МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ

С.П. Матыюк

МЕНЕДЖМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебно-методическое пособие по выполнению практических работ

для студентов IV курса
по специальности 10.05.02
очной формы обучения

Москва
2017

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ
БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ» (МГТУ ГА)

Кафедра основ радиотехники и защиты информации

С.П. Матыюк

МЕНЕДЖМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебно-методическое пособие
по выполнению практических работ

для студентов IV курса
по специальности 10.05.02
очной формы обучения

Москва-2017

ББК 001.8
М34

Рецензент канд. техн. наук, доц. К.Н. Матюхин

Матыюк С.П.

М34 Менеджмент информационной безопасности: учебно-методическое пособие по выполнению практических работ. – М.: МГТУ ГА, 2017. – 16 с.

Данное учебно-методическое пособие издается в соответствии с рабочей программой учебной дисциплины «Менеджмент информационной безопасности» по учебному плану для студентов IV курса специальности 10.05.02 очной формы обучения.

Рассмотрено и одобрено на заседаниях кафедры 20.10.2016 г. и методического совета 27.10.2016 г.

	Подписано в печать 03.02.2017 г.	
Печать офсетная	Формат 60х84/16	0,71 уч.-изд. л.
1,85 усл.печ.л.	Заказ № 1725/140	Тираж 50 экз.

Московский государственный технический университет ГА
125993 Москва, Кронштадтский бульвар, д.20
ООО «ИПП «ИНСОФТ»
107140, г.Москва, 3-й Красносельский переулок д.21, стр.1

ОБЩИЕ МЕТОДИЧЕСКИЕ УКАЗАНИЯ

При подготовке к практическому занятию студенты должны:

-уяснить цель и порядок проведения практического занятия;

-изучить материалы, изложенные на лекционных занятиях и в рекомендуемой литературе.

На занятии студент должен иметь конспект лекций, данное пособие и нормативную документацию.

Практическое занятие начинается с опроса студентов по знанию теоретических положений практического занятия с использованием контрольных вопросов, а также проверяется понимание решения типовых заданий.

Далее студенты решают приведенные в пособии задания с последующим обсуждением полученных результатов.

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

Основная литература.

1.1.Основы управления информационной безопасностью. Учебное пособие для вузов. А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия – Телеком, 2014.

1.2. Управление рисками информационной безопасности. Учебное пособие для вузов. Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - М.: Горячая линия – Телеком, 2014.

1.3. Технические, организационные и кадровые аспекты управления информационной безопасностью. Учебное пособие для вузов. А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия - Телеком, 2014.

Дополнительная литература.

2.1. Доктрина информационной безопасности Российской Федерации.

2.2. Сборник стандартов серии ISO/IEC 27000.

2.3. Сборник ГОСТ серии ИСО/МЭК 27000.

2.4. Онлайн – ресурс , www.ISO27000.ru

Практическое занятие №1
Нормативное обеспечение управления информационной безопасности

Цель занятия–изучение серии стандартов по управлению информационной безопасности.

Контрольные вопросы

1. Какой стандарт (серия стандартов) стал основоположником стандартизации систем управления ИБ?
2. Каковы отличительные черты серии стандартов ISO/IEC 27000?
3. В чем состоят основные различия и сходства стандартов ISO/IEC 27001 и ITU-T X.1051?
4. На основании чего может проводиться оценка эффективности СУИБ?
5. Какой из стандартов серии ISO/IEC 27000 признан каталогом “лучших” практик по ИБ?

Задание на практическое занятие

При подготовке к занятию необходимо изучить теоретические материалы и ответить на контрольные вопросы, используя литературу [1.1], с.33-83, [2.2], [2.3], и конспект лекций.

Пример рассмотрения стандарта ISO/IEC 27000:2009 – СУИБ: определения и основные принципы.

Международный стандарт ISO/IEC 27000:2009 “Information technology. Security techniques. Information security management system. Overview and vocabulary” (Информационная технология. Методы и средства обеспечения безопасности. Обзор и определения) содержит термины и определения, которые используются во всех стандартах серии 27000.

