с требованиями [8].

Б.3 В финансовой организации должны быть установлены критерии отнесения АС к информационным системам персональных данных (ИСПДн).

Б.4 В финансовой организации должны быть определены, выполняться, регистрироваться и контролироваться процедуры учета ресурсов ПДн, в том числе учета ИСПДн.

Для каждого ресурса ПДн должно быть обеспечено:

- установление цели обработки ПДн;
- установление и соблюдение сроков хранения ПДн и условий прекращения их обработки;
- определение перечня и категорий обрабатываемых ПДн (специальные категории ПДн, биометрические ПДн, ПДн, полученные из общедоступных источников, или иные ПДн);
- выполнение процедур учета количества субъектов ПДн, в том числе субъектов ПДн, не являющихся работниками финансовой организации;
- выполнение ограничения обработки ПДн достижением цели обработки ПДн;
- соответствие содержания и объема обрабатываемых ПДн установленным целям обработки;
- точность, достаточность и актуальность ПДн, в том числе по отношению к целям обработки ПДн;
- выполнение установленных процедур получения согласия субъектов ПДн (их законных представителей) на обработку их ПДн в случае, если получение такого согласия необходимо в соответствии с требованиями [8];
- выполнение установленных процедур получения согласия субъектов ПДн на передачу обработки их ПДн третьим лицам в случае, если получение такого согласия необходимо в соответствии с требованиями [8];
- прекращение обработки ПДн и уничтожение либо обезличивание ПДн по достижении целей обработки, по требованию субъекта ПДн в случаях, предусмотренных [8], в том числе при отзыве субъектом ПДн согласия на обработку его ПДн.

Б.5 В финансовой организации должны быть определены, выполняться, регистрироваться и контролироваться процедуры прекращения обработки ПДн и их уничтожения либо обезличивания в сроки, установленные [8], в следующих случаях:

- по достижении цели обработки ПДн (если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между финансовой организацией и субъектом ПДн);
- отзыва субъектом ПДн согласия на обработку его ПДн и в случае, если сохранение ПДн более не требуется для целей обработки ПДн (если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между организацией банковской системы РФ и субъектом ПДн);
- если ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки;
- выявления неправомерной обработки ПДн, осуществляемой финансовой организацией или обработчиком, действующим по ее поручению, если обеспечить правомерность обработки ПДн невозможно;
- выявления неправомерной обработки ПДн без согласия субъекта ПДн.

В случае отсутствия возможности уничтожения ПДн либо обезличивания ПДн в течение срока, установленного [8], финансовая организация обеспечивает их блокирование с последующим обеспечением уничтожения ПДн. Уничтожение ПДн производится не позднее шести месяцев со дня их блокирования.

Б.6 В финансовой организации должна быть определена, выполняться и контролироваться политика в отношении обработки ПДн, а также в случае необходимости установлены порядки обработки ПДн для отдельных ресурсов ПДн. Для ресурсов ПДн, обрабатываемых в АС, в том числе ИСПДн, порядок обработки ПДн может являться частью эксплуатационной документации на АС и разрабатываться на этапе создания (модернизации) АС.

Указанные документы:

- определяют процедуры предоставления доступа к ПДн;
- определяют процедуры внесения изменений в ПДн с целью обеспечения их точности, достоверности и актуальности, в том числе по отношению к целям обработки ПДн;

- определяют процедуры уничтожения, обезличивания либо блокирования ПДн в случае необходимости выполнения таких процедур;

- определяют процедуры обработки обращений субъектов ПДн (их законных представителей) для случаев, предусмотренных Федеральным законом «О персональных данных», в частности порядок подготовки информации о наличии ПДн, относящихся к конкретному субъекту ПДн, информации, необходимой для предоставления возможности ознакомления субъектом ПДн (их законных представителей) с его ПДн, а также процедуры обработки обращений об уточнении ПДн, их блокировании или уничтожении, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для установленной цели обработки;

- определяют процедуры обработки запроса уполномоченного органа по защите прав субъектов ПДн;

- определяют процедуры получения согласия субъекта ПДн на обработку его ПДн и на передачу обработки его ПДн третьим лицам;

- определяют процедуры передачи ПДн между пользователями ресурса ПДн, предусматривающего передачу ПДн только между работниками финансовой организации, имеющими доступ к ПДн;

- определяют процедуры передачи ПДн третьим лицам;

- определяют процедуры работы с материальными носителями ПДн;

- определяют процедуры, необходимые для осуществления уведомления уполномоченного органа по защите прав субъектов ПДн об обработке ПДн в сроки, установленные [8];

- определяют необходимость применения типовых форм документов для осуществления обработки ПДн и процедуры работы с ними. Под типовой формой документа понимается шаблон, бланк документа или другая унифицированная форма документа, используемая финансовой организацией с целью сбора ПДн.

