МОСКОВСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ПРИБОРОСТРОЕНИЯ И ИНФОРМАТИКИ

КБ-2

Кафедра
«ПРИКЛАДНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ»

Дисциплина
«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Лекция 3
«ПОСТРОЕНИЕ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ОРГАНИЗАЦИИ»

Летучка

- Получить листок с вопросом
- Написать ответ на вопрос
- Время 5 минут

Основные вопросы лекции

- Основные угрозы безопасности информации.
- Стандарты безопасности (ISO/IEC 17799:2005, ISO/IEC 27001).
- Политика безопасности для организации.

Основные угрозы безопасности информации

Угроза информационной безопасности автоматизированной системы - это возможность реализации воздействия на информацию, обрабатываемую в АС, приводящего к нарушению конфиденциальности, целостности или доступности этой информации, а также возможность воздействия на компоненты АС, приводящего к их утрате, уничтожению или сбою функционирования.

Классификация угроз:

- По природе возникновения: ***естественные*** и ***искусственные***.
- По степени преднамеренности: ***случайные*** и ***преднамеренные***.
- По источникам угроз: ***природная среда, человек, санкционированные программно-аппаратные средства, несанкционированные программно-аппаратные средства***.

- По свойствам информации: ***угроза нарушения конфиденциальности, угроза нарушения целостности, угроза нарушения доступности***.

Стандарт ISO/IEC 17799:2005

Стандарт ISO/IEC 17799:2005 “Information technology – Security techniques – Code of practice for information security management” (Информационные технологии. Методы обеспечения безопасности. Практическое руководство по управлению информационной безопасностью.)

Разработан Британским институтом стандартов (BSI – British Standards Institution). Внутреннее наименование BS 7799.

Принят в России в качестве ГОСТ.

Представляет собой набор практических рекомендаций по построению комплексной корпоративной системы управления информационной безопасностью.

Сервисы безопасности (ISO/IEC 17799)

Информационная безопасность рассматривается как процесс защиты информационных активов организации от различного рода угроз, который достигается путём реализации тех или иных ***сервисов безопасности***.

Сервисы выбираются таким образом, чтобы минимизировать идентифицированные ***информационные риски***.

Тематические разделы сервисов:

1. Политика безопасности.
2. Организация информационной безопасности.
3. Управление активами.
4. Безопасность человеческих ресурсов.
5. Физическая безопасность и безопасность окружающей среды.
6. Управление телекоммуникациями и операциями.
7. Управление доступом.
8. Приобретение, разработка и внедрение информационных систем.
9. Управление инцидентами в сфере информационной безопасности.
10. Управление непрерывностью бизнеса.
11. Соответствие.

Стандарт ISO/IEC 27001:2005

Стандарт ISO/IEC 27001:2005 “Information technology – Security techniques – Information security management systems - Requirements” (Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования.)

Представляет собой расширение ISO/IEC 17799:2005, устанавливающее требования по созданию, внедрению, эксплуатации, мониторингу, анализу, поддержке и совершенствованию корпоративных систем управления информационной безопасностью (СУИБ).

Реализация СУИБ осуществляется путём внедрения четырёхфазной ***модели PDCA*** (Plan-Do-Check-Act, Планирование – Реализация – Оценка - Корректировка).

Принят в качестве ГОСТ РФ.

Модель PDCA

Предварительное условие - принятие политики безопасности, устанавливающей общие принципы обеспечения информационной безопасности в организации и задающей область действия СУИБ.

Планирование осуществляется путём проведения оценки рисков и выбора сервисов безопасности, соответствующих требованиям, идентифицированным по результатам анализа рисков.

На этапе ***реализации*** необходимо реализовать выбранные на этапе планирования сервисы безопасности и обеспечить корректную их эксплуатацию. Осуществлять обучение пользователей вопросам ИБ, тщательно контролировать и корректно отрабатывать инциденты ИБ.

Проведение ***оценки*** СУИБ предполагает проведение анализа эффективности функционирования как отдельных сервисов безопасности, так и СУИБ в целом. Отслеживание изменений сопровождается пересмотром результатов анализа рисков. Внутренний аудит СУИБ должен проводиться через запланированные интервалы времени.

Фаза ***корректировки*** должна обеспечить непрерывное совершенствование СУИБ с учётом изменяющихся рисков и требований. В ряде случаев необходим возврат к предыдущим фазам модели – например, к этапам планирования и реализации.

