## Лекция № 9

# ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНИЗАЦИИ

# Лекция № 9
# ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНИЗАЦИИ

**Цель занятия:** рассмотреть основные сведения и характеристики политики информационной безопасности организации персональных данных

**ВОПРОС 1. Определение политики информационной безопасности персональных данных в организации**
**ВОПРОС 2. Принципы политики безопасности персональных данных**
**ВОПРОС 3. Практические аспекты выполнения законодательных требований при обработке персональных данных**
**ВОПРОС 4. Практические примеры частных политик информационной безопасности**

# Лекция № 9

## ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНИЗАЦИИ

**ВОПРОС 1. Определение политики информационной безопасности персональных данных в организации**

**ВОПРОС 1.**
**Определение политики информационной безопасности персональных данных в организации**

**ПОЛИТИКА БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ — формальное изложение правил поведения, процедур, практических приемов или руководящих принципов в области информационной безопасности, которыми руководствуется организация в своей деятельности.**

***ПРИМЕЧАНИЕ*** :

Политики должны содержать:

- предмет, основные цели и задачи политики безопасности;
- условия применения политики безопасности и возможные ограничения;
- описание позиции руководства организации в отношении выполнения политики безопасности и организации режима информационной безопасности организации в целом;
- права и обязанности, а также степень ответственности сотрудников за выполнение политики безопасности организации;
- порядок действия а чрезвычайных ситуациях а случае нарушения политики безопасности.

Национальный стандарт Российской Федерации ГОСТ Р 53114-2008
Защита информации.
Обеспечение информационной безопасности в организации.
Основные термины и определения

**ВОПРОС 1.**
**Определение политики информационной безопасности персональных данных в организации**

**ЦЕЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ОРГАНИЗАЦИИ) - заранее намеченный результат обеспечения информационной безопасности организации в соответствии с установленными требованиями в политике ИБ (организации).**

***ПРИМЕЧАНИЕ:***

**Результатом обеспечения ИБ может быть предотвращение ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию.**

**Национальный стандарт Российской Федерации ГОСТ Р 53114-2008**
**Защита информации.**
**Обеспечение информационной безопасности в организации.**
- **Основные термины и определения**

## ВОПРОС 1.
## Определение политики информационной безопасности персональных данных в организации

Среднестатистический проект по защите персональных данных организации длится 4-6 месяцев.

В условиях жесткой экономии времени, особенную актуальность приобретает вопрос комплексного подхода к разработке проекта по защите ПДн «под ключ», разработки правил поведения, процедур, практических приемов или руководящих принципов в области информационной безопасности, которыми будет руководствоваться организация в своей деятельности при защите ПДн.

Такой своеобразный набор услуг по защите ПДн разрабатывается на основании четкого понимания значимости его составляющих, их необходимости и срочности.

## ВОПРОС 1.
## Определение политики информационной безопасности персональных данных в организации

В классическом своем варианте данный классический набор услуг может быть представлен в виде следующих **5 позиций**, которые представляют собой основные этапы проекта по защите ПДн.

1. ПРЕДПРОЕКТНОЕ ОБСЛЕДОВАНИЕ
2. РАЗРАБОТКА НОРМАТИВНОЙ БАЗЫ
3. ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ
4. ВНЕДРЕНИЕ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ
5. ОЦЕНКА СООТВЕТСТВИЯ ИСПДн

# ВОПРОС 1.
# Определение политики информационной безопасности персональных данных в организации

## 1. ПРЕДПРОЕКТНОЕ ОБСЛЕДОВАНИЕ

Предпроектное обследование включает:

1. аудит имеющейся нормативной базы,
2. анализ информационных потоков ПДн и их уязвимостей,
3. инвентаризация ИСПДн,
4. выносятся предложения по оптимизации имеющихся структурных решений и т.п.

**Именно этот этап позволяет выявить и описать те требования, которые будут предъявляться к ИСПДн.**

**ВОПРОС 1.**
**Определение политики информационной безопасности персональных данных в организации**

## 2. РАЗРАБОТКА НОРМАТИВНОЙ БАЗЫ

**Разработка нормативной базы** по защите ПДн может быть проведена только на основании предварительно выполненного аудита.

