МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**



**МОСКОВСКИЙ**

**ПОЛИТЕХ**

ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Кафедра «Информационная безопасность»

Проектная деятельность

Тема: “Оценка зрелости процессов ИБ в соответствии с **ГОСТ 57580.1**”

Выполнил: Студент 2 курса гр. 191-331

Ефимов Артём Андреевич

Научный руководитель:

Агеева Елена Александровна

2020 г. Москва

**Содержание:**

Обозначения и сокращения……………………………………………………...3

1 этап……………………………………………………………………………...4

Вступление……………………………………………………………………….4Общие положения …………….……………….………………………………..5

Требования к системе защиты информации ……….…………………………8

Требования к организации и управлению защитой информации и требования к защите информации на этапах жизненного цикла автоматизированных систем и приложений ………………………………………………………….10

Вывод…………………………………………………………………………….13

2 этап……………………………………………………………………………..14

7 раздел настоящего стандарта…………………………………………………14

8 раздел настоящего стандарта…………………………………………………28

9 раздел настоящего стандарта…………………………………………………34

Заключение………………………………………………………………………36

**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.

**1 этап**

**Вступление:**

Развитие и укрепление банковской системы Российской Федерации, развитие и обеспечение стабильности финансового рынка Российской Федерации и национальной платежной системы являются целями деятельности Банка России. 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.

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 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.

**Общие положения**

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;

- применение на различных уровнях информационной инфраструктуры выбранных финансовой организацией мер защиты информации, направленных на непосредственное обеспечение защиты информации и входящих в систему защиты информации;

- 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;

- применение выбранных финансовой организацией мер защиты информации, направленных на обеспечение защиты информации на всех стадиях жизненного цикла АС и приложений;

При идентификации и учете объектов информатизации рассматриваются 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.

Выбор и применение мер защиты информации включает:

- выбор мер защиты информации, установленных для определенного уровня защиты информации;

- адаптация (уточнение) набора мер защиты с учетом модели угроз и нарушителя и характеристик объектов информатизации;

- исключение из базового состава тех мер, которые не связаны с используемыми информационными технологиями;

- дополнение набор мер защиты информации мерами, установленными НПА с области ЗИ;

- применение дополнительных мер организации управления защитой информации, а также мер ЗИ на этапах жизненного цикла.

При невозможности реализации некоторых мер и с учетом экономической целесообразности на этапе адаптации (уточнения) могут разрабатываться компенсирующие меры защиты.

В Стандарте установлены 3 возможных уровня защиты информации:

- уровень 3 – минимальный;

- уровень 2 – стандартный;

- уровень 1 – усиленный.

В финансовой организации могут быть сформированы один или несколько контуров безопасности.

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

- вида деятельности финансовой организации, состава предоставляемых финансовых услуг, реализуемых бизнес-процессов и (или) технологических процессов в рамках 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.

**Требования к системе защиты информации**

В данном разделе описаны меры защиты информации для 8 процессов и 10 подпроцессов защиты информации:

1. «Обеспечение защиты информации при управлении доступом» с подпроцессами:

     a. управление учетными записями и правами субъектов логического доступа;

  b. идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа;

     c. защита информации при осуществлении физического доступа;

     d. идентификация, классификация и учет ресурсов и объектов доступа.

2. «Обеспечение защиты вычислительных сетей» с подпроцессами:

     a. сегментация и межсетевое экранирование вычислительных сетей;

     b. выявление сетевых вторжений и атак;

     c. защита информации, передаваемой по вычислительным сетям;

     d. защита беспроводных сетей.

3. «Контроль целостности и защищенности информационной инфраструктуры».

4. «Защита от вредоносного кода».

5. «Предотвращение утечек информации, защита машинных носителей информации (МНИ)».

6. «Управление инцидентами защиты информации» с подпроцессами:

     a. мониторинг и анализ событий защиты информации;

     b. обнаружение инцидентов защиты информации и реагирование на них;

7. «Защита среды виртуализации».