Документация СУИБ (ISO/IEC 27001)

- положения политики безопасности организации;
- область действия СУИБ;
- процедуры и сервисы безопасности, поддерживающие СУИБ;
- описание применяемых методов оценки рисков;
- отчёты, содержащие результаты оценки рисков;
- план управления рисками;
- методики оценки эффективности применяемых сервисов безопасности;
- декларация применимости;
- записи, подтверждающие эффективность функционирования СУИБ и предоставляющие свидетельства её соответствия положениям стандарта.

Организационно-распорядительные документы организации по ИБ

- политика информационной безопасности организации - высокоуровневый документ, описывающий основные принципы и правила, направленные на защиту информационных ресурсов организации;

- регламенты информационной безопасности, раскрывающие более подробно процедуры и методы обеспечения информационной безопасности в соответствии с основными принципами и правилами, описанными в политике;

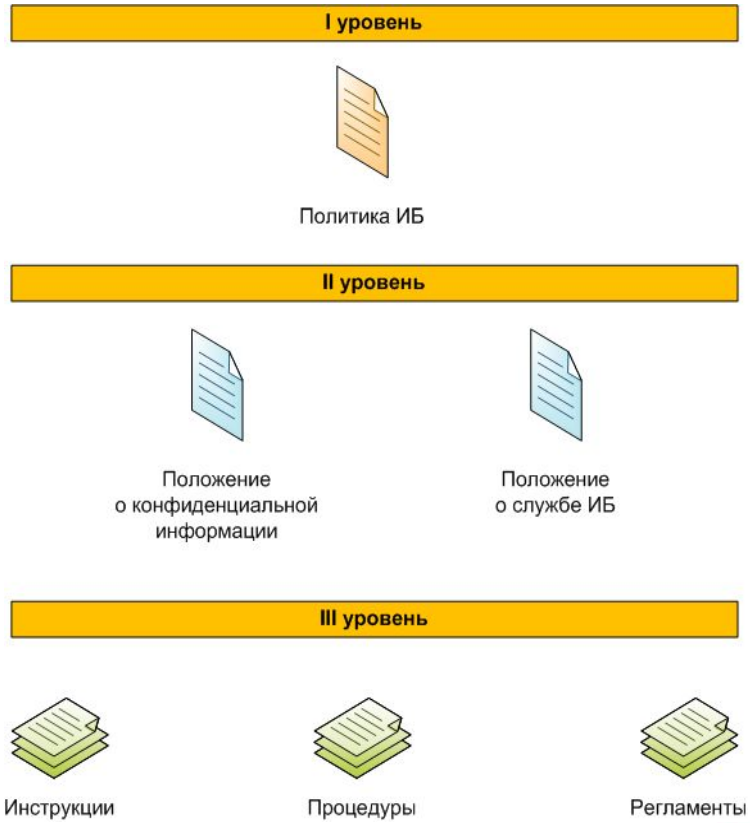
- инструкции по обеспечению информационной безопасности для должностных лиц организации с учетом требований политики и регламентов;

- прочие документы, представляющие собой отчеты, регистрационные журналы и прочие низкоуровневые руководящие документы.

Политика ИБ

Политика безопасности — это организационно-правовой и технический документ одновременно.

Любая защитная мера есть компромисс между снижением рисков и удобством работы пользователя.



Требования к содержанию ПБ

Политика безопасности — документ «верхнего» уровня, в котором должны быть указаны:

- лица, ответственные за безопасность функционирования организации;
- полномочия и ответственность отделов и служб в отношении безопасности;
- организация допуска новых сотрудников и их увольнения;
- правила разграничения доступа сотрудников к информационным ресурсам;
- организация пропускного режима, регистрации сотрудников и посетителей;
- использование программно-технических средств защиты;
- другие требования общего характера.

Пример ПБ (ОАО "Газпромбанк")

Содержание

Пример ПБ (ОАО "Газпромбанк")

1. Общие положения

1.1. Настоящая Политика разработана в соответствии с законодательством Российской Федерации и нормами права в части обеспечения информационной безопасности, требованиями нормативных актов Центрального банка Российской Федерации, федерального органа исполнительной власти, уполномоченного в области безопасности, федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, и основывается в том числе на:

- Доктрине информационной безопасности Российской Федерации (от 09.09.2000 Пр-1895);
- Стандарте Банка России СТО БР ИББС -1.0 – 2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».