Б.7 Финансовая организация должна опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему ее политику в отношении обработки ПДн, а также к сведениям о реализуемых требованиях по обеспечению безопасности персональных данных.

Б.8 В финансовой организации должно быть установлено, в каких случаях необходимо получение согласия субъектов ПДн, при этом форма и порядок получения согласия субъектов ПДн должны быть регламентированы.

Б.9 В финансовой организации должны быть определены, выполняться, регистрироваться и контролироваться процедуры учета лиц, имеющих доступ к ПДн.

Документ, определяющий перечень лиц, имеющих доступ к ПДн, утверждается руководителем финансовой организации.

Б.10 Обработка ПДн работниками финансовой организации должны осуществляться только с целью выполнения их должностных обязанностей.

Б.11 В финансовой организации должны быть определены, выполняться, регистрироваться и контролироваться процедуры ознакомления работников, непосредственно осуществляющих обработку ПДн, с положениями законодательства РФ и внутренними документами финансовой организации, содержащими требования по обработке и обеспечению безопасности ПДн в части, касающейся их должностных обязанностей.

Б.12 В финансовой организации должны быть определены, выполняться, регистрироваться и контролироваться процедуры учета помещений, в которых осуществляется обработка ПДн, а также доступа работников и иных лиц в помещения, в которых ведется обработка ПДн.

Б.13 При работе с МНИ ПДн должно быть обеспечено выполнение содержания, предусмотренного мерами ПУИ.20, ПУИ.21, ПУИ.22, ПУИ.24 и ПУИ.26 таблицы 31, а также:

- обособление ПДн от иной информации, в частности путем фиксации их на отдельных МНИ ПДн, в специальных разделах или на полях форм документов (при обработке ПДн на бумажных носителях);

- хранение ПДн, цели обработки которых заведомо несовместимы, на отдельных МНИ;

- регистрация и учет мест хранения МНИ ПДн с фиксацией категории обрабатываемых персональных данных (специальные категории ПДн, биометрические ПДн, ПДн, полученные из общедоступных источников, или иные ПДн), включая раздельное хранение ресурсов ПДн, обработка которых осуществляется с различными целями;

- установление и выполнение порядка гарантированного уничтожения (стирания) информации с МНИ ПДн.

Б.14 Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн.

Б.15 Общедоступные источники ПДн создаются и публикуются финансовой организацией только для цели выполнения требований законодательства Российской Федерации. В финансовой организации должны быть определены, выполняться, регистрироваться и контролироваться процедуры публикации ПДн в общедоступных источниках ПДн.

Б.16 Поручение обработки ПДн третьему лицу (далее — обработчик) должно осуществляться на основании договора. В указанном договоре должны быть определены перечень действий (операций) с ПДн, которые будут совершаться обработчиком, и цели обработки, должна быть установлена обязанность обработчика обеспечивать безопасность ПДн (в том числе соблюдать конфиденциальность ПДн) при их обработке, не раскрывать и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом, а также должны

быть указаны требования по обеспечению безопасности ПДн. При поручении обработки ПДн обработчику финансовая организация должна получить согласие субъекта ПДн, если иное не предусмотрено законодательством Российской Федерации.

Б.17 В финансовой организации должны быть определены, выполняться, регистрироваться и контролироваться процедуры, выполняемые в случаях необходимости осуществления трансграничной передачи ПДн.

Б.18 В финансовой организации должно быть назначено лицо, ответственное за организацию обработки ПДн. Полномочия лица, ответственного за организацию обработки ПДн, а также его права и обязанности должны быть установлены руководством финансовой организации.

Приложение В
(справочное)

Перечень событий защиты информации, потенциально связанных с несанкционированным доступом и инцидентами защиты информации, рекомендуемых для выявления, регистрации и анализа

В.1 Действия и (или) операции по созданию, удалению, копированию ресурсов доступа.

В.2 Действия и (или) операции по созданию, удалению, блокированию, разблокированию учетных записей.

В.3 Действия и (или) операции по изменению (предоставлению) прав логического доступа.

В.4 Действия и (или) операции по подключению СВТ к вычислительным сетям финансовой организации.

В.5 Действия и (или) операции по запуску программных процессов.

В.6 Действия и (или) операции при осуществлении логического доступа.

В.7 Факты выявления уязвимостей защиты информации.

В.8 Факты выявления вредоносного кода и (или) мобильного кода.