Стандартный пакет нормативных документов ПИБ ПДн входят:

- положения об обработке и защите ПДн,
- регламенты различных взаимодействий при обработке и передаче ПДн
- должностные инструкции для персонала в части обеспечения безопасности ПДн,
- инструкции по работе с ПДн,
- акты классификации ИСПДн,
- перечни ПДн и лиц, допущенных к их обработке,
- техническая и эксплуатационная документация (в том числе и на средства криптографической защиты) и др.

**ВОПРОС 1.**
**Определение политики информационной безопасности персональных данных в организации**

## 3. ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

**Проектирование** системы защиты ПДн, включает в себя:

- выбор способов, мер и классов средств защиты ПДн,
- разработка технического задания на разработку СЗПДн,
- разработка конкретных мероприятий по защите информации.

По окончании данного этапа организация уже вполне сможет пройти проверку одного из государственных регуляторов.

**ВОПРОС 1.**
**Определение политики информационной безопасности персональных данных в организации**

## 4. ВНЕДРЕНИЕ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

**Внедрение СЗПДн:**

- ввод в действие системы защиты,
- настройка существующих средств защиты.

Реализация данного этапа обычно проводится оператором ПДн самостоятельно, при необходимости специалистами интегратора оказывается консультативная поддержка процесса.

**ВОПРОС 1.**
**Определение политики информационной безопасности персональных данных в организации**

## 5. ОЦЕНКА СООТВЕТСТВИЯ ИСПДн

**Оценка соответствия** ИСПДн - в рамках такого процесса проводятся оценочные испытания ИСПДн и выдается соответствующий Аттестат.

## ВОПРОС 1.
## Определение политики информационной безопасности персональных данных в организации

В сформированную рабочую группу необходимо включить представителей всех структур организации, которые так или иначе имеют дело с обработкой персональных данных

Наиболее рациональный состав рабочей группы состоит из представителей различных отделов организации:

- отдел информационной безопасности и защиты информации,
- департамент программного и технического обеспечения,
- департамент персонала,
- департамент бухгалтерского учета,
- юридический отдел и т.п.

## ВОПРОС 1.
## Определение политики информационной безопасности персональных данных в организации

В сформированную рабочую группу необходимо включить представителей всех структур организации, которые так или иначе имеют дело с обработкой персональных данных

**Со стороны организации-Исполнителя проекта состав и численность рабочей группы может варьироваться, в зависимости от сложности проектных задач.**

Типовой вариант рабочей группы включает:

- **руководитель проекта,**
- **аналитик по информационной безопасности,**
- **специалист по информационной безопасности**
- **юрист.**

# Лекция № 9

## ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНИЗАЦИИ

ВОПРОС 2. **Принципы политики безопасности персональных данных**

# ВОПРОС 2.
# Принципы политики безопасности персональных данных

**Обработка персональных данных должна осуществляться на основе принципов:**

1) законности целей и способов обработки персональных данных и добросовестности;
2) соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;
3) соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
4) достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
5) недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

Федеральный закон от 27 июля 2006 г. №152-ФЗ "О персональных данных"

## ВОПРОС 2.
## Принципы политики безопасности персональных данных

**ПРИНЦИПЫ БЕЗОПАСНОСТИ .**

Для создания эффективной программы безопасности информационных и телекоммуникационных технологий фундаментальными являются следующие высокоуровневые принципы безопасности:

1. **менеджмент риска**
2. **обязательства**
3. **служебные обязанности и ответственность**
4. **цели, стратегии и политика**
5. **управление жизненным циклом**

**Национальный стандарт РФ ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий**

## ВОПРОС 2.
## Принципы политики безопасности персональных данных

**ПРИНЦИПЫ БЕЗОПАСНОСТИ .**

**1. МЕНЕДЖМЕНТ РИСКА**— скоординированные действия по руководству и управлению организацией в отношении риска *(ГОСТ Р 51897-2002, ст.3.1.7).*

**ПРИМЕЧАНИЕ**:

**Обычно менеджмент риска включает в себя**

— ***оценку риска,***

— ***обработку риска,***

— ***принятие риска и***

— ***коммуникацию риска.***

**Государственный стандарт Российской Федерации**
**ГОСТ Р 51897-2002.**
**Менеджмент риска.**
**Термины и определения**

## ВОПРОС 2.
## Принципы политики безопасности персональных данных

**ПРИНЦИПЫ БЕЗОПАСНОСТИ**

**2. <u>ОБЯЗАТЕЛЬСТВА</u> — важны обязательства организации в области безопасности ИТ и в управлении рисками.**

**Для формирования обязательств следует разъяснить персоналу преимущества от реализации безопасности ИТ.**

## ВОПРОС 2.
## Принципы политики безопасности персональных данных

**ПРИНЦИПЫ БЕЗОПАСНОСТИ**

**3. СЛУЖЕБНЫЕ ОБЯЗАННОСТИ И ОТВЕТСТВЕННОСТЬ — руководство организации несет ответственность за обеспечение безопасности активов.**