1.2. Настоящая Политика является документом, доступным любому сотруднику Банка и пользователю его ресурсов, и представляет собой официально принятую руководством «Газпромбанк» (Открытое акционерное общество) (далее – Банк) систему взглядов на проблему обеспечения информационной безопасности, и устанавливает принципы построения системы управления информационной безопасностью на основе систематизированного изложения целей, процессов и процедур информационной безопасности Банка.

1.3. Руководство Банка осознает важность и необходимость развития и совершенствования мер и средств обеспечения информационной безопасности в контексте развития законодательства и норм регулирования банковской деятельности, а также развития реализуемых банковских технологий и ожиданий клиентов Банка и других заинтересованных сторон. Соблюдение требований информационной безопасности позволит создать конкурентные преимущества Банку, обеспечить его финансовую стабильность, рентабельность, соответствие правовым, регулятивным и договорным требованиям и повышение имиджа.

Пример ПБ (ОАО "Газпромбанк")

1.4. Требования информационной безопасности, которые предъявляются Банком, соответствуют интересам (целям) деятельности Банка и предназначены для снижения рисков, связанных с информационной безопасностью, до приемлемого уровня. Факторы рисков в информационной сфере Банка имеют отношение к его корпоративному управлению (менеджменту), организации и реализации бизнес-процессов, взаимоотношениям с контрагентами и клиентами, внутрихозяйственной деятельности. Факторы рисков в информационной сфере Банка составляют значимую часть операционных рисков Банка, а также имеют отношение и к иным рискам основной и управленческой деятельности Банка.

1.5. Стратегия Банка в области обеспечения информационной безопасности и защиты информации наряду с прочим включает выполнение в практической деятельности требований:

- российского законодательства в области безопасности, безопасности информационных технологий и защиты информации, безопасности персональных данных, банковской тайны и других правовых актов;
- нормативных актов федеральных органов исполнительной власти, уполномоченных в области обеспечения физической безопасности и технической защиты информации, противодействия техническим разведкам и обеспечения информационной безопасности и приватности;
- нормативных актов Банка России и стандартов Банка России по обеспечению информационной безопасности из комплекса стандартов «СТО БР ИББС»;
- нормативных актов Банка России и документов Банка России в области стандартизации «Обеспечение информационной безопасности организаций банковской системы Российской Федерации», утвержденных распоряжением Банка России от 21 июня 2010

Пример ПБ (ОАО "Газпромбанк")

1.6. Необходимые требования обеспечения информационной безопасности Банка должны неукоснительно соблюдаться персоналом Банка и другими сторонами как это определяется положениями внутренних нормативных документов Банка, а также требованиями договоров и соглашений, стороной которых является Банк.

1.7. Настоящая Политика распространяется на бизнес - процессы Банка и обязательна для применения всеми сотрудниками и руководством Банка, а также пользователями его информационных ресурсов.

1.8. Положения настоящей Политики должны быть учтены при разработке политик информационной безопасности в дочерних и аффилированных организациях.

1.9. Настоящая Политика в соответствии с рекомендациями 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», принятыми и введенными в действие распоряжением Банка России от 28 апреля 2007г. № Р-348, является корпоративным документом по ИБ **первого уровня**.

1.10. Документами, детализирующими положения корпоративной Политики применительно к одной или нескольким областям ИБ, видам и технологиям деятельности Банка, являются частные политики по обеспечению ИБ (далее – Частные политики), которые являются документами по ИБ **второго уровня**, оформляются как отдельные внутренние нормативные документы Банка, разрабатываются и согласовываются в соответствии с установленным в Банке порядком, утверждаются Куратором.

Пример ПБ (ОАО "Газпромбанк")

2. Список терминов и определений

В настоящей Политике использованы термины с соответствующими определениями согласно СТО БР ИББС–1.0–2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».

2.1. **Бизнес-процесс** – последовательность технологически связанных операций по предоставлению банковских продуктов и/или осуществлению конкретного вида обеспечивающей деятельности Банка.

2.2. **Информационная безопасность Банка** (ИБ) – в настоящей Политике состояние защищенности технологических и бизнес - процессов Банка, объединяющих в своем составе сотрудников Банка, технические и программные средства обработки информации, информацию в условиях угроз в информационной сфере.