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

Способы реализации мер защиты информации установленные в таблицах раздела настоящего стандарта, обозначены следующим образом:  
  
- "О" - реализация путем применения организационной меры защиты информации  
 По решению финансовой организации, способ "О" может быть реализован путем применения технической меры защиты информации.  
- "Т" - реализация путем применения технической меры защиты информации;  
- "Н" - реализация является необязательной.

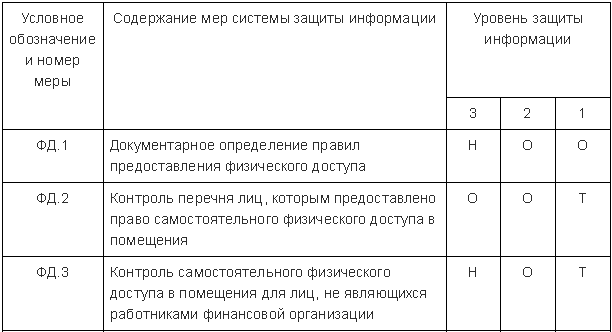


Рис.1 Пример таблицы требований для Подпроцесса "Защита информации при осуществлении физического доступа"

**Требования к системе защиты информации и требования к защите информации на этапах жизненного цикла автоматизированных систем и приложений**

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.

Меры системы организации и управления защитой информации применяются:  
- на системных уровнях информационной инфраструктуры;  
- 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.

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").

В Разделе 9 (Требования к защите информации на этапах жизненного цикла автоматизированных систем и приложений) описаны требования к защите информации на этапах жизненного цикла АС и приложений.

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.

Этапы жизненного цикла АС и приложений:

1. Создание (модернизация) АС.

2. Ввод в эксплуатацию АС.

3. Эксплуатация (сопровождение) АС.

4. Эксплуатация (сопровождение) и снятие с эксплуатации АС.

Для каждого направления раздела 8 и этапа жизненного цикла раздела 9 аналогично разделу 7 создаются таблицы с указанием содержания мер системы защиты информации и уровнем защиты безопасности

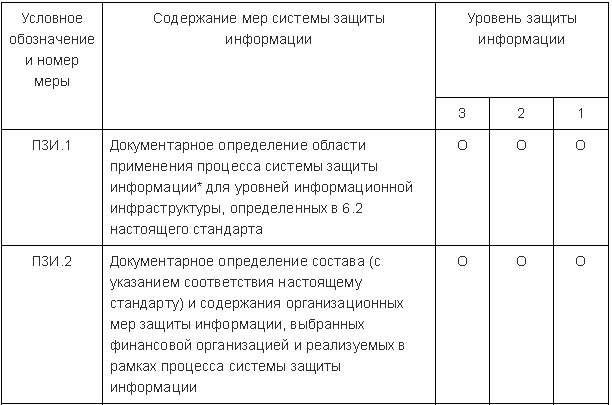


Рис.2 Пример таблицы базового состава мер планирования процесса системы защиты информации

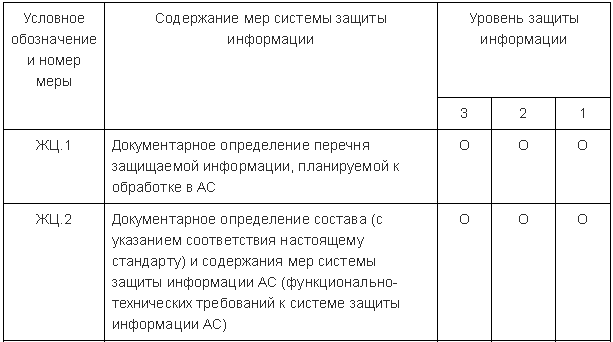


Рис.3 Пример таблицы базовый состава мер защиты информации на этапе "Создание (модернизация) АС"

**Вывод.**  
Таким образом, основными целями настоящего стандарта являются:

- определение уровней защиты информации и соответствующих им требований к содержанию базового состава организационных и технических 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;

- обеспечение эффективности и возможности стандартизированного контроля мероприятий по защите информации, проводимых финансовыми организациями.