**Служебные обязанности и ответственность, связанные с безопасностью ИТ, должны быть определены и доведены до сведения персонала.**

## ВОПРОС 2.
## Принципы политики безопасности персональных данных

**ПРИНЦИПЫ БЕЗОПАСНОСТИ .**

**4. ЦЕЛИ, СТРАТЕГИИ И ПОЛИТИКА – управление рисками, связанными с безопасностью ИТ, должно осуществляться с учетом целей, стратегий и Политики организации.**

## ВОПРОС 2.
## Принципы политики безопасности персональных данных

**ПРИНЦИПЫ БЕЗОПАСНОСТИ**

**5. УПРАВЛЕНИЕ ЖИЗНЕННЫМ ЦИКЛОМ — управление безопасностью ИТ должно быть непрерывным в течение всего их жизненного цикла.**

# ВОПРОС 2.
# Принципы политики безопасности персональных данных

## ПРИНЦИПЫ БЕЗОПАСНОСТИ

**ЖИЗНЕННЫЙ ЦИКЛ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ — совокупность взаимосвязанных процессов создания и последовательного изменения состояния АС от формирования исходных требований к ней до окончания эксплуатации и утилизации комплекса средств автоматизации АС.**

**Межгосударственный стандарт ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.**

# Лекция № 9

## ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНИЗАЦИИ

**ВОПРОС 3.** Практические аспекты выполнения законодательных требований при обработке персональных данных

# Служба информационной безопасности

- Удостоверяющий Центр Корпоративной Информационной Системы
- Отдел внедрения и сопровождения систем обеспечения информационной безопасности
- Отдел криптографической защиты информации
- Отдел администраторов безопасности
- Отдел информационной безопасности автоматизированных банковских систем
- Отдел безопасности платежных систем
- Отдел аудита и аттестации информационных систем

## СОДЕРЖАНИЕ ПИБ

1. Область применения
2. Нормативные ссылки
3. Термины и определения
4. Общие положения
5. Объекты защиты и субъекты информационных отношений
6. Исходная концептуальная схема обеспечения информационной безопасности
7. Основные принципы обеспечения информационной безопасности
8. Общие (основные) требования по обеспечению информационной безопасности
9. Система менеджмента информационной безопасности
10. Проверка и оценка информационной безопасности
11. Модель зрелости процессов менеджмента информационной безопасности
12. Правовые основы системы менеджмента информационной безопасности
13. Меры ответственности

# СОДЕРЖАНИЕ ПИБ

**12. Правовые основы системы менеджмента информационной безопасности**

12.1 Общие положения

12.2. Организация правовых процедур по защите информации, составляющей коммерческую тайну (сведений, являющихся секретом производства)

**12.3. Организация правовых процедур по защите персональных данных**

12.4. Организация правовых процедур по защите банковской тайны

12.5. Организация правовых процедур при лицензировании деятельности по защите информации и сертификации продукции (услуг).

# Основные мероприятия Плана по реализации требований Федерального закона «О персональных данных» № 152-ФЗ в банке

1. Корректировка Перечня сведений конфиденциального характера, подлежащих защите в банке, в части определения ПД.
2. Разработка Списка документов и форм, содержащих обрабатываемые ПД и порядка его ведения.
3. Разработка формы Согласия субъекта ПД – клиента банка.
4. Приведение в соответствие законодательным требованиям документационного обеспечения процессов обработки ПД в ИСПД банка.
5. Ревизия типовых договоров, анкет и других применяемых типовых форм.
6. Формирование Модели угроз безопасности персональных данных и Модели нарушителя.
7. Классификация ИСПД банка.
8. Обучение персонала.
9. Доработка ИСПД банка в соответствии с требованиями законодательства РФ по обработке ПД (по отдельному плану).
10. Аттестация ИСПД (объектов информатизации) банка.