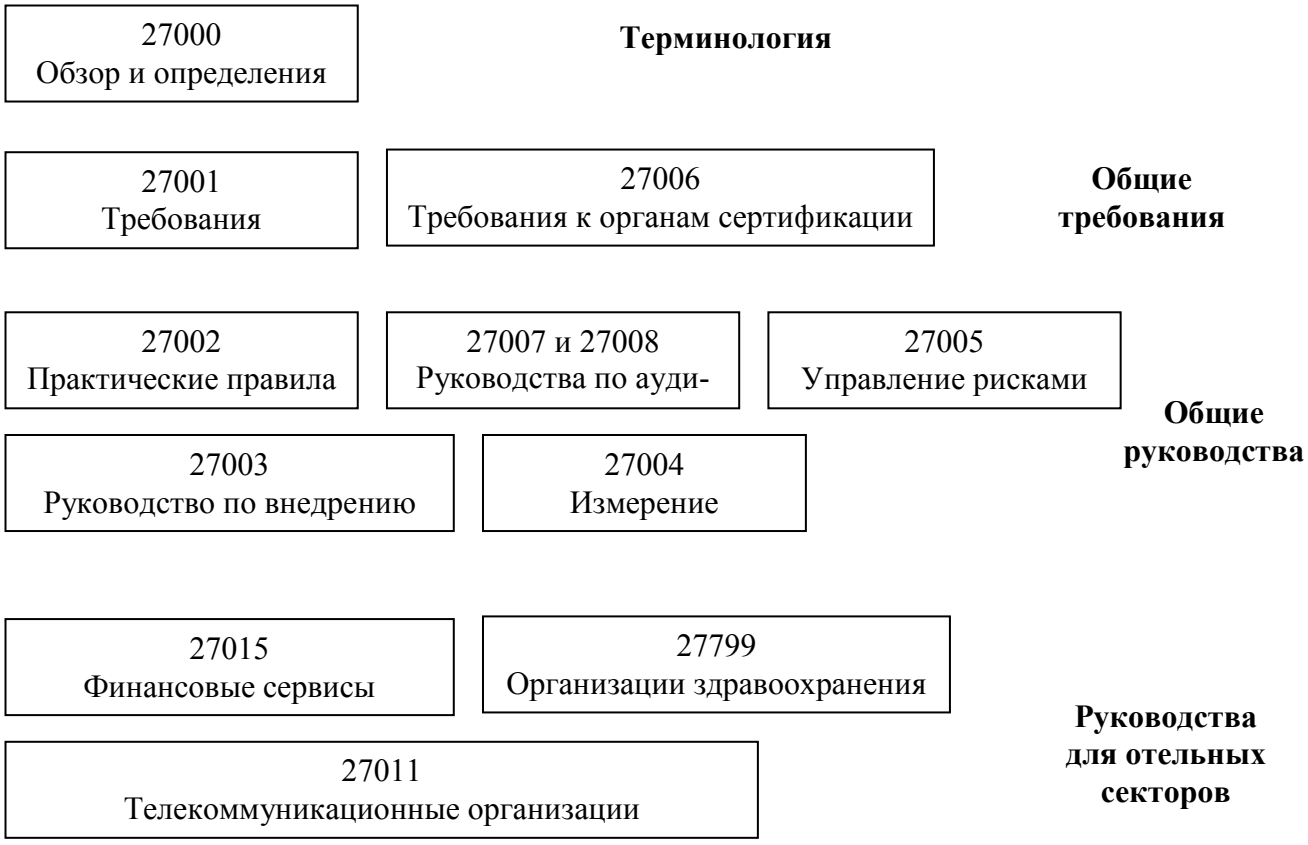

Рисунок 1

Основная цель ISO/IEC 27000:2009 – подробное описание основных принципов, концепций и определений для серии документов ISO/IEC 27000, регламентирующих все то, что связано с СУИБ.

В стандарте приведен обзор серии 27000 (рис. 1), представлено введение в СУИБ, являющееся предметом рассмотрения данной серии стандартов, определены требования к СУИБ и к их оценке соответствия, в том числе для тех, кто сертифицирует эти системы; описан цикл PDCA со всеми процессами и требованиями к ним, а также введены термины и определения, использующиеся в стандартах серии 27000.

При разработке стандарта ISO/IEC 27000:2009 были учтены основные положения следующих документов: ISO/IEC Guide 2:1996 «Стандартизация и смежная деятельность. Основные определения» и ISO/IEC Guide 73:2002 «Управление рисками. Определения. Рекомендации по использования в стандартах», а также проведена унификация со стандартами COBIT и ITIL.

В России Ассоциацией ЕВРААС и ООО «НИИ СОКБ» осенью 2011 г. была подготовлена первая редакция проекта национального стандарта ГОСТ Р ИСО/МЭК 27000-201х.

Стандарты для самостоятельного рассмотрения

Стандарт №1.Международный стандарт ISO/IEC 27001:2005 “Information technology. Security techniques. Information security management system. Requirements” (Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента ИБ. Требования). Содержит модель создания, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования СУИБ.

Рассмотреть, основанный на данном стандарте ГОСТ Р ИСО/МЭК 27001-2006 (Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента ИБ. Требования).

Стандарт №2. Международный стандарт ISO/IEC 17799:2005 (Информационные технологии. Управление ИБ. Практические правила). Включен в серию стандартов 27000, не претерпев существенных изменений.

В РФ стандарт начал применяться экспертами о области управления ИБ, и в 2005 г. был принят ГОСТ Р ИСО/МЭК 17799 – 2005.

Стандарт № 3. Международный стандарт ISO/IEC 27011:2008. (Руководство по менеджменту информационной безопасности для телекоммуникационных организаций).

Рассмотреть основанный на стандарте ГОСТ Р ИСО/МЭК 27011 – 2012. Национальный стандарт представляет дополнительные рекомендации по реализации и менеджменту информационной безопасности в телекоммуникационных организациях.

Практическое занятие №2
Нормативное обеспечение управления рисками информационной безопасности.

Цель занятия - изучение серии стандартов по управлению рисками информационной безопасности.

Контрольные вопросы

1. Почему аспекты, связанные с управлением рисками ИБ, играют больше значение в рамках системы управления ИБ?
2. В каких основных международных и национальных стандартах рассматриваются вопросы, посвященные рискам ИБ?

Задание на практическое занятие

При подготовке к занятию необходимо изучить теоретические материалы и ответить на контрольные вопросы, используя литературу[1.2],с.7-12, [2.2], [2.3]и конспект лекций.

В настоящее время имеется ряд нормативных документов, содержащих рекомендации по разработке СУРИБ. Наиболее актуальными являются:
Международный стандарт ISO/IEC 27005:2011 «Информационная технология. Методы и средства обеспечения безопасности. Управление рисками ИБ» и ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».

Британский стандарт BS 7799-3:2006 «Системы менеджмента ИБ. Руководство по управлению рисками ИБ»

Пример рассмотрения британского стандарта BS 7799-3:2006 «Системы менеджмента ИБ. Руководство по управлению рисками ИБ»

В британском стандарте BS 7799-3 описываются процессы управления рисками ИБ. BS 7799-3:2006 включает разделы по оценке рисков ИБ, их обработке, непрерывным действиям по управлению рисками ИБ и приложения с примерами активов, угроз ИБ, уязвимостей, методов оценки рисков ИБ.

Стандарт BS 7799-3:2006 придерживается самого общего понятия риска ИБ, под которым понимают комбинацию вероятности события и его последствий (стоимости компрометируемого ресурса). Управление риском ИБ сформулировано как скоординированные непрерывные действия по управлению и контролю рисков в организации. Непрерывный процесс управления делится на четыре фазы: оценка рисков ИБ, включающая анализ и вычисление рисков; обработка риска ИБ (выбор и реализация мер и средств защиты); контроль рисков ИБ путем мониторинга, тестирования, анализа механизмов безопасности и аудита ИБ системы; оптимизация рисков ИБ путем модификации и обновления правил, мер и средств защиты.

Помимо определения основных факторов риска и подходов к его оценке и обработке, стандарт также описывает взаимосвязи между рисками ИБ и други-

ми рисками организации, содержит требования и рекомендации по выбору методологии и инструментов для оценки рисков, определяет требования, предъявляемые к экспертам по оценке рисков и менеджерам, отвечающим за процессы управления рисками, содержит соображения по выбору законодательных и нормативных требований по организации ИБ и многое другое.

BS 7799-3:2006 допускает использование как количественных, так и качественных методов оценки рисков ИБ, но, к сожалению, в документе нет обоснования и рекомендаций по выбору математического и методического аппарата оценки рисков ИБ.