2.3. **Информационная система Банка** – совокупность программно-аппаратных комплексов Банка, применяемых для обеспечения бизнес - процессов Банка. Банкоматы в данной совокупности не рассматриваются как устройства, сильно отличающиеся от остальных компонентов информационной системы Банка и обладающие своими уникальными свойствами с точки зрения информационной безопасности.

2.4. **Инцидент информационной безопасности** – это появление одного или нескольких нежелательных рисковых событий информационной безопасности, с которыми связана значительная вероятность нарушения конфиденциальности, целостности или доступности информационных активов и инфраструктуры и создания угрозы информационной безопасности.

2.5. **ИТ-блок** – совокупность самостоятельных структурных подразделений Банка, ответственных за развитие, эксплуатацию и сопровождение информационных банковских систем.

Пример ПБ (ОАО "Газпромбанк")

2.6. **Конфиденциальная информация** (далее – КИ) – информация, в отношении которой Банком установлен режим конфиденциальности.

2.7. **Куратор** – заместитель Председателя Правления Банка, курирующий вопросы безопасности Банка, в том числе вопросы информационной безопасности.

2.8. **Модель угроз** – описательное представление свойств или характеристик угроз безопасности информации.

2.9. **Модель нарушителя** – описательное представление опыта, знаний, доступных ресурсов возможных нарушителей ИБ, необходимых им для реализации угрозы ИБ, и возможной мотивации действий.

2.10. **Ответственное подразделение** – Служба (департамент) безопасности. Основные функции в указанной сфере – внедрение настоящей Политики, разработка, внедрение и поддержка систем обеспечения информационной безопасности.

2.11. **Пользователь информационной системы** - физическое лицо, обладающее возможностью доступа к информационной системе Банка.

Пример ПБ (ОАО "Газпромбанк")

3. Описание объекта защиты

Основными объектами защиты системы информационной безопасности в Банке являются:

- информационные ресурсы, содержащие коммерческую тайну, банковскую тайну, персональные данные физических лиц, сведения ограниченного распространения, а также открыто распространяемая информация, необходимая для работы Банка, независимо от формы и вида ее представления;
- информационные ресурсы, содержащие конфиденциальную информацию, включая персональные данные физических лиц, а также открыто распространяемая информация, необходимая для работы Банка, независимо от формы и вида ее представления;
- сотрудники Банка, являющиеся разработчиками и пользователями информационных систем Банка;
- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

Пример ПБ (ОАО "Газпромбанк")

4. Цели и задачи деятельности по обеспечению информационной безопасности

Целью деятельности по обеспечению информационной безопасности Банка является снижение угроз информационной безопасности до приемлемого для Банка уровня.

Основные задачи деятельности по обеспечению информационной безопасности Банка:

- выявление потенциальных угроз информационной безопасности и уязвимостей[1] объектов защиты;
- предотвращение инцидентов информационной безопасности;
- исключение либо минимизация выявленных угроз.

Пример ПБ (ОАО "Газпромбанк")

5. Угрозы информационной безопасности

Все множество потенциальных угроз безопасности информации делится на три класса по природе их возникновения: антропогенные, техногенные и естественные (природные)[2].

5.1. Возникновение антропогенных угроз обусловлено деятельностью человека. Среди них можно выделить угрозы, возникающие вследствие как непреднамеренных (неумышленных) действий: угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала и т.п., так и угрозы, возникающие в силу умышленных действий, связанные с корыстными, идейными или иными устремлениями людей.

К антропогенным угрозам относятся угрозы, связанные с нестабильностью и противоречивостью требований регуляторов деятельности Банка и контрольных органов, с действиями в руководстве и управлении (менеджменте), неадекватными целям и сложившимся условиям, с потребляемыми услугами, с человеческим фактором.

5.2. Возникновение техногенных угроз обусловлено воздействиями на объект угрозы объективных физических процессов техногенного характера, технического состояния окружения объекта угрозы или его самого, не обусловленных напрямую деятельностью человека.

К техногенным угрозам могут быть отнесены сбои, в том числе в работе, или разрушение систем, созданных человеком.

5.3. Возникновение естественных (природных) угроз обусловлено воздействиями на объект угрозы объективных физических процессов природного характера, стихийных природных явлений, состояний физической среды, не обусловленных напрямую деятельностью человека.