# Перечень сведений, составляющих персональные данные

**1. Персональные данные 1 категории (специальные ПД).**

**1.1. Сведения о состоянии здоровья и интимной жизни, о расовой и национальной принадлежности, политических взглядах, религиозных или философских убеждениях (данные справок и медицинских заключений о состоянии здоровья, данные диспансеризации, данные листов о временной нетрудоспособности в части диагнозов заболеваний, признаки причастности клиентов к террористам или экстремистам, к влиятельным политическим лицам).**

**2. Персональные данные 2 категории (биометрические ПД).**

**Персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1:**
**2.1. Сведения о биометрических персональных данных, характеризующих физиологические особенности человека, за исключением персональных данных, относящихся к 1 категории (видеозаписи систем охранного телевидения, банковских терминальных устройств, ксерокопии с документов, удостоверяющих личность и имеющих фотографию владельца, фотографии сотрудников и клиентов Банка, данные в устройствах, использующих для идентификации биометрические данные человека).**

**3. Персональные данные 3 категории (общие ПД).**

**Персональные данные, позволяющие идентифицировать субъекта персональных данных:**
**3.1. Фамилия, имя, отчество, год, месяц, дата и место рождения, паспортные данные (номер, серия, данные о выдаче), сведения о месте и дате регистрации (месте жительства).**
**3.2. Сведения о номере и серии страхового свидетельства государственного пенсионного страхования.**
**3.3. Сведения из страховых полисов обязательного (добровольного) медицинского страхования (в т.ч. данные соответствующих карточек медицинского страхования).**
**3.4. Сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу.**
**……**

# Перечень сведений, составляющих персональные данные (продолжение)

**4. Персональные данные 4 категории (общедоступные ПД).**

**Обезличенные и (или) общедоступные персональные данные:**

**4.1. Сведения о семейном положении (состояние в браке, наличие брачного контракта, дата регистрации, фамилия, имя и отчество супруга (и) и его (ее) социальный статус, наличие детей и их возраст, семейные доходы и расходы, долги и другие сведения).**

**4.2. Данные о трудовой деятельности (данные о трудовой занятости на текущее время, стаж работы, наличие трудового договора, организации, занимаемые в них должности и время работы в этих организациях, а также другие сведения).**

**4.3. Сведения об образовании, квалификации, о наличии специальных знаний или специальной подготовки (образовательная категория, ученая степень, образовательное учреждение, дата начала и завершения обучения, квалификация и специальность по окончании учебного заведения и другие сведения).**