Отличительной чертой стандарта является использование принципа осведомленности о процессах оценки, обработки, контроля и оптимизации рисков ИБ в организации. На каждом этапе управления рисками ИБ предусмотрено информирование всех участников процесса управления ИБ, а также фиксирование событий системы управления ИБ. Стандарт перечисляет обязанности и задает требования к категории лиц, непосредственно участвующих в управлении рисками ИБ, а именно: экспертам по оценке рисков ИБ, менеджерам по безопасности, менеджерам рисков ИБ, владельцам ресурсов; руководству организации.

К основным документам по управлению рисками ИБ в BS 7799- 3:2006 отнесены описание методологии оценки рисков ИБ, отчет об оценке рисков ИБ, план обработки рисков ИБ. Кроме того, в непрерывном цикле управления рисками ИБ задействовано множество рабочей документации: реестры ресурсов, реестры рисков, декларации применимости, списки проверок, протоколы процедур и тестов, журналы безопасности, аудиторские отчеты, планы коммуникаций, инструкции, регламенты и т. п.

Следует отметить, что стандарт BS 7799-3:2006 носит концептуальный характер, что позволяет экспертам по ИБ реализовать любые методы, средства и технологии оценки, обработки и управления рисками ИБ. С другой стороны стандарт не содержат рекомендаций по выбору какого-либо аппарата оценки риска ИБ, а также по разработке мер, средств и сервисов защиты, используемых для минимизации рисков ИБ.

Стандарт для самостоятельного рассмотрения

Стандарт №1.Стандарт ISO/IEC 27005:2011 «Information technology. Security techniques. Information security risk management» (Информационная технология. Методы и средства обеспечения безопасности. Управление рисками ИБ) [3] содержит общее руководство по управлению рисками ИБ, которое может быть использовано в различных типах организаций - коммерческих, некоммерческих, государственных. ISO/IEC 27005:2011 предназначен для организации адекватного потребностям ОИБ на основе риск ориентированного подхода. Для правильного применения этого стандарта необходимо знание концепций, моделей, процессов и терминологии, введенных в ISO/IEC 27001 и 27002.

Рассмотреть ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности», идентичный ISO/IEC 27005:2011

Практическое занятие №3
Изучение методики анализа рисков информационной безопасности.

Цель занятия-закрепление теоретических знаний в области анализа рисков информационной безопасности

Контрольные вопросы

1. Какие подходы к анализу рисков выделятся в стандартах?
2. В чем состоят сходства и различия подходов базового и детального анализа рисков?
3. Какой из подходов к анализу ИБ предпочтительнее применять в небольшой организации, в которой эксплуатируются критичные системы, поддерживающие предоставление организацией услуг внешним заказчикам?
4. В какой ситуации и для какой организации целесообразно применять комбинированный подход к анализу риска ИБ?

Задание на практическое занятие

При подготовке к занятию необходимо изучить теоретические материалы и ответить на контрольные вопросы, используя литературу [1.2], с.69-89, [2.1], с.244-265,[2.3], с.80-84 и конспект лекций.

В стандартах ISO/IEC 13335-3:1998 и ГОСТ Р ИСО/МЭК 13335- 3-2007 рассматриваются четыре вида анализа рисков ИБ:

1) базовый (*baseline risk analysis)*с низкой степенью риска и выбором стандартных защитных мер;

2) неформальный (*informal risk analysis)*для активов организации, которые, как представляется, подвергаются наибольшему риску;

3) детальный (*detailed risk analysis)*с использованием формального подхода ко всем активам организации;

4) комбинированный (англ.*combined risk analysis)* — сначала высокоуровневый анализ для выбора подхода к анализу рисков ИБ с последующим проведением детального анализа для наиболее критичных выделенных систем (если прекращение их функционирования может причинить ущерб или принести убытки организации, отрицательно повлиять на ее деятельность или активы) и базового для всех остальных.

В стандартах ISO/IEC 27005:2011 и ГОСТ Р ИСО/МЭК 27005-2010 выделяются два основных типа оценки рисков ИБ и упоминается их комбинация:

5) высокоуровневая (high-level IS risk assessment);

6) детальная (detailed IS risk assessment)

Пример рассмотрения базового анализа с низкой степенью риска и выбора стандартных защитных мер

Любая организация может выработать свой базовый уровень ИБ в соответствии с собственными условиями функционирования. При данном подходе организация может применить базовый уровень ИБ для всех защищаемых активов за счет выбора стандартных защитных мер.

