**Лекция 5: Порядок организации защиты персональных данных. Организационно-распорядительная документация в Республике Казахстан**

**Цель лекции:** раскрыть порядок организации защиты ПД, в том числе определение замысла защиты и оценки обстановки. Изучить перечень основных документов, необходимых для организации защиты персональных данных.

### 5.1.Общий порядок организации обеспечения безопасности персональных данных в информационных системах персональных данных

### «Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»,

### утвержденным Постановлением Правительства Республики Казахстан № 887 от 3 сентября 2013 года.

### Этот нормативный акт принят в развитие положений Закона РК «О персональных данных и их защите» и устанавливает обязательные меры по защите ПД при их обработке в ИСПДн (информационных системах персональных данных).

### Основные положения Положения №887:

### Цель документа — обеспечение конфиденциальности, целостности и доступности персональных данных в процессе их обработки в информационных системах.

### Категории угроз:

### Несанкционированный доступ;

### Утечка данных;

### Нарушение работоспособности системы;

### Вредоносное воздействие на компоненты ИСПДн.

### Классификация информационных систем:

### В зависимости от объема и характера обрабатываемых данных (например, наличие чувствительных ПД);

### Уровень защищенности выбирается в соответствии с возможными последствиями утечки.

### Меры по обеспечению безопасности ПД включают:

### Организационные (регламентирующие документы, внутренние политики, инструктаж сотрудников);

### Технические (антивирусы, межсетевые экраны, системы контроля доступа);

### Криптографические средства защиты;

### Контроль за действиями пользователей;

### Аудит и анализ защищенности.

### Ответственность за обеспечение безопасности:

### Несут владельцы, операторы и третьи лица, осуществляющие обработку ПД;

### Они обязаны назначить ответственных лиц, обеспечить обучение персонала и контроль за соблюдением режима защиты.

### Оценка защищенности ИСПДн:

### Проводится на этапе проектирования и внедрения;

### Регулярно обновляется в случае изменений в архитектуре системы или законодательстве.

### 5.2. Оценка обстановки и формирование замысла защиты персональных данных

Оценка обстановки является этапом, во многом определяющим эффективность решения задач обеспечения безопасности ПД. В ее основе лежит комплексное обследование организации и ИСПД, использующихся для обработки ПД. Прежде всего, определяется *информация*, которую необходимо защищать, производится ее *категорирование* и оценивается необходимость защиты от таких угроз, как уничтожение или хищение аппаратных средств или носителей с ПД, утечки информации по техническим каналам, от НСД и прочих рассмотренных ранее угроз.

При оценке обстановки учитывается степень ущерба в случае успешной реализации одной из угроз. Рассмотрим основные подэтапы оценки обстановки:

1. Анализ информационных ресурсов:
   * Определение состава, содержания и местонахождения ПД, подлежащих защите;
   * *Категорирование* ПД;
   * Оценка выполнения обязанностей по обеспечению безопасности ПД оператором в текущий момент времени.
2. *Анализ уязвимых* звеньев и возможных угроз безопасности ПД:
   * Оценка возможности физического доступа к ИСПД;
   * Выявление технических каналов утечки информации;
   * Анализ возможностей программно-математического воздействия на ИСПД;
   * Анализ возможностей электромагнитного воздействия на ПД.
3. Оценка ущерба от реализации угроз
   * Оценка непосредственного ущерба от реализации угроз;
   * Оценка опосредованного ущерба от реализации угроз;
4. Анализ имеющихся в распоряжении мер и средств защиты ПД:
   * от физического доступа;
   * от утечки по техническим каналам утечки информации;
   * от НСД;
   * от программно-математических воздействий;
   * от электромагнитных воздействий.

В зависимости от объекта, причинение ущерба которому, в конечном счете, вызывается неправомерными действиями с ПД, рассматриваются два вида ущерба: непосредственный и опосредованный.

**Непосредственный ущерб** связан с причинением физического, материального, финансового или морального вреда непосредственно субъекту ПД. Он возникает за счет незаконного использования (в том числе распространения) ПД или за счет несанкционированной модификации этих данных и может проявляться в виде:

* нанесения вреда здоровью субъекта ПД;
* незапланированных и (или) непроизводительных финансовых или материальных затрат субъекта;
* потери субъектом свободы действий вследствие шантажа и угроз, осуществляемых с использованием ПД;
* нарушения конституционных прав субъекта вследствие вмешательства в его личную жизнь путем осуществления контактов с ним по различным поводам без его на то согласия (например – рассылка персонифицированных рекламных предложений и т.п.).

**Опосредованный ущерб** связан с причинением вреда обществу и (или) государству вследствие нарушения нормальной деятельности экономических, политических, военных, медицинских, правоохранительных, социальных, кредитно-финансовых и иных государственных органов, органов местного самоуправления, муниципальных органов, организаций различных форм собственности за счет неправомерных действий с ПД.

Разработка замысла защиты является важным этапом построения СЗПД, в ходе которого определяются основные направления *защиты персональных данных*, и производится выбор способов защиты. К способам защиты относятся как технические средства, так и организационные меры. В качестве технических средств защиты следует использовать сертифицированные средства защиты. Основные этапы формирования замысла защиты показаны на [рисунке 5.1](https://www.intuit.ru/studies/courses/697/553/lecture/12448?page=1" \l "image.5.1).



**Рис. 5.1.**Формирование замысла защиты персональных данных

К основным вопросам управления относятся:

1. распределение функций управления доступом к данным и их обработкой между должностными лицами;
2. определение порядка изменения правил доступа к защищаемой информации;
3. определение порядка изменения правил доступа к резервируемым информационным и аппаратным ресурсам;
4. определение порядка действий должностных лиц в случае возникновения нештатных ситуаций;
5. определение порядка проведения контрольных мероприятий и действий по его результатам.

Для поддержания эффективного уровня *защиты персональных данных* необходимо своевременно решать вопросы по управлению защитой, а также основные вопросы, такие как подготовка кадров, финансирование и закупка необходимого оборудования. Только *комплексный подход* может гарантировать достаточность принятых мер *защиты персональных данных*.

1. Вопросы **для закрепления:**
2. Какие цели ставятся при организации защиты персональных данных в информационных системах?
3. Какие основные требования предъявляются к обеспечению безопасности персональных данных?
4. Перечислите этапы организации безопасности ПД в ИСПД.
5. Что включает в себя этап оценки обстановки при защите персональных данных?
6. В чём заключается замысел защиты персональных данных?
7. Какие виды ущерба различают при оценке рисков реализации угроз безопасности ПД?
8. Что понимается под непосредственным ущербом при нарушении безопасности персональных данных?
9. Приведите примеры опосредованного ущерба от несанкционированного доступа к ПД.
10. Какие организационные мероприятия применяются для физической защиты информации?
11. Какие меры предпринимаются для предотвращения несанкционированного доступа к персональным данным?
12. В чем заключается анализ уязвимых звеньев и возможных угроз при оценке обстановки?
13. Какую роль играют сертифицированные средства защиты в обеспечении безопасности ПД?
14. Каковы основные функции управления доступом к персональным данным?
15. Почему важно планировать мероприятия по защите ПД и вести соответствующую документацию?
16. Какие документы необходимы для организации эксплуатации системы защиты персональных данных?