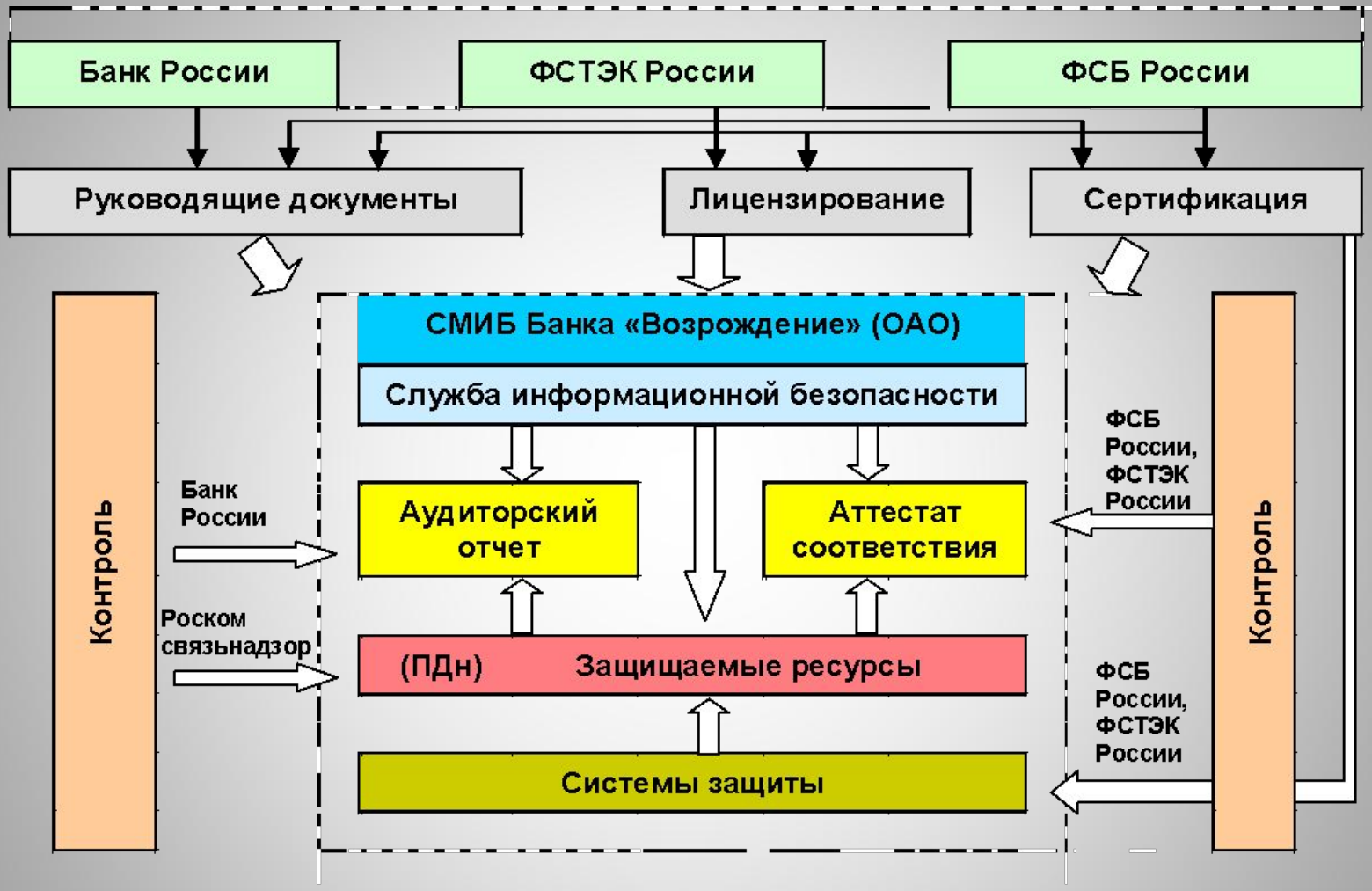
**4.4. Сведения об имуществе (имущественное положение):**

**- автотранспорт (вид владения, марка, модель, производство, год выпуска, способ получения и другие сведения, кроме указанных в соответствующем пункте раздела 3);**

**- недвижимое имущество (вид, тип, способ получения, общие характеристики, стоимость и другие сведения);**

**……**

# Система аудита и аттестации Банка «Возрождение» (ОАО)



# Основные цели аудита информационной безопасности

1. Повышение доверия к Банку как элементу банковской системы РФ.
2. Локализация уязвимых мест в системе защиты информации.
3. Анализ рисков и оценка возможного ущерба от реализации угроз безопасности информации.
4. Оценка соответствия состояния защищенности ресурсов Банка нормативным документам в области ИБ.
5. Аттестация объектов информатизации (автоматизированных систем и защищаемых помещений).
6. Определение зон ответственности и стимулирование сотрудников Банка к повышению уровня ИБ.
7. Разработка требований и рекомендаций по внедрению новых и повышению эффективности существующих механизмов ИБ.
8. Определение потребностей в ресурсах и обоснованное управление инвестициями в ИБ на основе анализа данных аудита

# Начальник Службы информационной безопасности:

1. Организует аудит центрального аппарата и филиалов Банка.
2. Обеспечивает подготовку и внедрение программы (программ), плана (планов) аудита, методик проверки и других документов.
3. Организует аттестацию объектов информатизации Банка.
4. Организует координацию работы и взаимодействие с государственными структурами (ФСБ, ФСТЭК, Банком России и др.).
5. Обеспечивает совершенствование уровня профессиональной подготовки сотрудников Службы и материально-технической базы аудита.
6. Контролирует работу системы аудита и аттестации.

# Аудиторская группа (формируется, как правило, из сотрудников отдела аудита и аттестации информационных систем СИБ Банка)

1. Проводит аудит подразделений Банка.
2. Аттестует объекты информатизации.
3. Оформляет «Аттестаты соответствия».
4. Готовит отчет по результатам проведения аудита.
5. Разрабатывает (при необходимости) предложения по устранению (недопущению) нарушений и уязвимостей.