Пример ПБ (ОАО "Газпромбанк")

6. Модель нарушителя информационной безопасности

По отношению к Банку нарушители могут быть разделены на внешних и внутренних нарушителей.

6.1. Внутренние нарушители.

В качестве потенциальных внутренних нарушителей Банком рассматриваются:

- зарегистрированные пользователи информационных систем Банка;
- сотрудники Банка, не являющиеся зарегистрированными пользователями и не допущенные к ресурсам информационных систем Банка, но имеющие доступ в здания и помещения;
- персонал, обслуживающий технические средства корпоративной информационной системы Банка;
- сотрудники самостоятельных структурных подразделений Банка, задействованные в разработке и сопровождении программного обеспечения;
- сотрудники самостоятельных структурных подразделений, обеспечивающие безопасность Банка;
- руководители различных уровней.

6.2. Внешние нарушители.

В качестве потенциальных внешних нарушителей Банком рассматриваются:

- бывшие сотрудники Банка;
- представители организаций, взаимодействующих по вопросам технического обеспечения Банка;
- клиенты Банка;
- посетители зданий и помещений Банка;
- конкурирующие с Банком кредитные организации;
- члены преступных организаций, сотрудники спецслужб или лица, действующие по их заданию;
- лица, случайно или умышленно проникшие в корпоративную информационную систему Банка из внешних телекоммуникационных сетей (хакеры).

Пример ПБ (ОАО "Газпромбанк")

6.3. В отношении внутренних и внешних нарушителей принимаются следующие ограничения и предположения о характере их возможных действий:

- нарушитель скрывает свои несанкционированные действия от других сотрудников Банка;
- несанкционированные действия нарушителя могут быть следствием ошибок пользователей, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, хранения и передачи информации;
- в своей деятельности вероятный нарушитель может использовать любое имеющееся средство перехвата информации, воздействия на информацию и информационные системы, адекватные финансовые средства для подкупа персонала, шантаж, методы социальной инженерии и другие средства и методы для достижения стоящих перед ним целей;
- внешний нарушитель может действовать в сговоре с внутренним нарушителем.

Пример ПБ (ОАО "Газпромбанк")

7. Основные положения по обеспечению информационной безопасности

7.1. Требования об обеспечении информационной безопасности Банка обязательны к соблюдению всеми работниками Банка и пользователями информационных систем.

7.2. Руководство Банка приветствует и поощряет в установленном порядке деятельность работников Банка и пользователей информационных систем по обеспечению информационной безопасности.

7.3. Неисполнение или некачественное исполнение сотрудниками Банка и пользователей информационных систем обязанностей по обеспечению информационной безопасности может повлечь лишение доступа к информационным системам, а также применение к виновным административных мер воздействия, степень которых определяется установленным в Банке порядком либо требованиями действующего законодательства.

7.4. Стратегия Банка в части противодействия угрозам информационной безопасности заключается в сбалансированной реализации взаимодополняющих мер по обеспечению безопасности: от организационных мер на уровне руководства Банка, до специализированных мер информационной безопасности по каждому выявленному в Банке риску, основанных на оценке рисков информационной безопасности.

7.5. С целью поддержки заданного уровня защищенности Банк придерживается процессного подхода в построении системы менеджмента информационной безопасности.

Система менеджмента информационной безопасности Банка основывается на осуществлении следующих основных процессов (планирование, реализация и эксплуатация защитных мер, проверка (мониторинг и анализ), совершенствование) соответствующих требованиям стандарта

Пример ПБ (ОАО "Газпромбанк")

7.5. С целью поддержки заданного уровня защищенности Банк придерживается процессного подхода в построении системы менеджмента информационной безопасности.

Система менеджмента информационной безопасности Банка основывается на осуществлении следующих основных процессов (планирование, реализация и эксплуатация защитных мер, проверка (мониторинг и анализ), совершенствование) соответствующих требованиям стандарта Банка России СТО БР ИББС–1.0 и положениям международных стандартов по обеспечению информационной безопасности. Реализация этих процессов осуществляется в виде непрерывного цикла – «планирование – реализация – проверка – совершенствование – планирование – …», направленного на постоянное совершенствование деятельности по обеспечению информационной безопасности Банка и повышение ее эффективности.

На всех этапах жизненного цикла управление информационной безопасностью Банка осуществляется с соблюдением нормативных документов, определяющих процессы управления операционными рисками Банка.

