МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

Методические указания

для обучающихся по организации и проведению самостоятельной работы по дисциплине «**ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»**

для студентов направления подготовки **10.03.01 Информационная безопасность**
направленность (профиль) **Безопасность компьютерных систем**

Пятигорск, 2024

СОДЕРЖАНИЕ

1. Общие положения

Самостоятельная работа – планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль за работой студентов).

Самостоятельная работа студентов (СРС) в ВУЗе является важным видом учебной и научной деятельности студента. Самостоятельная работа студентов играет значительную роль в рейтинговой технологии обучения.

К основным видам самостоятельной работы студентов относятся:

- формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);
- написание докладов;
- подготовка к семинарам, практическим и лабораторным работам, их оформление;
- составление аннотированного списка статей из соответствующих журналов по отраслям знаний (педагогических, психологических, методических и др.);
- выполнение учебно-исследовательских работ, проектная деятельность;
- подготовка практических разработок и рекомендаций по решению проблемной ситуации;
- выполнение домашних заданий в виде решения отдельных задач, проведения типовых расчетов, расчетно-компьютерных и индивидуальных работ по отдельным разделам содержания дисциплин и т.д.;
- компьютерный текущий самоконтроль и контроль успеваемости на базе электронных обучающих и аттестующих тестов;
- выполнение курсовых работ (проектов) в рамках дисциплин;
- выполнение выпускной квалификационной работы и др.

Методика организации самостоятельной работы студентов зависит от структуры, характера и особенностей изучаемой дисциплины, объема часов на ее изучение, вида заданий для самостоятельной работы студентов, индивидуальных качеств студентов и условий учебной деятельности.

Процесс организации самостоятельной работы студентов включает в себя следующие этапы:

- подготовительный (определение целей, составление программы, подготовка методического обеспечения, подготовка оборудования);
- основной (реализация программы, использование приемов поиска информации, усвоения, переработки, применения, передачи знаний, фиксирование результатов, самоорганизация процесса работы);
- заключительный (оценка значимости и анализ результатов, их систематизация, оценка эффективности программы и приемов работы, выводы о направлениях оптимизации труда).

2.Цель и задачи самостоятельной работы

Ведущая цель организации и осуществления СРС совпадает с целью обучения студента – формирование универсальных компетенций.

При организации СРС важным и необходимым условием становятся формирование умения самостоятельной работы для приобретения знаний, навыков и возможности организации учебной и научной деятельности. Целью самостоятельной работы студентов является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности. Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Задачами СРС являются:

- систематизация и закрепление полученных теоретических знаний и практических умений студентов;
- углубление и расширение теоретических знаний;
- формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развитие исследовательских умений;
- использование материала, собранного и полученного в ходе самостоятельной работы и лабораторных занятий.

3.Технологическая карта самостоятельной работы студента

Коды реализуемых компетенций	Вид деятельности студентов	Средства и технологии оценки	Объем часов, в том числе (акад.)		
			СРС	Контактная работа с преподавателем	Всего
8 семестр					
ОПК-5(ИД-1.ИД-2.ИД-3), ОПК-1.1(ИД-1.ИД-2.ИД-3), ОПК-1.2(ИД-1.ИД-2.ИД-3)	Самостоятельное изучение литературы и источников	Собеседование	73,08	8,12	81,2
ОПК-5(ИД-1.ИД-2.ИД-3), ОПК-1.1(ИД-1.ИД-2.ИД-3),	Подготовка к практическим занятиям	Опрос	4,32	0,48	4,8

ОПК-1.2(ИД-1.ИД-2.ИД-3)					
ОПК-5(ИД-1.ИД-2.ИД-3), ОПК-1.1(ИД-1.ИД-2.ИД-3), ОПК-1.2(ИД-1.ИД-2.ИД-3)	Написание реферата/доклада	Доклад	9	1	10
Итого за 8 семестр			**86,4**	**9,6**	**96**

4.Порядок выполнения самостоятельной работы студентом

4.1. Методические рекомендации по работе с учебной литературой

При работе с книгой необходимо подобрать литературу, научиться правильно ее читать, вести записи. Для подбора литературы в библиотеке используются алфавитный и систематический каталоги.

Важно помнить, что рациональные навыки работы с книгой - это всегда большая экономия времени и сил.

Правильный подбор учебников рекомендуется преподавателем, читающим лекционный курс. Необходимая литература может быть также указана в методических разработках по данному курсу.

Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и вычисления (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода).

При изучении любой дисциплины большую и важную роль играет самостоятельная индивидуальная работа.

Особое внимание следует обратить на определение основных понятий курса. Студент должен подробно разбирать примеры, которые поясняют такие определения, и уметь строить аналогичные примеры самостоятельно. Нужно добиваться точного представления о том, что изучаешь. Полезно составлять опорные конспекты. При изучении материала по учебнику полезно в тетради (на специально отведенных полях) дополнять конспект лекций. Там же следует отмечать вопросы, выделенные студентом для консультации с преподавателем.

Выводы, полученные в результате изучения, рекомендуется в конспекте выделять, чтобы они при перечитывании записей лучше запоминались.