# Содержание аудита ИБ (проверяемые области)

1. Система менеджмента информационной безопасности.
2. Идентификация, аутентификация, авторизация.
3. Управление доступом к активам.
4. Использование средств криптографической защиты информации.
5. ИБ процессинговой системы.
6. Состояние аппаратных и программных ресурсов.
7. Антивирусная защита.
8. Порядок обращения с носителями информации.
9. Обеспечение непрерывности бизнеса (деятельности) и его восстановление после прерываний.
10. Использование электронной почты и сети Интернет.
11. Порядок копирования информации ограниченного доступа.
12. Эксплуатация объектов информатизации.
13. Выполнение требований по ИБ к специализированным ПАК (ДБО, обмен ЭД с Банком России, электронные платежи и т.д.).
14. Состояние инженерно-технических систем (охранно-пожарная и тревожная сигнализация, охранное телевидение, контроль и управление доступом и т. д.).
15. Организация охраны, пропускного и внутриобъектового режима.
16. Специальная проверка защищаемых помещений.
17. Специальные исследования (при наличии требований по обязательному проведению).
18. Аттестация объектов.

# Документы по управлению программой аудита в Банке

1. Приказы, указания, распоряжения и другие руководящие документы по обеспечению ИБ Банка России, ФСТЭК России, ФСБ России и других ведомств.
2. Локальные нормативные акты Банка по обеспечению ИБ.
3. Программа и план аудита ИБ Банка.
4. Перечень сведений конфиденциального характера Банка.
5. Перечни объектов информатизации (АС и ЗП).
6. Акты классификации АС по классам защищенности.
7. Технические паспорта АС и ЗП.
8. Заявки на аттестацию объектов информатизации.
9. Методики проведения аудита ИБ и аттестации объектов информатизации Банка.
10. Технологические карты для проведения аудита.
11. План аудита проверяемого Подразделения.
12. Распоряжения (приказы) Заместителя Председателя Правления Банка, курирующего ИБ, о проведении внепланового аудита (аттестации).
13. Свидетельства аудита.
14. Протоколы аттестационных испытаний.
15. Справка по результатам аудита.
16. Аудиторские отчеты.
17. Отчеты об устранении нарушений и уязвимостей, выявленных в ходе аудита и аттестации.
18. Аттестаты соответствия АС и ЗП требованиям по ИБ.
19. Эксплуатационная документация на объекты информатизации и средства ЗИ и т.д.

# Внедренная в Банке система аудита и аттестации позволяет:

1. Существенно понизить операционные риски Банка.
2. Обеспечить безусловное выполнение требований законодательства РФ в области защиты информации.
3. Обеспечить требуемый уровень защиты:
   - персональных данных (включая данные держателей банковских карт);
   - коммерческой тайны;
   - банковской тайны.
4. Проводить аудит подразделений Банка на соответствие требованиям по ИБ международных стандартов, ФСТЭК, ФСБ и Банка России.

## Внедренная в Банке система аудита и аттестации позволяет:

5. Участвовать во внедрении и вводить в эксплуатацию системы обеспечения безопасности персональных данных в соответствии с требованиями руководящих документов.
6. Контролировать соблюдение лицензионных требований и условий видов деятельности, на которые Банком получены лицензии ФСТЭК и ФСБ России.
7. Аттестовать объекты информатизации по требованиям безопасности информации ФСТЭК России.
8. Проводить специальные исследования СВТ и специальные проверки защищаемых помещений Банка.
9. Непрерывно совершенствовать систему обеспечения ИБ Банка.

# Лекция № 9

## ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНИЗАЦИИ

**ВОПРОС 4.** Практические примеры частных политик информационной безопасности

# ВОПРОС 4. Практические примеры частных политик информационной безопасности организации

## ПОЛИТИКА КЛАССИФИКАЦИИ ИНФОРМАЦИИ

**Назначение и область действия**

**Настоящая Политика устанавливается для классификации информации в целях обеспечения адекватной защиты информационных ресурсов Организации[1].**

**Политика распространяется на владельцев информационных ресурсов, а также на всех работников Организации и третьих лиц, использующих информационные ресурсы Организации, и являются обязательными для исполнения.**

**Все исключения из настоящих правил должны быть согласованы со Службой ИБ Организации.**

**1) ИСО/МЭК27001:2005, А.7.2.**

# ВОПРОС 4. Практические примеры частных политик информационной безопасности организации

## ПОЛИТИКА КЛАССИФИКАЦИИ ИНФОРМАЦИИ

**Основные требования**

**Для обеспечения адекватного потребностям уставным целям Организации уровня защиты информационных ресурсов содержащаяся в них информация классифицируется в соответствии со степенью ее важности для Организации.**