В.9 Факты выявления попыток осуществления вторжений и сетевых атак.

В.10 Факты выявления атак типа «отказ в обслуживании».

В.11 Действия и (или) операции, направленные на изменение правил сегментации и межсетевого экранирования вычислительных сетей финансовой организации.

В.12 Действия и (или) операции по изменению параметров настроек технических мер защиты информации, параметров настроек системного ПО, влияющих на обеспечение защиты информации.

В.13 Факты выявления нарушений и сбоев в работе технических мер защиты информации.

В.14 Факты выявление нарушений и сбоев в установлении (обновлении) ПО и параметров настроек технических мер защиты информации, их сигнатурных баз (в случае их использования).

В.15 Факты выявления нарушений и сбоев в установлении (обновлении) системного ПО и параметров его настроек, влияющих на обеспечение защиты информации.

В.16 Действия и (или) операции по изменению состава ПО АРМ пользователей и эксплуатационного персонала, в том числе запускаемого автоматически при загрузке операционных систем.

В.17 Действия и (или) операции по изменению состава ПО серверного оборудования.

В.18 Факты выявления нарушений целостности ПО АС на АРМ пользователей и эксплуатационного персонала.

В.19 Факты выявления нарушений доверенной загрузки операционных систем АРМ пользователей и эксплуатационного персонала.

В.20 Факты выявления нарушений целостности эталонных копий ПО, в том числе при осуществлении их распространения и (или) обновления.

В.21 Факты выявления смены и (или) компрометации аутентификационных данных, используемых для доступа к серверному и сетевому оборудованию.

В.22 Действия и (или) операции со средствами криптографической защиты информации и ключевой информацией.

В.23 Действия и (или) операции по использованию разблокированных коммуникационных портов.

В.24 Действия и (или) операции по передаче информации с использованием электронной почты.

В.25 Действия и (или) операции при осуществлении доступа к ресурсам сети Интернет.

В.26 Действия и (или) операции при осуществлении доступа к серверным компонентам виртуализации виртуальными машинами, логическими разделами или томами.

В.27 Факты выявления нарушений при доверенной загрузке виртуальных машин.

В.28 Действия и (или) операции при администрировании системы хранения данных.

В.29 Действия и (или) операции по использованию подконтрольных мобильных устройств.

Библиография

[1] Федеральный закон от 10 июля 2002 г. № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)»

[2] Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе»

[3] Федеральный закон от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации»

[4] ИСО/МЭК 29115:2013 (ISO/IEC 29115:2013) — Информационная технология. Техника безопасности. Схема обеспечения идентификации объекта (Information technology — Security techniques — Entity authentication assurance framework)

[5] Рекомендации в области стандартизации Банка России РС БР ИББС-2.2—2009 — Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности

[6] Рекомендации в области стандартизации Банка России РС БР ИББС-2.7—2015 — Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Ресурсное обеспечение информационной безопасности

[7] Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

[8] Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

[9] Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»

[10] Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденное Приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 г. № 66

[11] Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»

[12] Требования к системам обнаружения вторжений, утвержденные Приказом ФСТЭК России от 6 декабря 2011 г. № 638

[13] Требования к средствам антивирусной защиты, утвержденные Приказом ФСТЭК России от 20 марта 2012 г. № 28

[14] Рекомендации в области стандартизации Банка России РС БР ИББС-2.9—2016 — Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Предотвращение утечек информации

[15] Рекомендации в области стандартизации Банка России РС БР ИББС-2.5—2014 — Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности

[16] Рекомендации в области стандартизации Банка России РС БР ИББС-2.8—2015 — Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности при использовании технологии виртуализации

[17] Рекомендации в области стандартизации Банка России РС БР ИББС-2.0—2007 — Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0

[18] Рекомендации в области стандартизации Банка России РС БР ИББС-2.6—2014 — Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем

УДК 351.864.1:004:006.354

ОКС 03.060
35.240.40

Ключевые слова: защита информации, система защиты информации, уровень защиты информации, требования к системе защиты информации, требования к системе управления защитой информации, организационные меры защиты информации, технические меры защиты информации

Редактор *Е.В. Яковлева*
Технические редакторы *В.Н. Прусакова, И.Е. Черепкова*
Корректор *Е.Р. Ароян*
Компьютерная верстка *Ю.В. Поповой*

Сдано в набор 27.02.2020. Подписано в печать 06.04.2020. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 7,44. Уч.-изд. л. 6,73.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

ИД «Юриспруденция», 115419, Москва, ул. Орджоникидзе, 11.
gost.e-ecolog.ru gost.e-ecolog.ru

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru