Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КАЛИНИНГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

А. Г. Жестовский

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Учебно-методическое пособие по выполнению практических
занятий для студентов специальности
10.05.03 Информационная безопасность
автоматизированных систем

Калининград
Издательство ФГБОУ ВО «КГТУ»
2023

УДК 519.6

Рецензент
заведующий кафедрой информационной безопасности
Института цифровых технологий ФГБОУ ВО
«Калининградский государственный технический университет»,
кандидат физико-математических наук, доцент
Н. Я. Великите

Жестовский, А. Г.

Управление информационной безопасностью: учебно-методическое пособие по выполнению практических занятий для студентов специальности 10.05.03 Информационная безопасность автоматизированных систем / А. Г. Жестовский. – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2023. – 26 с.

Учебно-методическое пособие по выполнению практических занятий по дисциплине «Управление информационной безопасностью» содержит информацию для подготовки и проведения занятий, в частности рассмотрена нормативно-правовая база, предложено рассмотрение жизненного цикла программы информационной безопасности.

Пособие подготовлено в соответствии с требованиями утвержденной рабочей программы модуля «Методы и средства обеспечения информационной безопасности автоматизированных систем» 10.05.03 Информационная безопасность автоматизированных систем.
Табл. 1, рис. 2, список лит. – 25 наименований

Учебно-методическое пособие рассмотрено и одобрено в качестве локального электронного методического материала на заседании кафедры ИБ ФГБОУ ВО «Калининградский государственный технический университет» 30 июня 2023 г., протокол № 11

Учебно-методическое пособие по изучению дисциплины рекомендовано к использованию в качестве локального электронного методического материала в учебном процессе методической комиссией ИЦТ 5 июля 2023 г., протокол № 8

УДК 519.6

ОГЛАВЛЕНИЕ

1. Введение..... 4
2. Практическое занятие № 1 Нормативное обеспечение управления информационной безопасности 8
3. Практическое занятие № 2 Нормативное обеспечение управления рисками информационной безопасности 10
4. Практическое занятие № 3 Изучение методики анализа рисков информационной безопасности 12
5. Практическое занятие № 4 Сравнительный анализ моделей организационного управления информационной безопасностью 15
6. Практическое занятие № 5 Функциональных обязанности работников подразделения информационной безопасности 17
7. Практическое занятие № 6 Компетентностные уровни специалистов в области информационной безопасности..... 18
8. Практическое занятие № 7 Оценочные стандарты в информационной безопасности 20
9. Литература..... 22
10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» 24

1. ВВЕДЕНИЕ

Информация и поддерживающие ее информационные системы и сети являются ценными производственными ресурсами организации. Их доступность, целостность и конфиденциальность могут иметь особое значение для обеспечения конкурентоспособности, движения денежной наличности, рентабельности, соответствия правовым нормам и имиджа организации. Современные организации могут столкнуться с возрастающей угрозой нарушения режима безопасности, исходящей от целого ряда источников. Информационным системам и сетям могут угрожать такие опасности, как компьютерное мошенничество, шпионаж, саботаж, вандализм, а также другие источники отказов и аварий. Появляются все новые угрозы, способные нанести ущерб организации, такие, как, широко известные компьютерные вирусы или хакеры. Предполагается, что такие угрозы информационной безопасности со временем станут более распространенными, опасными и изощренными. В то же время из-за возрастающей зависимости организаций от информационных систем и сервисов, они могут стать более уязвимыми по отношению к угрозам нарушения защиты. Распространение вычислительных сетей предоставляет новые возможности для несанкционированного доступа к компьютерным системам, а тенденция к переходу на распределенные вычислительные системы уменьшает возможности централизованного контроля информационных систем специалистами.

Защитные меры оказываются значительно более дешевыми и эффективными, если они встроены в информационные системы и сервисы на стадиях задания требований и проектирования. Чем скорее организация примет меры по защите своих информационных систем, тем более дешевыми и эффективными они будут для нее впоследствии.

Не все средства контроля применимы к каждой информационной среде; их следует использовать выборочно с учетом местных условий. Это становиться ясно из описания. Однако большинство средств контроля, описанных в данном документе, широко применяются крупными организациями с большим опытом работы, и их использование рекомендуется для всех ситуаций, разумеется, с учетом ограничений, накладываемых технологией и окружающей средой. Эти общепринятые средства контроля часто называют базовыми средствами управления безопасностью, поскольку все они в совокупности определяют базовый промышленный стандарт на поддержание режима безопасности.