**2 этап**

На данном этапе я более подробно освещу каждый процесс, подпроцесс и направление требований к организации и управлению защитой информации.

**7 раздел настоящего стандарта**

Настоящий раздел “Требования к системе защиты информации” устанавливает требования к содержанию базового состава мер защиты информации для следующих процессов (направлений) защиты информации:

**Процесс 1** «Обеспечение защиты информации при управлении доступом»:

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

**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.

**Процесс 3** «Контроль целостности и защищенности информационной инфраструктуры». **Процесс 4** «Защита от вредоносного кода».

**Процесс 5** «Предотвращение утечек информации».

**Процесс 6** «Управление инцидентами защиты информации»:

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

**Процесс 7** «Защита среды виртуализации».

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

### Процесс 1 "Обеспечение защиты информации при управлении доступом"

### Подпроцесс "Управление учетными записями и правами субъектов логического доступа"

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.

### Подпроцесс "Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа"

Применяемые финансовой организацией меры по идентификации, аутентификация, 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.

### Подпроцесс "Защита информации при осуществлении физического доступа"

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.

Подпроцесс "Идентификация и учет ресурсов и объектов доступа"

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](http://docs.cntd.ru/document/1200004675).

### Процесс 2 "Обеспечение защиты вычислительных сетей"

Подпроцесс "Сегментация и межсетевое экранирование вычислительных сетей"

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](http://docs.cntd.ru/document/1200089172).

Подпроцесс "Выявление вторжений и сетевых атак"

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.

Подпроцесс "Защита информации, передаваемой по вычислительным сетям"

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

Подпроцесс "Защита беспроводных сетей"

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.

### Процесс 3 "Контроль целостности и защищенности информационной инфраструктуры"

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.

### Процесс 4 "Защита от вредоносного кода"

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.

### Процесс 5 "Предотвращение утечек информации"

# 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 РС БР ИББС-2.9-2016.

### Процесс 6 "Управление инцидентами защиты информации"

Подпроцесс "Мониторинг и анализ событий защиты информации"

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](http://docs.cntd.ru/document/1200068822).  
  
Примечание - Рекомендации по обнаружению инцидентов информационной безопасности и реагированию на инциденты информационной безопасности приведены в РС БР ИББС-2.5-2014.

Подпроцесс "Обнаружение инцидентов защиты информации и реагирование на них"

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](http://docs.cntd.ru/document/1200068822).  
  
Примечание - Рекомендации по обнаружению инцидентов информационной безопасности и реагированию на инциденты информационной безопасности приведены в РС БР ИББС-2.5-2014.

### Процесс 7 "Защита среды виртуализации"

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

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 РС БР ИББС-2.8-2015 и [ГОСТ Р 56938](http://docs.cntd.ru/document/1200135524).

### Процесс 8 "Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств"

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.

Ниже приведена сводная таблица по количеству мер, установленных для процессов и подпроцессов раздела 7.