7.6. При планировании мероприятий по обеспечению информационной безопасности в Банке осуществляются:

7.6.1. Определение и распределение ролей персонала Банка, связанного с обеспечением информационной безопасности (ролей информационной безопасности).

7.6.2. Оценка важности информационных активов с учетом потребности в обеспечении их свойств с точки зрения информационной безопасности.

7.6.3. Менеджмент рисков информационной безопасности, включающий:

- анализ влияния на информационную безопасность Банка применяемых в деятельности Банка технологий, а также внешних по отношению к Банку событий;
- выявление проблем обеспечения информационной безопасности, анализ причин их возникновения и прогнозирование их развития;
- определение моделей угроз информационной безопасности;
- выявление, анализ и оценка значимых для Банка угроз информационной безопасности;

Пример ПБ (ОАО "Газпромбанк")

- выявление возможных негативных последствий для Банка, наступающих в результате проявления факторов риска информационной безопасности, в том числе связанных с нарушением свойств безопасности информационных активов Банка;
- идентификацию и анализ рисковых событий информационной безопасности;
- оценку величины рисков информационной безопасности и определение среди них рисков, неприемлемых для Банка;
- обработку результатов оценки рисков информационной безопасности, базирующейся на методах управления операционными рисками, определенных в Банке;
- оптимизацию рисков информационной безопасности за счет выбора и применения защитных мер, противодействующих проявлениям факторов риска и минимизирующих возможные негативные последствия для Банка в случае наступления рисковых событий;
- оценку влияния защитных мер на цели основной деятельности Банка;
- оценку затрат на реализацию защитных мер;
- рассмотрение и оценку различных вариантов решения задач по обеспечению информационной безопасности;
- разработку планов управления рисками, предусматривающих различные защитные меры и варианты их применения, и выбор из них такого, реализация которого максимально положительно скажется на целях основной деятельности Банка и будет оптимальна с точки зрения произведенных затрат и ожидаемого эффекта;
- документальное оформление целей и задач обеспечения информационной безопасности Банка, поддержка в актуальном состоянии нормативно – методического обеспечения деятельности в сфере информационной безопасности.

Пример ПБ (ОАО "Газпромбанк")

7.7. В рамках реализации деятельности по обеспечению информационной безопасности в Банке осуществляются:

7.7.1. Менеджмент инцидентов информационной безопасности, включающий:

- сбор информации о событиях информационной безопасности;
- выявление и анализ инцидентов информационной безопасности;
- расследование инцидентов информационной безопасности;
- оперативное реагирование на инцидент информационной безопасности;
- минимизация негативных последствий инцидентов информационной безопасности;
- оперативное доведение до руководства Банка информации по наиболее значимым инцидентам информационной безопасности и оперативное принятие решений по ним, включая регламентирование порядка реагирования на инциденты информационной безопасности;
- выполнение принятых решений по всем инцидентам информационной безопасности в установленные сроки;
- пересмотр применяемых требований, мер и механизмов по обеспечению информационной безопасности по результатам рассмотрения инцидентов информационной безопасности;
- повышение уровня знаний персонала Банка в вопросах обеспечения информационной безопасности;
- обеспечение регламентации и управления доступом к программным и программно-техническим средствам и сервисам автоматизированных систем Банка и информации, обрабатываемой в них;

Пример ПБ (ОАО "Газпромбанк")

- применение средств криптографической защиты информации;
- обеспечение бесперебойной работы автоматизированных систем и сетей связи;
- обеспечение возобновления работы автоматизированных систем и сетей связи после прерываний и нештатных ситуаций;
- применение средств защиты от вредоносных программ;
- обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных систем Банка, связанных с проектированием, разработкой, приобретением, поставкой, вводом в действие, сопровождением (сервисным обслуживанием);
- обеспечение информационной безопасности при использовании доступа в сеть Интернет и услуг электронной почты;
- контроль доступа в здания и помещения Банка.

7.7.2. Обеспечение защиты информации от утечки по техническим каналам, включающее:

- применение мер и технических средств, снижающих вероятность несанкционированного получения информации в устной форме - пассивная защита;
- применение мер и технических средств, создающих помехи при несанкционированном получении информации - активная защита;
- применение мер и технических средств, позволяющих выявлять каналы несанкционированного получения информации - поиск.