При использовании некоторых из средств контроля, например, шифрование данных, могут потребоваться советы специалистов по безопасности и оценки рисков, чтобы определить, нужны ли они и каким образом их реализовать. Для обеспечения более высокого уровня защиты особенно ценных ресурсов или оказания противодействия исключительно высоким уровням угроз нарушения режима безопасности, в ряде случаев могут потребоваться другие (более сильные) средства контроля, которые выходят за рамки данных правил.

Десять ключевых средств контроля представляют собой либо обязательные требования, например, требования действующего законодательства, либо считаются основными структурными элементами информационной безопасно-

сти, например, обучение правилам безопасности. Они служат в качестве основы для организаций, приступающих к реализации средств управления информационной безопасностью.

Ключевыми являются следующие средства контроля:

- документ о политике информационной безопасности;
- распределение обязанностей по обеспечению информационной безопасности;
- обучение и подготовка персонала к поддержанию режима информационной безопасности;
- уведомление о случаях нарушения защиты;
- средства защиты от вирусов;
- процесс планирования бесперебойной работы организации;
- контроль за копированием программного обеспечения, защищенного законом об авторском праве;
- защита документации организации;
- защита данных;
- соответствие политике безопасности.

Существуют три основных группы требований к системе безопасности в любой организации.

Первая группа требований – это уникальный набор рисков нарушения безопасности, состоящий из угроз, которым подвергаются информационные ресурсы, и их слабостей и возможное воздействие этих рисков на работу организации. Однако существуют риски, требующие специального обращения, и их необходимо рассматривать с учетом их оценки в каждой конкретной организации или для каждого конкретного компонента системы.

Вторая группа требований – это набор правовых и договорных требований, которым должны удовлетворять организация, ее торговые партнеры, подрядчики и поставщики услуг; при этом возрастает необходимость стандартизации по мере распространения электронного обмена информацией по сетям между организациями. Данные практические правила могут служить надежной основой для задания общих требований этого типа.

Третья группа требований – это уникальный набор принципов, целей и требований к обработке информации, который разработан организацией для производственных целей. Важно (например, для обеспечения конкурентоспособности), чтобы в политике безопасности были отражены эти требования, и жизненно важно, чтобы реализация или отсутствие средств управления безопасностью в информационной инфраструктуре не мешали производственной деятельности организации.

Расходы на систему защиты информации необходимо сопоставить и привести в соответствие с ценностью защищаемой информации и других информационных ресурсов, подвергающихся риску, а также с ущербом, который может быть нанесен организации из-за сбоев в системе защиты.

Обычно методики анализа рисков применяются к полным информационным системам и сервисам, но этими же методиками можно воспользоваться и для отдельных компонентов системы или сервисов, если это целесообразно и

практично. Для оценки рисков необходимо систематически рассматривать следующие аспекты:

а) ущерб, который может нанести деятельности организации серьезное нарушение информационной безопасности, с учетом возможных последствий нарушения конфиденциальности, целостности и доступности информации;

б) реальная вероятность такого нарушения защиты в свете превалирующих угроз и средств контроля.

Результаты этой оценки необходимы для разработки основной линии и определения надлежащих действий и приоритетов для управления рисками нарушения информационной безопасности, а также для реализации средств контроля, рекомендуемых в настоящих практических правилах.

Оценка этих двух аспектов риска зависит от следующих факторов:

• характера производственной информации и систем;

• производственной цели, для которой информация используется;

• среды, в которой система используется и управляется;

• защиты, обеспечиваемой существующими средствами контроля.

Оценка рисков может выявить исключительно высокий риск нарушения информационной безопасности организации, требующий реализации дополнительных, более сильных средств контроля, чем те, которые рекомендуются в настоящих правилах. Использование таких средств контроля необходимо обосновать исходя из выводов, полученных в результате оценки рисков.

Опыт показывает, что перечисленные ниже факторы часто являются определяющими для успешной реализации системы информационной безопасности в организации:

а) цели безопасности и ее обеспечение должны основываться на производственных целях и требованиях, функции управления безопасностью должно взять на себя руководство организации;

б) явная поддержка и приверженность к поддержанию режима безопасности высшего руководства;

в) хорошее понимание рисков нарушения безопасности (как угроз, так и слабостей), которым подвергаются ресурсы организации, и уровня их защищенности в организации, который должен основываться на ценности и важности этих ресурсов;

г) ознакомление с системой безопасности всех руководителей и рядовых сотрудников организации;

д) предоставление исчерпывающего пособия по политике и стандартам информационной безопасности всем сотрудникам и подрядчикам.