|  |  |  |  |
| --- | --- | --- | --- |
| **Процесс защиты информации, подпроцесс или группа мер ЗИ** | **Уровень защиты информации** | | |
| **3** | **2** | **1** |
| Процесс 1 «Обеспечение защиты информации при управлении доступом» | Т – 30  О – 33  Н – 39 | Т – 55  О – 33  Н – 14 | Т – 73  О – 25  Н – 4 |
| Подпроцесс «Управление учетными записями и правами субъектов логического доступа» | Т – 7  О – 15  Н – 7 | Т – 18  О – 9  Н – 2 | Т – 21  О – 7  Н – 1 |
| Подпроцесс «Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа» | Т – 23  О – 8  Н – 13 | Т – 30  О – 9  Н – 5 | Т – 33  О – 9  Н – 2 |
| Подпроцесс «Защита информации при осуществлении физического доступа» | Т – 0  О – 6  Н – 15 | Т – 3  О – 12  Н – 6 | Т – 11  О – 9  Н – 1 |
| Подпроцесс «Идентификация и учет ресурсов и объектов доступа» | Т – 0  О – 4  Н – 4 | Т – 4  О – 3  Н – 1 | Т – 8  О – 0  Н – 0 |
| Процесс 2 «Обеспечение защиты вычислительных сетей» | Т – 11  О – 0  Н – 36 | Т – 32  О – 1  Н – 14 | Т – 45  О – 0  Н – 2 |
| Подпроцесс «Сегментация и межсетевое экранирование вычислительных сетей» | Т – 6  О – 0  Н – 15 | Т – 14  О – 1  Н – 6 | Т – 20  О – 0  Н – 1 |
| Подпроцесс «Выявление вторжений и сетевых атак» | Т – 1  О – 0  Н – 13 | Т – 9  О – 0  Н – 5 | Т – 14  О – 0  Н – 0 |
| Подпроцесс «Защита информации, передаваемой по вычислительным сетям» | Т – 2  О – 0  Н – 0 | Т – 2  О – 0  Н – 0 | Т – 2  О – 0  Н – 0 |
| Подпроцесс «Защита беспроводных сетей» | Т – 2  О – 0  Н – 8 | Т – 7  О – 0  Н – 3 | Т – 9  О – 0  Н – 1 |
| Процесс 3 «Контроль целостности и защищенности информационной инфраструктуры» | Т – 0  О – 13  Н – 23 | Т – 21  О – 8  Н – 7 | Т – 33  О – 3  Н – 0 |
| Процесс 4 «Защита от вредоносного кода» | Т – 20  О – 1  Н – 7 | Т – 26  О – 1  Н – 1 | Т – 26  О – 1  Н – 1 |
| Процесс 5 «Предотвращение утечек информации» | Т – 2  О – 5  Н – 26 | Т – 22  О – 6  Н – 5 | Т – 24  О – 6  Н – 3 |
| Процесс 6 «Управление инцидентами защиты информации» | Т – 14  О – 11  Н – 17 | Т – 29  О – 9  Н – 4 | Т – 31  О – 8  Н – 3 |
| Подпроцесс «Мониторинг и анализ событий защиты информации» | Т – 11  О – 1  Н – 11 | Т – 21  О – 0  Н – 2 | Т – 22  О – 0  Н – 1 |
| Подпроцесс «Обнаружение инцидентов защиты информации и реагирование на них» | Т – 3  О – 10  Н – 6 | Т – 8  О – 9  Н – 2 | Т – 9  О – 8  Н – 2 |
| Процесс 7 «Защита среды виртуализации» | Т – 12  О – 2  Н – 29 | Т – 25  О – 6  Н – 12 | Т – 33  О – 6  Н – 4 |
| Процесс 8 «Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств» | Т – 6  О – 1  Н – 5 | Т – 11  О – 1  Н – 0 | Т – 11  О – 1  Н – 0 |
| **Всего по разделу 7** | **Т – 95**  **О – 66**  **Н – 182** | **Т – 221**  **О – 65**  **Н – 57** | **Т – 276**  **О – 50**  **Н – 17** |

- «О» – реализация путем применения организационной меры защиты информации (по решению финансовой организации способ реализации может быть заменен на техническую меру ЗИ);  
- «Т» – реализация путем применения технической меры защиты информации;  
- «Н» – реализация является необязательной.

**8 раздел настоящего стандарта**

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.

Меры системы организации и управления защитой информации применяются:  
- на системных уровнях информационной инфраструктуры;  
- 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.

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.

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").

### Направление 1 "Планирование процесса системы защиты информации"

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 РС БР ИББС-2.0-2007.

### Направление 2 "Реализация процесса системы защиты информации"

Деятельность в рамках направления "Реализация" выполняется по результатам выполнения направлений "Планирование" и (или) "Совершенствование".  
  
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 РС БР ИББС-2.7-2015.

