# 

**Методические указания по выполнению лабораторной работы №1**

по дисциплине «Планирование и управление информационной безопасностью»

на тему: «ВВЕДЕНИЕ В ПРОЦЕСС КЛАССИФИКАЦИИ ИНФОРМАЦИОННЫХ РЕСУРСОВ»

Казань 2017

**Цель работы**

Сформировать у контингента обучающихся четкое представление о процессе классификации информационных ресурсов, его преимуществах и ограничениях.

**Программно-аппаратные средства**

Компьютерная лаборатория, Microsoft Word, Microsoft Visio

**Теоретический материал**

В настоящее время многие информационные ресурсы приобретают значительную ценность. Информация стала одним из важнейших ресурсов автоматизированных бизнес-процессов организации и требует надлежащей защиты.

Под информационным ресурсом понимается информационная сущность, участвующая в реализации бизнес-процессов организации (формализованных и неформализованных), неделимая с их точки зрения, имеющая определенного владельца и место размещения.

Стоимость информации, циркулирующей в автоматизированной системе, зачастую во множество раз превышает стоимость оборудования, поддерживающего процессы ее хранения и обработки. Примером такой информации может служить информация о взаимодействии с поставщиками, о планах стратегического развития компании и т.п. Несанкционированное разглашение такой информации может нанести значительный ущерб ее собственнику.

Уничтожение, блокирование или несанкционированное искажение информационных ресурсов, используемых бизнес-процессами (БП), может значительно снизить эффективность выполнения последних, привести к невозможности их выполнения, чем нанести значительный ущерб.

Например, нарушение беспрепятственного доступа к информации в системе, осуществляющей автоматизированное управление добычей газа, ставит под угрозу работоспособность данной автоматизированной системы. Искажение информации в данной системе, может привести к некорректному управлению процессом и, как следствие, к аварии.

Таким образом, многие информационные ресурсы требуют своей защиты с позиций конфиденциальности, целостности, доступности. Однако ущерб, наносимый в результате нарушения данных свойств, может быть различен, поэтому неправильно будет применять равнозначные меры защиты для различных информационных ресурсов. Использование неадекватных мер защиты может привести к тому, что информационные ресурсы либо окажутся недостаточно защищенными, либо на их защиту будут тратиться излишние средства.

Для того чтобы определить требуемые меры по защите информационного ресурса, следует вводить метрики, характеризующие его важность с точки зрения конфиденциальности, целостности и доступности. В качестве данных метрик используются категории информационных ресурсов. Назначение адекватных категорий информационным ресурсам и их поддержка в актуальном состоянии является очень важной задачей для организации. Эта задача решается в рамках процесса классификации информационных ресурсов.

Под **классификацией информационных ресурсов** понимается установка в соответствие каждому из информационных ресурсов категорий конфиденциальности, целостности и доступности, адекватных ущербу, наносимому в результате нарушения соответствующих свойств.

**Категория информационного ресурса** – это мера важности информационного ресурса, отражающая возможный ущерб, наносимый в результате нарушения его конфиденциальности, целостности или доступности.

Классификация информационных ресурсов является основой создания нормативно-методической базы для дифференцированного подхода к их защите (установки адекватного уровня защиты ресурса в соответствии с возможным ущербом). В рамках процесса классификации формируются категории всех информационных ресурсов, и поддерживается их актуальность.

Необходимо отметить, что чем более высокая категория назначена информационному ресурсу, тем больше сил и средств будет потрачено организацией на их поддержание, тем больше ограничений будет налагаться на использование данных информационных ресурсов.

Процесс классификации информационных ресурсов является одним из основных процессов при внедрении политики информационной безопасности организации. Он напрямую связан с рядом других процессов управления ИБ: управлением доступом к информационным ресурсам, управлением носителями информации, управлением непрерывностью ИТ-сервисов.

Внедрение процесса классификации требует наличия формализованных описаний бизнес-процессов в организации, либо утвержденных документов (Инструкций, Положений, Регламентов и т.д.), четко регламентирующих порядок решения пользователями информационно-управляющей системы (ИУС) функциональных задач, требующих доступа к информационным ресурсам.

**Этапы процесса классификации**

Жизненный цикл процесса классификации информационных ресурсов включает в себя несколько основных видов деятельности (рис. 1-1).



Рисунок -1 Жизненный цикл процесса классификации

На этапе инициализации работ создается Группа инвентаризации и категорирования, подготавливается календарный план, осуществляется его согласование с руководством.