Пример ПБ (ОАО "Газпромбанк")

7.8. В целях проверки деятельности по обеспечению информационной безопасности в Банке осуществляются:

- контроль правильности реализации и эксплуатации защитных мер;
- контроль изменений конфигурации систем и подсистем Банка;
- мониторинг факторов рисков[3] и соответствующий их пересмотр;
- контроль реализации и исполнения требований сотрудниками Банка действующих внутренних нормативных документов по обеспечению информационной безопасности Банка;
- контроль деятельности сотрудников и других пользователей информационных систем Банка, направленный на выявление и предотвращение конфликтов интересов.

7.9. В целях совершенствования деятельности по обеспечению информационной безопасности в Банке осуществляется периодическое, а при необходимости оперативное, уточнение/пересмотр целей и задач обеспечения информационной безопасности (при изменениях целей и задач основной деятельности Банка).

Пример ПБ (ОАО "Газпромбанк")

8. Организационная основа деятельности по обеспечению информационной безопасности

8.1. В целях выполнения задач по обеспечению информационной безопасности Банка, в соответствии с рекомендациями международных и российских стандартов по безопасности в Банке должны быть определены следующие роли:

- **Куратор;**
- **Ответственное подразделение;**
- **Сотрудник банка.**

При необходимости могут быть определены и другие роли по информационной безопасности.

8.2. Оперативная деятельность и планирование деятельности по обеспечению информационной безопасности Банка осуществляются и координируются **Ответственным подразделением**. Задачами **Ответственного подразделения** являются:

- установление потребностей Банка в применении мер обеспечения информационной безопасности, определяемых как внутренними корпоративными требованиями, так и требованиями нормативных актов;
- соблюдение действующего федерального законодательства, нормативных актов федеральных органов исполнительной власти, уполномоченных в области обеспечения безопасности и противодействия техническим разведкам и технической защиты информации, нормативных актов Банка России и стандартов Банка России по обеспечению информационной безопасности, нормативных актов по обеспечению информационной безопасности, приватности и неразглашению, принятых регуляторами рынков, на которых представлены интересы и бизнес Банка;
- разработка и пересмотр внутренних нормативных документов по обеспечению информационной безопасности Банка, включая планы, политики, положения, регламенты, инструкции, методики, перечни сведений и иные виды внутренних нормативных документов;

Пример ПБ (ОАО "Газпромбанк")

- осуществление контроля актуальности и непротиворечивости внутренних нормативных документов (политик, планов, методик и т.д.), затрагивающих вопросы информационной безопасности Банка;
- обучение, контроль и непосредственная работа с персоналом Банка в области обеспечения информационной безопасности;
- планирование применения, участие в поставке и эксплуатации средств обеспечения информационной безопасности на объекты и системы в Банке;
- выявление и предотвращение реализации угроз информационной безопасности;
- выявление и реагирование на инциденты информационной безопасности;
- информирование в установленном порядке ответственных лиц (Департамент анализа и контроля банковских рисков) об угрозах и рисковых событиях информационной безопасности;
- прогнозирование и предупреждение инцидентов информационной безопасности;
- пресечение несанкционированных действий нарушителей информационной безопасности;
- поддержка базы инцидентов информационной безопасности, анализ, разработка оптимальных процедур реагирования на инциденты и обучение персонала;
- типизация решений по применению мер и средств обеспечения информационной безопасности и распространение типовых решений на филиалы и представительства Банка;
- обеспечение эксплуатации средств и механизмов обеспечения информационной безопасности;
- мониторинг и оценка информационной безопасности, включая оценку полноты и достаточности защитных мер и видов деятельности по обеспечению информационной безопасности Банка;

Пример ПБ (ОАО "Газпромбанк")

- контроль обеспечения информационной безопасности Банка, в том числе, и на основе информации об инцидентах информационной безопасности, результатах мониторинга, оценки и аудита информационной безопасности;
- информирование руководства Банка и руководителей его самостоятельных структурных подразделений Банка об угрозах информационной безопасности, влияющих на деятельность Банка.

8.3. **Ответственное подразделение** может создавать оперативные группы для проведения расследований инцидентов информационной безопасности, возглавляемые сотрудником **Ответственного подразделения**, и может, при наличии обоснованной необходимости по согласованию с руководителями соответствующих подразделений, привлекать для работы в них сотрудников других самостоятельных структурных подразделений Банка на основе совмещения работы в группе со своими основными должностными обязанностями.