Преимущества использования этого варианта анализа рисков ИБ очевидны:

1) возможность обойтись минимальным количеством ресурсов при проведении анализа рисков ИБ для каждого случая принятия защитных мер и, соответственно, потратить меньше времени и усилий на выбор этих мер;

2) при применении базовых защитных мер можно принять экономически эффективное решение, поскольку те же или схожие базовые защитные меры могут быть без особых проблем применены во многих системах, если большое число систем в рамках организации функционирует в одних и тех же условиях и предъявляемые к организации ИБ требования соизмеримы.

В то же время данный подход имеет следующие недостатки:

1) если принимается слишком высокий базовый уровень ИБ, то для ряда активов уровень организации ИБ будет завышен и будут выбраны слишком дорогостоящие или излишне ограничительные средства управления;

2) если базовый уровень будет принят слишком низким, то для ряда защищаемых активов уровень организации ИБ будет недостаточен, что увеличит риск нарушения ИБ;

3) могут возникнуть трудности при внесении изменений, затрагивающих вопросы организации ИБ (как это требуется на этапах проверки и совершенствования в модели PDCA). Так, если была проведена модернизация системы, то могут возникнуть сложности при оценке способностей первоначально примененных базовых защитных мер и всей системы управления ИБ и далее оставаться достаточно эффективными.

Если все защищаемые в организации активы характеризуются низким уровнем требований по организации ИБ, то первый вариант стратегии анализа рисков ИБ может оказаться экономически эффективным. В этом случае базовый уровень ИБ выбирается таким образом, чтобы он соответствовал уровню защиты, требуемому для большинства активов. Для многих организаций для удовлетворения требований правовых и нормативных актов всегда существует необходимость использовать некоторые минимальные стандартные уровни для организации ИБ важнейшей информации. Однако в случаях, если отдельные системы организации характеризуются различной степенью критичности, разными объемами и сложностью информации, использование общих стандартов применительно ко всем системам будет логически неверным и экономически неоправданным.

Цель организации ИБ на основе базового подхода состоит в том, чтобы подобрать для организации минимальный набор защитных мер для всех или

отдельных активов. Используя базовый подход, можно применять соответствующий ему базовый уровень ИБ в организации и, кроме того, дополнительно использовать результаты детального анализа риска ИБ для организации ИБ активов с высоким уровнем риска или систем, играющих важную роль в деятельности организации. Применение базового подхода позволяет снизить инвестиции организации на исследование результатов анализа рисков ИБ.

Требуемая защита при таком подходе обеспечивается за счет использования справочных материалов (каталогов) и лучших практик по защитным мерам, в которых можно подобрать набор средств для защиты активов от наиболее часто встречающихся угроз. Базовый уровень ИБ устанавливается в соответствии с потребностями организации, при этом в проведении детальной оценки угроз ИБ, уязвимостей и рисков ИБ для систем нет необходимости.

Типичным примером области применения данного подхода является часть организации, в которой проводятся не слишком сложные бизнес-операции и зависимость которой от обработки информации и работы в сети не очень велика. Применение данного подхода возможно также в случае небольших организаций. Однако его могут применять и небольшие организации, которые имеют более сложную бизнес-среду, сильно зависят от использования ИТ, и принимают участие в обработке коммерчески важной информации.

Содержание всех этапов процесса управления рисками ИБ при базовом анализе рисков ИБ приведено в таблице 1.

Таблица 1

Этапы	Содержание этапов
Идентификация и оценка ценности активов	Составить список активов, связанных со средой деятельности, операциями и информацией, оцениваемой в пределах области применения СУИБ, и определить уровень их важности, используя простую шкалу оценки.
Идентификация угроз ИБ, уязвимостей и последствий	Идентифицировать требования по ОИБ и определить уровень всех идентифицированных требований по ОИБ, используя простую шкалу оценки.
Расчет рисков ИБ	Рассчитать риски ИБ на основе информации об активах и требованиях по ОИБ, используя простую схему расчета.
Идентификация и оценка вариантов обработки рисков ИБ	Идентифицировать подходящий вариант обработки риска ИБ для из них; документировать результаты для плана обработки рисков ИБ.
Выбор средств управления ИБ, уменьшение и принятие рисков ИБ	Для каждого из активов идентифицировать являющиеся значимыми защитные меры. Гарантировать, что выбранные меры уменьшают риски ИБ до приемлемого уровня.