На этапе инвентаризации, формируется перечень информационных ресурсов ИУС, отраженных в формализованных и неформализованных бизнес-процессах, не относящихся к служебной и государственной тайне.

На этапе категорирования информационных ресурсов устанавливаются категории, соответствующие их важности.

Жизненный цикл процесса классификации является непрерывным. Следует постоянно поддерживать актуальность перечня защищаемых информационных ресурсов путем выявления новых информационных ресурсов, а также периодического пересмотра перечня инвентаризированных информационных ресурсов, существующих категорий на предмет их актуальности.

**Ресурсы, необходимые для успешного внедрения и поддержки процесса классификации**

Для успешного внедрения и поддержки процесса классификации, организация должна выделить следующие ресурсы (рис 1-2):

1. Сотрудники – участники Группы инвентаризации и категорирования (5-6 человек), а также приглашенные эксперты, являющиеся сотрудниками ОИТ, СБ, владельцы информационных ресурсов и бизнес-процессов, их подчиненные. Численность экспертной группы составляет 8-10 человек. Требуется выделить время и согласовать временные сроки, в рамках которых будут выделяться сотрудники. При оценке временных сроков следует исходить из расчета 16 человеко-часов на классификацию 10 информационных ресурсов.
2. Помещения – для проведения совещания в рамках работ по инвентаризации и категорированию.
3. Вычислительная техника – для автоматизации деятельности по инвентаризации и категорированию информационных ресурсов.
4. Расходные материалы – для осуществления бумажного документооборота в рамках деятельности по инвентаризации и категорированию информационных ресурсов.



Рисунок 1- Ресурсы, необходимые для успешного внедрения и поддержки процесса классификации

**Документы, регламентирующие процесс классификации.**

Деятельность по классификации информационных ресурсов подчинена следующим документам (рис. 1-3):

«Положение об инвентаризации и категорировании информационных ресурсов» - основной документ, которому подчиняется процесс классификации. В данном документе дается общая информация о процессе классификации, его структуре, жизненном цикле, а также о работах, проводимых на каждой из стадии его жизненного цикла. Дается представление об информационных ресурсах, их структуре, типах, видах, категориях и форме представления.

«Положение о Группе инвентаризации и категорирования информационных ресурсов» определяет порядок создания и работы группы, ее структуру, цели, задачи, функции. Определяет права, обязанности и ответственность участников группы, взаимодействие группы с подразделениями организации и группами поддержки других процессов.

«Регламент инвентаризации и категорирования информационных ресурсов» определяет общий порядок выполнения действий по инвентаризации и категорированию информационных ресурсов, по поддержке актуальности перечня защищаемых информационных ресурсов и установленных категорий

«Инструкция по инвентаризации и категорированию информационных ресурсов» определяет детальные шаги, выполняемые участниками процесса при инвентаризации и категорировании информационных ресурсов, поддержке актуальности перечня защищаемых информационных ресурсов и установленных категорий.



Рисунок 1- Документы, определяющие процесс классификации

**Участники процесса классификации.**

Процесс классификации реализуется Группой инвентаризации и категорирования (ГИК), постоянно действующей в организации. Ее состав включает в себя 5-6 человек. Состав Группы Инвентаризации и Категорирования формируется руководителем данной группы и утверждается руководством организации.

**Руководитель ГИК**

Руководитель Группы инвентаризации и категорирования подчиняется руководству организации.

Функции, выполняемые руководителем ГИК, включают в себя следующие:

Руководитель ГИК осуществляет общее руководство и контроль деятельности Группы Инвентаризации и Категорирования, организует и планирует работы по инвентаризации и категорированию информационных ресурсов, обеспечивает их непрерывность. Он обеспечивает своевременность и качество выполнения задач, возложенных на Группу Инвентаризации и Категорирования.

Руководитель ГИК создает необходимые условия для продуктивного труда в процессе инвентаризации и категорирования, способствует повышению профессионального уровня членов группы. Консультирует участников Группы Инвентаризации и Категорирования по всем возникающим у них вопросам, относящихся к деятельности группы.

Руководитель ГИК участвует в оценке эффективности процесса классификации информационных ресурсов, формирует отчеты для руководства о ходе выполнения работ по инвентаризации и категорированию информационных ресурсов, контролирует выполнение работ по улучшению процесса классификации информационных ресурсов.

Руководитель ГИК координирует деятельность Группы Инвентаризации и Категорирования со структурными подразделениями организации.