Не существует единой оптимальной структуры защиты информации. Каждая категория пользователей или специалистов по информационным технологиям, работающих в конкретной среде, может иметь свой собственный, отличающийся от других, набор требований, проблем и приоритетов, в зависимости от функций конкретной организации и производственной или вычислительной среды.

Многие организации решают эту проблему, разрабатывая набор отдельных руководящих принципов для соответствующих групп сотрудников, чтобы

обеспечить более эффективное распространение знаний в области защиты информации. Организациям, решившим принять другую структуру (или даже разработать свои рекомендации), желательно ввести перекрестные ссылки на текст настоящих правил, чтобы их будущие деловые партнеры или аудиторы могли установить прямые связи между этим стандартом и принятыми в данной организации принципами системы защиты информации.

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.

2. ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 1. НОРМАТИВНОЕ ОБЕСПЕЧЕНИЕ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Общие сведения

Цель занятия – изучение серии стандартов по управлению информационной безопасности.

2.2. Теоретическое введение

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.

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. Также определены требования к СУИБ и к их оценке соответствия, в том числе для тех, кто сертифицирует эти системы; описан цикл PDCA, а также введены термины и определения, использующиеся в стандартах серии 27000.

Рисунок 1 – Обзор стандарта 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 использованию 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.

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?

2.3. Задание на практическое занятие

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, ив 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.

2.4. Методические указания и порядок выполнения работы

При подготовке к занятию необходимо изучить теоретические материалы

и ответить на контрольные вопросы, используя литературу [1], [7], [11], [22], и конспект лекций.

3. ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 2. НОРМАТИВНОЕ ОБЕСПЕЧЕНИЕ УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Общие сведения

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

3.2. Теоретическое введение

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 другими 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 содержит рекомендаций по выбору какого-либо аппарата оценки риска ИБ, а также по разработке мер, средств и сервисов защиты, используемых для минимизации рисков ИБ.

Контрольные вопросы

1. Почему аспекты, связанные с управлением рисками ИБ, имеют большое значение в рамках системы управления ИБ?

2. В каких основных международных и национальных стандартах рассматриваются вопросы, посвященные рискам ИБ?

3.3. Задание на практическое занятие

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.

3.4. Методические указания и порядок выполнения работы

При подготовке к занятию необходимо изучить теоретические материалы и ответить на контрольные вопросы, используя литературу [3, 4], [6], [12], [17] и конспект лекций.

4. ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 3. ИЗУЧЕНИЕ МЕТОДИКИ АНАЛИЗА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Общие сведения

Цель занятия – закрепление теоретических знаний в области анализа рисков информационной безопасности.

4.2. Теоретическое введение

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:

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

2) 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 экономиче-

ски 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- опера-

ции 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.

Таблица. Этапы процесса управления рисками ИБ

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 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.

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?

4.3. Задание на практическое занятие

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

4.4. Методические указания и порядок выполнения работы

При подготовке к занятию необходимо изучить теоретические материалы и ответить на контрольные вопросы, используя литературу [3, 4], [9], [16], [22] и конспект лекций.

5. ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 4. СРАВНИТЕЛЬНЫЙ АНАЛИЗ МОДЕЛЕЙ ОРГАНИЗАЦИОННОГО УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

5.1. Общие сведения

Цель занятия – изучение моделей организационного управления информационной безопасностью.

5.2. Теоретическое введение

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, так 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.

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. На рисунке 2 это влияние изображено стрелками.