Задание для самостоятельной работы

Рассмотреть оставшиеся виды анализа рисков, область их применения. Привести достоинства и недостатки каждого подхода.

Практическое занятие №4
Сравнительный анализ моделей организационного управления информационной безопасностью.

Цель занятия-изучение моделей организационного управления информационной безопасностью.

Контрольные вопросы

1. Какие два основные деятельности составляют основу управления ИБ?
2. Как можно проиллюстрировать централизацию и децентрализацию руководства ИБ?
3. Каковы четыре базовых модели организационного управления ИБ?
4. Каковы участники процесса управления ИБ в организации и их зоны ответственности?

Задание на практическое занятие

При подготовке к занятию необходимо изучить теоретические материалы и ответить на контрольные вопросы, используя литературу[1.3], с.92-108,и конспект лекций.

Главная цель организационного управления ИБ – наиболее продуктивным способом объединить существующие в организации структуры и культуру с новой деятельностью по разработке и внедрению системы обеспечения ИБ. Это достигается за счет определения и классифицирования существующей в организации структуры как соответствующей определенному типу управления ИБ.

Организационное управление ИБ определяет способ, которым ИБ передается под контроль, реализуется и управляется во всей организации. Управление может быть, как правило, централизованным или децентрализованным, но эти категории специально упрощаются для практических целей построения модели организационного управления ИБ. Причина состоит в том, что многие объекты должны применять сразу оба атрибута для достижения организации ИБ экономически эффективным образом, и, таким образом, они часто в одно и то же время централизованы и децентрализованы. Это можно смоделировать, признав, что управление ИБ заключается в двух основных видах деятельности – руководстве и администрировании, каждый из которых может быть как централизованным и децентрализованным.

Руководство относится к органу управления ИБ, имеющему соответствующие компетенции и полномочия для принятия решений по управлению ИБ в интересах организации.

Администрирование относится к органу управления, применяющему, собственно управляющему и обеспечивающему исполнение деятельности по организации ИБ в соответствии с тем, как это предписано.

Централизация указывает на наличие единого органа, который может отдельным лицом, комитетом или другой структурной единицей.

Децентрализация подразумевает наличие нескольких органов с одинаковым уровнем полномочий.

На этой основе можно разработать четыре базовых модели организационного управления ИБ.

1)Централизованное руководство/ централизованное администрирование;

2) Централизованное руководство/децентрализованное администрирование;

3)Децентрализованное руководство/ централизованное администрирование;

4)Децентрализованное руководство/ децентрализованное администрирование

Пример рассмотрения базовой модели «Централизованное руководство/централизованное администрирование»

Этот тип управления соответствует полной централизации всей деятельности в области ИБ. Одно лицо из высшего руководства отвечает за разработку политик, применяемых во всей организации. Персонал в рамках одной цепочки подчиненности выполняет все административные функции по управлению ИБ. Все подразделения организации делегируют своих представителей в комитет по управлению вопросами ИБ, что обеспечивает их достаточное влияние на принятие политических решений в области ИБ (это влияние изображено большими стрелками).

В этом случае Исполнительный директор определяет, что Управляющий директор отвечает за исполнение утвержденной программы обеспечения ИБ. Управляющий директор назначает ответственного на должность Директора службы ИБ. Комитет по управлению вопросами ИБ существует для гарантии того, чтобы каждое подразделение организации могло должным образом влиять на процесс принятия решений, поскольку в каждом подразделении возникают вопросы, связанные с ИБ, которые необходимо решать. Сопровождение ИБ и ИТ полностью разделено и осуществляется параллельно: директор службы ИБ отвечает за все вопросы ИБ, а директор службы информатизации – за использование и обслуживание ИТ. Их обязанности не пересекаются, хотя зона ответственности распространяется на одно и то же аппаратное и программное обеспечение.

В этом случае Исполнительный директор определяет, что Управляющий директор отвечает за исполнение утвержденной программы обеспечения ИБ. Управляющий директор назначает ответственного на должность Директора службы ИБ. Комитет по управлению вопросами ИБ существует для гарантии того, чтобы каждое подразделение организации могло должным образом влиять

на процесс принятия решений, поскольку в каждом подразделении возникают вопросы, связанные с ИБ, которые необходимо решать. Сопровождение ИБ и ИТ полностью разделено и осуществляется параллельно: директор службы ИБ отвечает за все вопросы ИБ, а директор службы информатизации – за использование и обслуживание ИТ. Их обязанности не пересекаются, хотя зона

ответственности распространяется на одно и то же аппаратное и программное обеспечение.