Для эффективного выполнения своих функций, руководитель ГИК вправе:

1. Выходить от лица Группы Инвентаризации и Категорирования на руководство организации при возникновении конфликтных ситуаций.
2. Привлекать необходимых экспертов к работам по инвентаризации и категорированию информационных ресурсов.
3. Принимать решение о «заочном» участии владельца информационного ресурса в процессе категорирования.

Руководитель ГИК является ответственным за своевременность и качество решения задач, возложенных на Группу Инвентаризации и Категорирования; обеспечение непрерывности процесса классификации информационных ресурсов; назначение окончательных категорий конфиденциальности, целостности и доступности инвентаризированным информационным ресурсам; поддержку в актуальном состоянии перечня информационных ресурсов.

Более подробно права, обязанности и ответственность Руководителя ГИК представлены в «Положении об инвентаризации и категорировании информационных ресурсов»

**Члены группы инвентаризации и категорирования**

Членами ГИК являются сотрудники ОИТ и СБ. Количество членов ГИК должно составлять 4-5 человек. Члены Группы Инвентаризации и Категорирования подчиняются ее руководителю и на постоянной основе участвуют в деятельности группы.

Функции, выполняемые членами ГИК, включают в себя следующие:

Члены ГИК помогают руководителю Группы Инвентаризации и Категорирования в организации деятельности группы, консультируют приглашенных экспертов по всем возникающих у них вопросам, касающихся деятельности группы, в частности по порядку заполнения опросных листов.

Члены ГИК непосредственно взаимодействуют с экспертами, организуют совещания, проводят интервьюирование и анкетирование экспертов по вопросам, связанным с инвентаризацией и категорированием информационных ресурсов.

Совместно со специалистами ОИТ, владельцами бизнес-процессов (БП), члены ГИК выполняют инвентаризацию информационных ресурсов. При участии внешних экспертов (владельцев информационных ресурсов и сотрудников подразделений) – выполняют категорирование и пересмотр категорий инвентаризированных информационных ресурсов.

Для эффективного выполнения своих функций, члены ГИК вправе:

1. Требовать от руководителя Группы Инвентаризации и Категорирования предоставления доступа к необходимым документам (формализованным описаниям бизнес-процессов; положениям, регламентам, инструкциям, содержащим сведения об информационных ресурсах и т.д.).

2. Требовать от руководителя Группы Инвентаризации и Категорирования создания необходимых условий для продуктивного труда.

Члены ГИК являются ответственными за полноту сформированного перечня информационных ресурсов ИУС организации; правильность определения типа, вида и формы представления информационного ресурса; качество сформированных оценок категорий информационных ресурсов в составе экспертной группы.

**Внешние эксперты**

В ходе своей деятельности по инвентаризации и категорированию, ГИК создает экспертные группы, привлекая в них владельцев бизнес-процессов, специалистов ОИТ, руководителей отделов (для решения задачи инвентаризации информационных ресурсов); владельцев информационных ресурсов, сотрудников подразделений (для решения задачи категорирования инвентаризированных информационных ресурсов). Для категорирования по степени конфиденциальности информационных ресурсов, относящихся к коммерческой тайне, могут привлекаться лица из числа руководства организации. Члены экспертных групп подчиняются непосредственно руководителю Группы Инвентаризации и Категорирования.

Эксперты должны иметь адекватное представление о технологии автоматизированной обработки информации в организации, о бизнес-процессах, использующих информационные ресурсы, о типах и видах, местах размещения информационных ресурсов.

Функции, выполняемые экспертами, включают в себя следующие:

Владельцы бизнес-процессов, специалисты ОИТ, привлекаемые к инвентаризации информационных ресурсов, участвуют совместно с членами ГИК в анализе формализованных описаний бизнес-процессов на предмет выделения используемых ими информационных ресурсов.

Специалисты ОИТ, руководители подразделений (отделов) участвуют в деятельности по выделению информационных ресурсов, не включенных в формализованные описания БП, но используемые сотрудниками организации для решения функциональных задач, четко регламентированных и утвержденных в различных документах (Инструкциях, Положениях, Регламентах и т.д.).

Владельцы информационных ресурсов, специалисты ОИТ, интервьюируются членами ГИК на предмет определения типа, вида информационных ресурсов, формы их представления и места размещения.

Владельцы информационных ресурсов, сотрудники подразделений, а также при необходимости лица из числа высшего руководства организации, участвуют в категорировании инвентаризированных информационных ресурсов (отвечая на опросные листы).