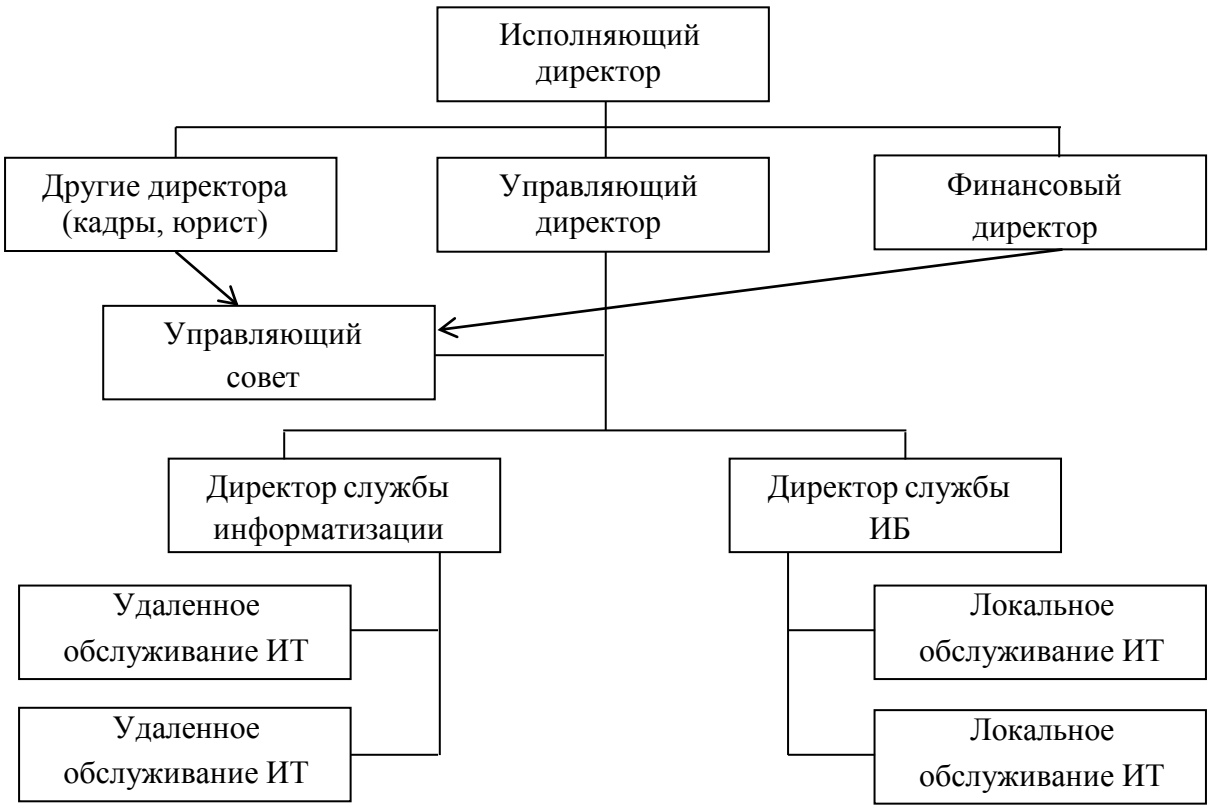

Рисунок 2 – Базовая модель «Централизованное руководство/централизованное администрирование»

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 информационной безопасности 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.

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?

5.3. Задание на практическое занятие

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

5.4. Методические указания и порядок выполнения работы

При подготовке к занятию необходимо изучить теоретические материалы и ответить на контрольные вопросы, используя литературу [1, 2, 5, 6, 10, 13, 25] и конспект лекций.

6. ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 5. ФУНКЦИОНАЛЬНЫЕ ОБЯЗАННОСТИ РАБОТНИКОВ ПОДРАЗДЕЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. Общие сведения

Цель занятия – изучение функциональных обязанностей работников подразделения информационной безопасности.

6.2. Теоретическое введение

Существует два основных варианта создания службы ИБ в организации:

1. Системные администраторы и администраторы прикладных программ, фактически выполняющие функции службы ИБ.
2. Выделенные в организации работники или отдельное подразделение, основной задачей которого является организация обеспечения ИБ:
   - Подразделение находится в структуре службы безопасности.
   - Подразделение ИБ находится в ИТ – подразделении организации.
   - 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;
− тестировщик ИБ;
− внутренний аудитор ИБ;
− технические специалисты;
− техник по компьютерным вирусам.

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?

6.3. Задание на практическое занятие

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

6.4. Методические указания и порядок выполнения работы

При подготовке к занятию необходимо изучить теоретические материалы и ответить на контрольные вопросы, используя литературу [2, 3], [11], [14], [18], [24] и конспект лекций.

7. ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 6. КОМПЕТЕНТНОСТНЫЕ УРОВНИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

7.1. Общие сведения

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

7.2. Теоретическое введение

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 перечню 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 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.

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?

7.3. Задание на практическое занятие

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

7.4. Методические указания и порядок выполнения работы

При подготовке к занятию необходимо изучить теоретические материалы и ответить на контрольные вопросы, используя литературу [2, 3], [9], [13], [15], [16], [22], [25] и конспект лекций.