8.4. Финансирование работ по реализации положений настоящей Политики осуществляется как в рамках целевого бюджета **Ответственного подразделения** Банка, так и в рамках бюджетов бизнес - подразделений и подразделений ИТ-блока.

8.5. Основными функциями Куратора в вопросах информационной безопасности являются:

- назначение ответственных лиц в области ИБ,
- координация и внедрение информационной безопасности в Банке.

Пример ПБ (ОАО "Газпромбанк")

8.6. Основными задачами работников Банка при выполнении возложенных на них обязанностей и в рамках их участия в оперативной деятельности по обеспечению информационной безопасности Банка являются:

- соблюдение требований информационной безопасности, устанавливаемых нормативными документами Банка;
- выявление и предотвращение реализации угроз информационной безопасности в пределах своей компетенции;
- выявление и реагирование на инциденты информационной безопасности;
- информирование в установленном порядке ответственных лиц (Департамент анализа и контроля банковских рисков) о выявленных угрозах и рисковых событиях информационной безопасности;
- прогнозирование и предупреждение инцидентов информационной безопасности в пределах своей компетенции;
- мониторинг и оценка информационной безопасности в рамках своего участка работы (рабочего места, структурного подразделения) и в пределах своей компетенции;
- информирование своего руководства и **Ответственного подразделения** о выявленной угрозе в информационной среде Банка.

Пример ПБ (ОАО "Газпромбанк")

9. Ответственность за соблюдение положений Политики

Общее руководство обеспечением информационной безопасности Банка осуществляет Куратор.

Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы системы менеджмента информационной безопасности Банка лежит на руководстве **Ответственного подразделения**.

Ответственность работников Банка за невыполнение настоящей Политики определяется соответствующими положениями, включаемыми в договоры с работниками Банка, а также положениями внутренних нормативных документов Банка.

Пример ПБ (ОАО "Газпромбанк")

10. Контроль за соблюдением положений Политики

Общий контроль состояния информационной безопасности Банка осуществляется Куратором.

Текущий контроль соблюдения настоящей Политики осуществляет **Ответственное подразделение**. Контроль осуществляется путем проведения мониторинга и менеджмента инцидентов информационной безопасности Банка, по результатам оценки информационной безопасности, а также в рамках иных контрольных мероприятий.

Департамент внутреннего контроля осуществляет контроль соблюдения настоящей Политики на основе проведения внутреннего аудита информационной безопасности.

Пример ПБ (ОАО "Газпромбанк")

11. Заключительные положения

11.1. Требования настоящей Политики могут развиваться другим внутренними нормативными документами Банка, которые дополняют и уточняют ее.

11.2. В случае изменения действующего законодательства и иных нормативных актов, а также Устава Банка настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также Уставу Банка. В этом случае **Ответственное подразделение** обязано незамедлительно инициировать внесение соответствующих изменений.

11.3. Внесение изменений в настоящую Политику осуществляется на периодической и внеплановой основе:

- периодическое внесение изменений в настоящую Политику должно осуществляться не реже одного раза в 24 месяца;
- внеплановое внесение изменений в настоящую Политику может производиться по результатам анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности используемых мер обеспечения информационной безопасности, результатам проведения внутренних аудитов информационной безопасности и других контрольных мероприятий.

11.4. Ответственным за внесение изменений в настоящую Политику является руководитель **Ответственного подразделения**.

Пример ПБ (ОАО "РАДИОТЕХНИЧЕСКИЙ ИНСТИТУТ ИМЕНИ АКАДЕМИКА А.Л. МИНЦА")

Пример ПБ (ОАО "РАДИОТЕХНИЧЕСКИЙ ИНСТИТУТ ИМЕНИ АКАДЕМИКА А.Л. МИНЦА")

Пример ПБ (ИНСТИТУТ ИМЕНИ АКАДЕМИКА А.Л. МИНЦА")

Практическое задание

Разработать политику безопасности для вымышленной организации.

Время - 2 академических часа.

Форма представления результата – письменно.

Заключение

В данной лекции были рассмотрены стандарты управления ИБ, пример политики информационной безопасности.

На практическом занятии получены навыки составления политики информационной безопасности для организации.

Политика безопасности является нормативной основой для дальнейшего применения ***средств и методов обеспечения информационной безопасности***.

Задание на СРС:
Изучение ГОСТ Р 53112-2008.

Ответы на вопросы