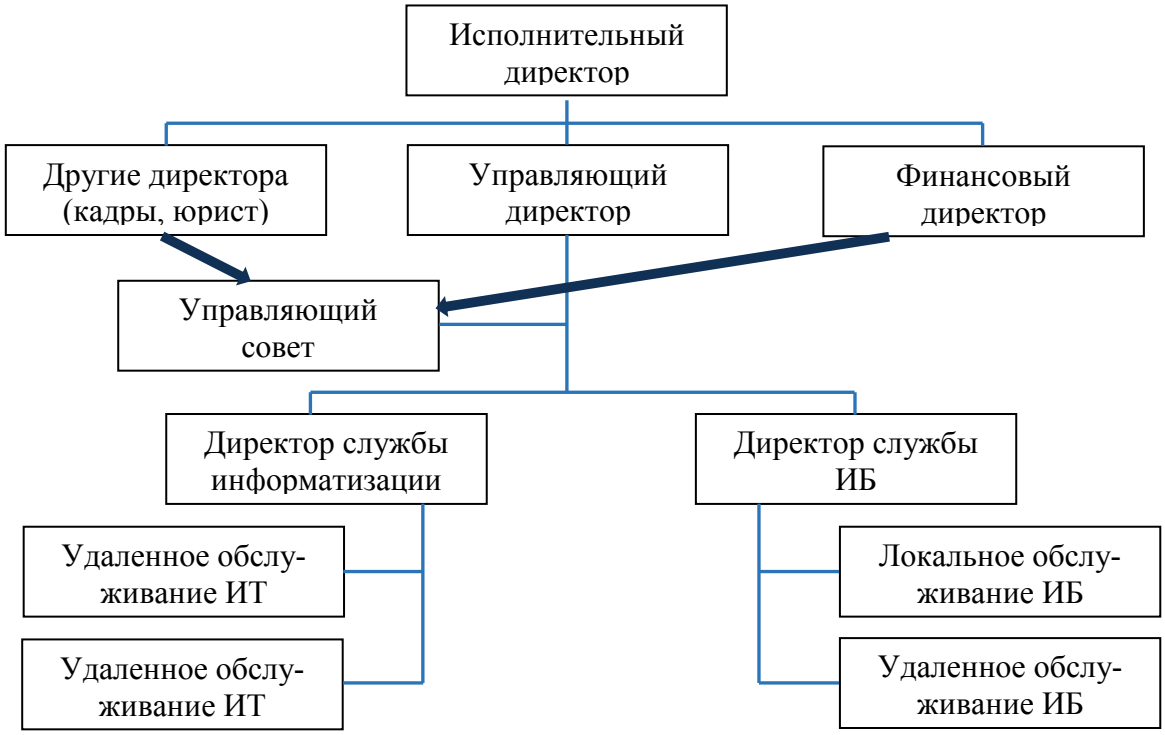

Рисунок 2

Задание для самостоятельной работы

Рассмотреть оставшиеся из базовых моделей, нарисовать структурную схему. Привести достоинства и недостатки каждого типа управления.

Практическое занятие №5
Функциональных обязанности работников подразделения информационной безопасности

Цель занятия-Изучение функциональных обязанностей работников подразделения информационной безопасности.

Контрольные вопросы

1. Перечислите полномочия службы ИБ.
2. Назовите основные функции службы ИБ.
3. Какие сотрудники должны входить в состав службы ИБ?
4. Каковы основные задачи руководителя службы ИБ?

Задание на практическое занятие

При подготовке к занятию необходимо изучить теоретические материалы и ответить на контрольные вопросы, используя литературу[1.3], с.101-130, [2.2], [2.3] и конспект лекций.

Существует два основных варианта создания службы ИБ в организации:

Системные администраторы и администраторы прикладных программ, фактически выполняющие функции службы ИБ.

Выделенные в организации работники или отдельное подразделение, основной задачей которого является организация обеспечения ИБ:

2.1) Подразделение находится в структуре службы безопасности;

2.2) Подразделение ИБ находится в ИТ – подразделении организации;

2.3) Подразделение ИБ является самостоятельным и подчиненным непосредственно высшим руководством организации.