8. ПРАКТИЧЕСКОЕ ЗАДАНИЕ № 7. ОЦЕНОЧНЫЕ СТАНДАРТЫ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

8.1. Общие сведения

Цель работы: Изучение вопросов оценки классификации информационных систем и средств защиты информации требованиям безопасности. Изучение подходов, методов и средств, необходимых для реализации и использования защиты информации. Закрепление теоретических знаний в области правового обеспечения информационной безопасности.

8.2. Теоретическое введение

Существуют две группы стандартов:

1 группа – оценочные стандарты:

– стандарт «Критерии оценки доверенных компьютерных систем» или разговорное название «Оранжевая книга»;

– международный стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий» или разговорное название «Общие критерии».

2 группа стандартов:

– рекомендации X.800, «Архитектура безопасности для взаимодействия открытых систем» – регламентирует методы и средства обеспечения ИБ в компьютерных сетях;

– международный стандарт ISO/IEC17799 «Практические правила управления информационной безопасностью», разработанный на основе одноименного британского стандарта BS 7799;

– международный стандарт ISO/IEC 27001:2005 «Системы менеджмента информационной безопасности. Требования»

Контрольные вопросы:

1. Что является хорошей практикой при выборе области действия СУИБ? Какие стратегии выбора области действии СУИБ существуют?
2. Какие факторы необходимо учитывать при выборе области действия СУИБ?
3. Какие параметры процессов являются наиболее значимыми при выборе области действия проектируемой СУИБ?

4. Что входит в документальное обеспечение СУИБ? Каковы этапы его жизненного цикла?

5. Какие уровни документов включает в себя иерархия документов СУИБ? Какие виды конкретных документа создаются на каждом из уровней?

6. И чем состоит основное отличие между понятиями документ и запись?

7. В чем заключается процесс управления документами и записями?

8. Какова взаимосвязь между понятиями ПолИБ и политика СУИБ?

9. Что должна включать в себя политика СУИБ?

10. На каких панах руководство организации должно продемонстрировать свою приверженность к разработке, реализации, эксплуатации, мониторингу, анализу, сопровождению и совершенствованию СУИБ?

8.3. Задание на практическое занятие

Вариант 1

Тема: Первая группа стандартов.

Изучаемые вопросы:

1. Оранжевая книга: Политика безопасности. Подотчетность, Гарантии.

2. Международный стандарт ISO/IEC 15408: Основные идеи, предположения безопасности, угрозы безопасности, политика безопасности, функциональные требования, требования доверия.

Вариант 2

Тема: Вторая группа стандартов.

Изучаемые вопросы

1. рекомендации X.800

2. ISO/IEC17799. BS 7799. Основная идея, структура стандарта. Вопросы разработки политики безопасности. Определение вероятности ущерба.

3. ISO/IEC 27001:2005: Область применения, назначение, общие положения стандарта, этапы создания СУИБ.

8.4. Методические указания и порядок выполнения работы

Практическое задание должно выполняться в следующем порядке:

1. Изучить две группы стандартов

2. Ответить на контрольные вопросы.

3. Оформить отчет, содержащий краткую информацию по контрольным вопросам.

4. Защитить практическую работу преподавателю (защита в виде опроса).

9. ЛИТЕРАТУРА

1. Громов, Ю. Ю. Информационная безопасность и защита информации: учеб. пособие / Ю. Ю. Громов, В. О. Драчев, О. Г. Иванова. – Ст. Оскол: ТНТ, 2017. – 384 с.

2. Курило, А. П. Основы управления информационной безопасностью: учеб. пособие для вузов. / А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. – Москва: Горячая линия – Телеком, 2014. – 170 с.

3. Курило, А. П. Технические, организационные и кадровые аспекты управления информационной безопасностью: учеб. пособие для вузов. / А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. – Москва: Горячая линия – Телеком, 2014. – 214 с.

4. Милославская, Н. Г. Управление рисками информационной безопасности: учеб. пособие для вузов. / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. – Москва: Горячая линия – Телеком, 2014. – 130 с.

5. Чипига, А. Ф. Информационная безопасность автоматизированных систем / А. Ф. Чипига. – Москва: Гелиос АРВ, 2017. – 336 с.

6. ГОСТ Р 53113.1-2008. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Ч. 1. Общие положения. – Москва: Стандартинформ, 2009.

7. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Методы и средства обеспечения безопасности. Практические правила управления информационной безопасностью. – Москва: Стандартинформ, 2006.

8. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – Москва: Стандартинформ, 2008.

9. ГОСТ Р ИСО/МЭК 51897-2002. Менеджмент риска. Термины и определения. – Москва: Госстандарт России, 2003.

10. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – Москва: Стандартинформ, 2011.

11. ГОСТ Р ИСО/МЭК 27006:2008. Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, обеспечивающим аудит и сертификацию систем менеджмента ИБ. – Москва: Стандартинформ, 2010.

12. ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. – Москва: Стандартинформ, 2009.

13. Жигулин, Г. П. Организационное и правовое обеспечение информационной безопасности / Г. П. Жигулин. – Санкт-Петербург: СПбНИУИТМО,

2014. – 173 с.

14. Егоров, В. П. Конфиденциальное делопроизводство [Электрон. ресурс]: учеб. пособие / В. П. Егоров, А.В. Слиньков. – Москва: Юридический институт МИИТа, 2015. – 178 с.

15. Современные методы защиты информации [Электрон. ресурс] // Camafon.ru [сайт]. [2019]. URL: https://camafon.ru/informatsionnaya-bezopasnost/metodyi-zashhityi

16. Астахова, А. В. Информационные системы в экономике и защита информации на предприятиях – участниках ВЭД: учеб. пособие / А. В. Астахова. – Санкт-Петербург: Троицкий мост, 2014.

17. Лачихина, А. Б. Подходы и методы управления информационной безопасностью в процессе управления промышленным предприятием / А. Б. Лачихина, А. А. Петраков. // Вопросы радиоэлектроники. – 2017. – № 11. – С.48–51.

18. Домуховский, Н. А. Обзор закона «О безопасности критической информационной инфраструктуры Российской Федерации» / Н. А. Домуховский. // Защита информации. Инсайд. – 2017. – № 6. – С.8–13.

19. Доктрина информационной безопасности Российской Федерации: утверждена Президентом Российской Федерации 5 декабря 2016 г. № 646.

20. Стратегия развития информационного общества в Российской Федерации: утверждена Президентом Российской Федерации 07.02.2008 № Пр-212. // Консультант Плюс. – 2014. – С. 2–7.

21. Стратегия национальной безопасности Российской Федерации до 2020 г.: указ Президента Российской Федерации от 12 мая 2009 г. № 537 (в ред. указа Президента РФ от 01.07.2014 N 483) // Консультант Плюс. – 2014. – С. 2–19.

22. Об информации, информационных технологиях и о защите и информации: федеральный закон от 27 июля 2006 г. № 149-ФЗ (в ред. федерального закона от 21.07.2014 N 222-ФЗ) // Консультант Плюс. – 2014. – С. 2–19.

23. Федеральный закон РФ от 06.04.2011 № 63-ФЗ «Об электронной подписи».

24. Трудовой кодекс Российской Федерации (Федеральный закон от 30.12.2001 № 197-ФЗ), гл. 14.

25. Указ Президента Российской Федерации от 3 декабря 2008 года № 1715 «О некоторых вопросах государственного управления в сфере связи, информационных технологий и массовых коммуникаций».

10. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ»

1. http://www.inside-zi.ru – сайт журнала «Защита информации».
2. http://www.inside-zi.ru – сайт журнала «Инсайд».
3. http://garant.ru – Гарант: законодательство РФ.
4. http://www.consultant.ru – Консультант +: Законодательство РФ.
5. http://fstec.ru/ – официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России).
6. http://www.infosait.ru – библиотека гостов, стандартов и нормативов.
7. http://avoidance.ru – правовые аспекты обеспечения информационной безопасности.
8. http://www.iqlib.ru – электронная интернет библиотека.
9. http://www.biblioclub.ru – полнотекстовая электронная библиотека.
10. http://www.elibrary.ru – научная электронная библиотека.

Локальный электронный методический материал

Александр Георгиевич Жестовский

УПРАВЛЕНИЕ ИНФОРМАЦИОНОЙ БЕЗОПАСНОСТЬЮ

Редактор С. Кондрашова

Уч.-изд. л. 2,2. Печ. л. 1,6.

Издательство федерального государственного бюджетного образовательного
учреждения высшего образования
«Калининградский государственный технический университет»
236022, Калининград, Советский проспект, 1