**Информация классифицируется по следующим категориям:**

**а) I категория (повышенные требования к обеспечению конфиденциальности, целостности и/или доступности);**

**б) II категория (минимально достаточные требования);**

**в) III категория (требования по защите не предъявляются).**

## ВОПРОС 4. Практические примеры частных политик информационной безопасности организации

### ПОЛИТИКА КЛАССИФИКАЦИИ ИНФОРМАЦИИ

**К информации I категории относятся: персональные данные, коммерческая тайна, а также иная информация, в отношении которой требования к обеспечению конфиденциальности, целостности и/или доступности установлены действующим законодательством, условиями соглашений с третьими сторонами или решением владельца этой информации.**

**К информации II категории относится внутренняя информация, являющаяся собственностью Организации, не отнесенная к I и III категориям, включая любые служебные документы.**

**К информации III категории относится открытая информация и информация, предназначенная для публикации.**

# ВОПРОС 4. Практические примеры частных политик информационной безопасности организации

## ПОЛИТИКА КЛАССИФИКАЦИИ ИНФОРМАЦИИ

Информационные ресурсы, содержащие классифицированную информацию, снабжаются соответствующей маркировкой.

Конфиденциальная информация не подлежит передаче по открытым каналам передачи данных и в открытой переписке, в личных и деловых переговорах по открытым каналам связи и средствах массовой информации.

Использование персональных данных в деятельности Организации производится только с согласия их владельца. Порядок использования определяется соответствующими внутренними документами Организации.

Присвоенные информации классификационные категории подвергаются периодическому пересмотру.

# ВОПРОС 4. Практические примеры частных политик информационной безопасности организации

## ПОЛИТИКА КЛАССИФИКАЦИИ ИНФОРМАЦИИ

**Ответственность**

**Ответственность за проведение классификации информации возлагается на владельцев информационных ресурсов Организации.**

**Ответственность за соблюдение правил возлагается на всех работников Организации и третьих лиц, использующих информационные ресурсы Организации .**

**Контроль выполнения и пересмотр Политики классификации информации возлагаются на Службу информационной безопасности Организации .**

# ВОПРОС 4. Практические примеры частных политик информационной безопасности организации

## ПОЛИТИКА ИНВЕНТАРИЗАЦИИ ИНФОРМАЦИОННЫХ РЕСУРСОВ

**1. Назначение и область действия**

**Настоящая Политика устанавливается для закрепления ответственности за информационные ресурсы, определения типов подлежащих инвентаризации ресурсов и инвентаризируемых параметров в целях обеспечения и поддержания соответствующей защиты информационных ресурсов Организации[1].**

**Политика распространяются на руководителей структурных подразделений, а также на всех работников Организации и третьих лиц, использующих информационные ресурсы Организации, и являются обязательными для исполнения.**

**Все исключения из настоящей Политики должны быть согласованы со Службой ИБ Организации.**

**[1]ИСО/МЭК27001:2005, А.7.1.**

# ВОПРОС 4. Практические примеры частных политик информационной безопасности организации

## ПОЛИТИКА ИНВЕНТАРИЗАЦИИ ИНФОРМАЦИОННЫХ РЕСУРСОВ

**2. Основные требования**

**Все информационные ресурсы (базы данных и файлы данных, системная и эксплуатационная документация, нормативные, методические и организационно-распорядительные документы, планы и документация, архивная информация, контракты, договоры и другие документы Организации) подлежат обязательной инвентаризации с документированием результатов в соответствующем реестре.**

**В реестре информационных ресурсов отражаются следующие атрибуты:**

**а) наименование;**

**б) местоположение;**

**в) владелец информационного ресурса;**

**г) наивысшая категория информации, содержащейся в информационном ресурсе (категория информационного ресурса).**

**Актуальность реестра обеспечивается на основе непрерывного официального процесса его поддержки.**

# ВОПРОС 4. Практические примеры частных политик информационной безопасности организации

## ПОЛИТИКА ИНВЕНТАРИЗАЦИИ ИНФОРМАЦИОННЫХ РЕСУРСОВ

Для каждого защищаемого информационного ресурса составляется Паспорт информационного ресурса, в котором перечисляются компоненты информационных систем, обеспечивающих его функционирование:

в) услуги информационно-технического обеспечения (доступ к данным, обработка и передача данных, телефонная, видео- и конференцсвязь).