Пример рассмотрения базовой организационно-штатной структуры службы ИБ

Количественный состав службы ИБ различен и зависит, прежде всего, от возможностей самой организации.

Типовой состав следующий:

Руководитель/ начальник или директор (заместитель директора);

Заместитель начальника службы ИБ;

Архитектор ИБ;

Аналитики по вопросам ИБ;

Риск – менеджер;

Криптоаналитик;

Криптограф;

Специалисты в области экономической разведки и промышленной контрразведки;

Ответственные за организацию конфиденциального (секретного) делопроизводства;

Ответственные за работу с персональными данными;

Сотрудники физической охраны и пропускного режима;

Администраторы средств защиты, контроля и управления;

Сотрудник службы ИБ, ответственный за решение вопросов ИБ в разрабатываемых и внедряемы АО и ПО;

Администратор ИБ;

Член группы расследования инцидентов ИБ;

Специалист по восстановлению;

Юрист и технический специалист по компьютерным преступлениям/сотрудник отдела компьютерной форенфизики;

Тестировщик ИБ;

Внутренний аудитор ИБ;

Технические специалисты;

Техник по компьютерным вирусам.

Задание для самостоятельной работы

Рассмотреть функциональные обязанности каждого из сотрудников службы ИБ. Изучить функционал Руководителя службы ИБ.

Практическое занятие №6
Компетентностные уровни специалистов в области информационной безопасности.

Цель занятия-изучение компетентностных уровней специалистов в области информационной безопасности.

Контрольные вопросы

1. По каким группам компетенций должно осуществляться обучение специалистов в области ИБ? На основании какого документа синтезирован этот список?
2. Какие обобщенные названия должностей специалистов сегодня можно встретить в зарубежных и российских организациях?
3. Как отражаются вопросы ИБ в должностных обязанностях работников организации?

Задание на практическое занятие

При подготовке к занятию необходимо изучить теоретические материалы и ответить на контрольные вопросы, используя литературу [1.3],с.122 - 150, [2.2], [2.3]и конспект лекций.

Обеспечение эффективности и результативности управления ИБ во многом определяются профессиональным уровнем персонала организации. В данном случае принципиально важным является определение требований уровню знаний, умений и навыкам к сотрудникам, занимающие определенные должности, и выполняющим определенные обязанности в области организации ИБ.

Информацию о квалификационных характеристиках профессионалов в области ИБ можно получить из следующих источников:

1) Единый квалификационный справочник должностей руководителей, специалистов и служащих, раздел «Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации».
2) Федеральные государственные образовательные стандарты (ФГОС) третьего поколения по направлению и специальностям укрупненного образовательного направления 090000 – «Информационная безопасность».
3) Нормативные документы международного уровня и иностранных государств, в которых обобщены лучшие практики в рассматриваемой области.

Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации (ОБИ) в ключевых системах

информационной инфраструктуры (КСИИ), противодействию техническим разведкам (ПТР) и технической защите информации (ТЗИ) определены в одном из разделов Единого квалификационного справочника, утвержденного Приказом Министерства здравоохранения и социального развития РФ от 22 апреля 2009 года № 205.

При этом рассмотрены только три области деятельности: ОБИ в КСИИ, ПТР и ТЗИ.

Пример рассмотрения обязанностей и квалификации Администратора по ОБИ

1) устанавливает разграничение полномочий пользователей и порядок доступа к информационным ресурсам;

2) проводит контроль выполнения работниками организации работ согласно перечня мероприятий по ОБИ;

3) осуществляет администрирование сервисами и механизмами безопасности АСУ, комплексами и средствами технической защиты информации и контроля;

4) контролирует работы по установке, модернизации и профилактике аппаратных и программных средств;

5) принимает участие в работах по внесению изменений в программно-программную конфигурацию АСУ;

6) ведет учет носителей информации, осуществляет их хранение, прием, выдачу ответственным исполнителям, контролирует правильность их использования.

Требования к квалификации: для выполнения своих должностных обязанностей администратор ОБИ должен иметь высшее профессиональное образование по специальности «Информационная безопасность» и стаж работы в должности специалиста по защите информации не менее трех лет.

Задание для самостоятельной работы

Рассмотреть квалификационные характеристики должностей руководителей и других специалистов по организации ИБ используя вышеперечисленные документы для государственных и негосударственных структур.