Для эффективного выполнения своих функций, эксперты вправе:

1. Требовать от руководителя Группы Инвентаризации и Категорирования создания необходимых условий для продуктивного труда.
2. На период участия в деятельности ГИК освобождаться от выполнения своих прямых обязанностей.

Эксперты являются ответственными за достоверность предоставляемой информации на этапе интервьюирования, за качество сформированных ими оценок категорий информационных ресурсов.

**Выводы**

Итак, подытожим основные положения изложенного материала первого занятия:

1. Информационные ресурсы являются неотъемлемой частью существующих бизнес-процессов организации и требуют надлежащей защиты с точки зрения их конфиденциальности, целостности и доступности.
2. Под классификацией информационных ресурсовпонимается установка в соответствие каждому из них категорий конфиденциальности, целостности и доступности, адекватных ущербу, наносимому в результате нарушения соответствующих свойств. Категория информационного ресурса – это мера важности информационного ресурса, отражающая возможный ущерб, наносимый в результате нарушения его конфиденциальности, целостности или доступности.
3. Процесс классификации включает в себя этап инициализации работ, инвентаризации информационных ресурсов, отраженных в формализованных и неформализованных бизнес-процессах, этап категорирования инвентаризированных информационных ресурсов. Жизненный цикл процесса классификации является непрерывным. Следует постоянно поддерживать актуальность перечня защищаемых информационных ресурсов, периодически пересматривать категории информационных ресурсов на предмет их актуальности.
4. Деятельность по классификации информационных ресурсов подчиняется и регламентируется следующими документами: «Положением об инвентаризации и категорировании информационных ресурсов», «Положением о Группе инвентаризации и категорирования информационных ресурсов», «Регламентом инвентаризации и категорирования информационных ресурсов», «Инструкцией по инвентаризации и категорированию информационных ресурсов».
5. Участниками процесса классификации являются: Руководитель ГИК, Члены ГИК, Внешние эксперты. В экспертные группы привлекаются владельцы БП, специалисты ОИТ, руководители отделов (для решения задачи инвентаризации информационных ресурсов); владельцы информационных ресурсов, сотрудники подразделений (для решения задачи категорирования инвентаризированных информационных ресурсов). Для категорирования по степени конфиденциальности информационных ресурсов, относящихся к коммерческой тайне, могут привлекаться лица из числа руководства организации.

## Контрольные вопросы

1. Что понимается под классификацией информационных ресурсов?
2. Чем определяется категория информационного ресурса?
3. Какие требование предъявляются при внедрения классификации информационных ресурсов?
4. Какие виды деятельности включает в себя процесс классификации? Какие процессы на каждом этапе?
5. Какой жизненный цикл процесса классификации?
6. Какие необходимы ресурсы для успешного внедрения и поддержки процесса классификации
7. Какие документы регламентируют процесс классификации?
8. Кто реализует процесс классификации?
9. Какие функции возложены на руководителя ГИК?
10. Какие действия может предпринять руководитель ГИК с целью повышения эффективности процесса?
11. За что ответственен руководитель ГИК.
12. Сотрудники каких подразделений включены в ГИК?
13. Какие функции возложены на членов ГИК?
14. Какие действия могут предпринять члены ГИК с целью повышения эффективности процесса?
15. За что ответственные члены ГИК?
16. Кто может входить в состав экспертной группы и кому они подчиняются? Требования к экспертам
17. Какие функции возложены на экспертов?
18. За что ответственные члены экспертной группы?

## Задание на лабораторную работу № 1

**Название работы**

Введение в процесс классификации информационных ресурсов

**Задание (не забудьте оформить отчет)**

Задание 1. В программе Microsoft Visio по теоретическому материалу смоделировать процесс классификации информационных ресурсов, взаимодействие между его участниками, подразделениями и требованиями к каждому блоку.

Задание 2. Ответьте на контрольные вопросы.

Задание 3. Задайте свою компанию. Издайте приказ по назначению руководителя группы ГИК. Составьте календарный план и утвердите его руководителем компании. Составьте утвержденный список членов гик с указанием ФИО, должности.

## Отчет по лабораторной работе № 1

**Название работы**

Введение в процесс классификации информационных ресурсов

**Цель**

Сформировать четкое представление о процессе классификации информационных ресурсов, его выгодах и ограничениях.

**Выполнил**

Студент гр. № \_\_\_\_\_\_

ФИО \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Отчет**

1. Схема процесса классификация ресурсов с комментариями среде Microsoft Visio
2. Результаты практической части
3. Ответы на контрольные вопросы