**В Паспорте информационного ресурса указываются:**

а) закрепление ролей ИБ;

б) данные, подлежащие резервному копированию;

в) способ и регулярность резервного копирования;

г) целевая точка восстановления и целевое время восстановления.

# ВОПРОС 4. Практические примеры частных политик информационной безопасности организации

## ПОЛИТИКА ИНВЕНТАРИЗАЦИИ ИНФОРМАЦИОННЫХ РЕСУРСОВ

### Ответственность

**Ответственность за проведение инвентаризации информационных ресурсов возлагается на руководителей структурных подразделений Организации.**

**Ответственность за соблюдение правил возлагается на всех работников Организации и третьих лиц, использующих информационные ресурсы Организации.**

**Контроль выполнения и пересмотр правил возлагаются на Службу ИБ Организации.**

# ВОПРОС 4. Практические примеры частных политик информационной безопасности организации

## ПОЛИТИКА УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

### 1. Назначение и область действия

Настоящая Политика устанавливается для организации процесса управления рисками ИБ в целях реализации системы управления ИБ, соответствующей требованиям стандарта ИСО/МЭК 27001:2005, противодействия прерываниям деятельности Организации и защиты критичных процессов от сбоев информационных систем или природных бедствий.

Политика распространяются на всех работников Организации, принимающих участие в информационном обеспечении и документационном сопровождении процесса управления рисками, а также в его реализации, и является обязательной для исполнения.

Все исключения из настоящих правил должны быть согласованы с Координационным советом по ИБ Организации.

ИСО/МЭК 27001:2005, 4.2.1.

ИСО/МЭК 27001:2005, A.14.1.

# ВОПРОС 4. Практические примеры частных политик информационной безопасности организации

## ПОЛИТИКА УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

### 2 Основные требования

**Методология оценки рисков должна быть определена и документально оформлена.**

**Должны быть определены критерии принятия рисков и установлен приемлемый уровень риска.**

**Должны быть идентифицированы все информационные ресурсы, подлежащие защите.**

**Идентификация ресурсов и назначение их владельцев производится согласно Политике инвентаризации информационных ресурсов (А.2) в соответствии с установленными процедурами.**

**Должны быть определены угрозы в отношении защищаемых информационных ресурсов и их уязвимости, а также возможные воздействия, которые могут привести к нарушению конфиденциальности, целостности и доступности защищаемых информационных ресурсов.**

# ВОПРОС 4. Практические примеры частных политик информационной безопасности организации

## ПОЛИТИКА УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Анализ и оценка рисков должны включать оценку возможного ущерба, который может быть нанесен в результате нарушения ИБ, оценку вероятности такого нарушения с учетом применяемых мер защиты, определение уровня рисков.**

**На этапе анализа и оценки рисков должны быть учтены, в частности, риски, являющиеся следствием участия в уставных целях Организации внешних сторон[3], а также возникающие при использовании оборудования вне территории Организации[4].**

**При анализе и оценке рисков следует учитывать результаты аудита ИБ и данные мониторинга событий ИБ.**

[3] ИСО/МЭК 27001:2005, A.6.2.1.

[4] ИСО/МЭК 27001:2005, A.9.2.5.

# ВОПРОС 4. Практические примеры частных политик информационной безопасности организации

## ПОЛИТИКА УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

При анализе и оценке рисков следует учитывать результаты аудита ИБ и данные мониторинга событий ИБ.

Для рисков, уровни которых не являются приемлемыми, должны быть выбраны варианты их обработки (снижение, избежание, перенос на сторонние организации) и определены необходимые меры по корректировке.

Меры корректировки рисков ИБ должны быть изложены в Программе управления рисками ИБ, которая рассматривается и утверждается Генеральным директором Организации.

# ВОПРОС 4. Практические примеры частных политик информационной безопасности организации

## ПОЛИТИКА УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

### 3. Ответственность

**Ответственность за организацию процесса управления рисками возлагается на Координационный совет по ИБ.**

**Ответственность за информационное обеспечение и документационное сопровождение процесса управления рисками возлагается на Службу ИБ.**

**Контроль выполнения и пересмотр правил возлагаются на Службу ИБ.**