### Направление 3 "Контроль процесса системы защиты информации"

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.

### Направление 4 "Совершенствование процесса системы защиты информации"

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".

Ниже приведена таблица по количеству мер защиты, установленных для каждого из направлений управления защитой информации.

|  |  |  |  |
| --- | --- | --- | --- |
| **Направление защиты информации** | **Уровень защиты информации** | | |
| **3** | **2** | **1** |
| Направление 1 «Планирование процесса системы защиты информации» | Т – 0  О – 5  Н – 0 | Т – 0  О – 5  Н – 0 | Т – 0  О – 5  Н – 0 |
| Направление 2 «Реализация процесса системы защиты информации» | Т – 1  О – 9  Н – 6 | Т – 1  О – 10  Н – 5 | Т – 6  О – 8  Н – 2 |
| Направление 3 «Контроль процесса системы защиты информации» | Т – 0  О – 8  Н – 4 | Т – 6  О – 6  Н – 0 | Т – 8  О – 4  Н – 0 |
| Базовый состав мер контроля процесса системы защиты информации | Т – 0  О – 8  Н – 0 | Т – 2  О – 6  Н – 0 | Т – 4  О – 4  Н – 0 |
| Базовый состав мер контроля процесса системы защиты информации, в части регистрации событий защиты информации | Т – 0  О – 0  Н – 4 | Т – 4  О – 0  Н – 0 | Т – 4  О – 0  Н – 0 |
| Направление 4 «Совершенствование процесса системы защиты информации» | Т – 0  О – 4  Н – 0 | Т – 0  О – 4  Н – 0 | Т – 0  О – 4  Н – 0 |
| **Всего по разделу 8** | **Т – 1**  **О – 26**  **Н – 10** | **Т – 7**  **О – 25**  **Н – 5** | **Т – 14**  **О – 21**  **Н – 2** |

- «О» – реализация путем применения организационной меры защиты информации (по решению финансовой организации способ реализации может быть заменен на техническую меру ЗИ);  
- «Т» – реализация путем применения технической меры защиты информации;  
- «Н» – реализация является необязательной.

**9 раздел настоящего стандарта**

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).

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 “Требования к системе защиты информации” 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.

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.

Ниже приведена таблица по количеству мер, установленных для каждого этапа жизненного цикла.

|  |  |  |  |
| --- | --- | --- | --- |
| **Этап жизненного цикла АС и приложений** | **Уровень защиты информации** | | |
| **3** | **2** | **1** |
| Создание (модернизация) АС | Т – 0  О – 8  Н – 3 | Т – 0  О – 11  Н – 0 | Т – 0  О – 11  Н – 0 |
| Ввод в эксплуатацию АС | Т – 0  О – 2  Н – 1 | Т – 0  О – 3  Н – 0 | Т – 0  О – 3  Н – 0 |
| Эксплуатация (сопровождение) АС | Т – 0  О – 5  Н – 6 | Т – 1  О – 9  Н – 1 | Т – 2  О – 9  Н – 0 |
| Эксплуатация (сопровождение) и снятие с эксплуатации АС | Т – 0  О – 1  Н – 2 | Т – 0  О – 3  Н – 0 | Т – 0  О – 3  Н – 0 |
| **Всего по разделу 9** | **Т – 0**  **О – 16**  **Н – 12** | **Т – 1**  **О – 26**  **Н – 1** | **Т – 2**  **О – 26**  **Н – 0** |

- «О» – реализация путем применения организационной меры защиты информации (по решению финансовой организации способ реализации может быть заменен на техническую меру ЗИ);  
- «Т» – реализация путем применения технической меры защиты информации;  
- «Н» – реализация является необязательной.

**Заключение**

В статье представлен краткий обзор национального стандарта Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер». Стандарт включил в себя как различные положения существующих практик по информационной безопасности в Банке России, так и новые подходы. В частности, введена классификация по уровням защиты информации, а также предоставлен гибкий механизм выбора защитных мер.