Опыт показывает, что многим студентам помогает составление листа опорных сигналов, содержащего важнейшие и наиболее часто употребляемые формулы и понятия. Такой лист помогает запомнить формулы, основные положения лекции, а также может служить постоянным справочником для студента.

Чтение научного текста является частью познавательной деятельности. Ее цель – извлечение из текста необходимой информации. От того на сколько осознанна читающим собственная внутренняя установка при обращении к печатному слову (найти нужные сведения, усвоить информацию полностью или частично, критически проанализировать материал и т.п.) во многом зависит эффективность осуществляемого действия.

Выделяют ***четыре основные установки в чтении научного текста***:

информационно-поисковый (задача – найти, выделить искомую информацию)

усваивающая (усилия читателя направлены на то, чтобы как можно полнее осознать и запомнить как сами сведения излагаемые автором, так и всю логику его рассуждений)

аналитико-критическая (читатель стремится критически осмыслить материал, проанализировав его, определив свое отношение к нему)

творческая (создает у читателя готовность в том или ином виде – как отправной пункт для своих рассуждений, как образ для действия по аналогии и т.п. – использовать суждения автора, ход его мыслей, результат наблюдения, разработанную методику, дополнить их, подвергнуть новой проверке).

Основные виды систематизированной записи прочитанного:

Аннотирование – предельно краткое связное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;

Планирование – краткая логическая организация текста, раскрывающая содержание и структуру изучаемого материала;

Тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;

Цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;

Конспектирование – краткое и последовательное изложение содержания прочитанного.

Конспект – сложный способ изложения содержания книги или статьи в логической последовательности. Конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи. Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.

Методические рекомендации по составлению конспекта:

1. Внимательно прочитайте текст. Уточните в справочной литературе непонятные слова. При записи не забудьте вынести справочные данные на поля конспекта.
2. Выделите главное, составьте план.
3. Кратко сформулируйте основные положения текста, отметьте аргументацию автора.
4. Законспектируйте материал, четко следуя пунктам плана. При конспектировании старайтесь выразить мысль своими словами. Записи следует вести четко, ясно.
5. Грамотно записывайте цитаты. Цитируя, учитывайте лаконичность, значимость мысли.

В тексте конспекта желательно приводить не только тезисные положения, но и их доказательства. При оформлении конспекта необходимо стремиться к емкости каждого предложения. Мысли автора книги следует излагать кратко, заботясь о стиле и выразительности написанного. Число дополнительных элементов конспекта должно быть логически обоснованным, записи должны распределяться в определенной последовательности, отвечающей логической структуре произведения. Для уточнения и дополнения необходимо оставлять поля.

Овладение навыками конспектирования требует от студента целеустремленности, повседневной самостоятельной работы.

4.2. Методические рекомендации по подготовке к практическим занятиям

Для того чтобы практические занятия приносили максимальную пользу, необходимо помнить, что упражнение и решение задач проводятся по вычитанному на лекциях материалу и связаны, как правило, с детальным разбором отдельных вопросов лекционного курса. Следует подчеркнуть, что только после усвоения лекционного материала с определенной точки зрения (а именно с той, с которой он излагается на лекциях) он будет закрепляться на лабораторных занятиях как в результате обсуждения и анализа лекционного материала, так и с помощью решения проблемных ситуаций, задач. При этих условиях студент не только хорошо усвоит материал, но и научится применять его на практике, а

также получит дополнительный стимул (и это очень важно) для активной проработки лекции.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы (задачи), то нужно сравнить их и выбрать самый рациональный. Полезно до начала вычислений составить краткий план решения проблемы (задачи). Решение проблемных задач или примеров следует излагать подробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями, схемами, чертежами и рисунками.

Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом. Полученный ответ следует проверить способами, вытекающими из существа данной задачи. Полезно также (если возможно) решать несколькими способами и сравнить полученные результаты. Решение задач данного типа нужно продолжать до приобретения твердых навыков в их решении.

4.3. Методические рекомендации по самопроверке знаний

После изучения определенной темы по записям в конспекте и учебнику, а также решения достаточного количества соответствующих задач на практических занятиях и самостоятельно студенту рекомендуется провести самопроверку усвоенных знаний, ответив на контрольные вопросы по изученной теме.

В случае необходимости нужно еще раз внимательно разобраться в материале.

Иногда недостаточность усвоения того или иного вопроса выясняется только при изучении дальнейшего материала. В этом случае надо вернуться назад и повторить плохо усвоенный материал. Важный критерий усвоения теоретического материала – умение отвечать на вопросы для собеседования.

Вопросы для собеседования

Базовый уровень

1. Понятие «защита информации». Раскрытие сущности защиты информации по функциональной и содержательной направленности.
2. Цели, задачи и основные объекты защиты информации.
3. Основные направления обеспечения безопасности информационных ресурсов.
4. Современные условия, определяющие значение защиты информации.
5. Основные положения теории защиты информации, связь с проблемами информатизации общества, охраны информационных ресурсов.
6. Защита прав собственника на владение и распоряжение своими информационными ресурсами.
7. Понятие и назначение системы защиты информации. Основные характеристики системы защиты информации.
8. Элементы системы защиты: правовой, организационный, инженерно-технический, программно-аппаратный, криптографический. Взаимосвязь и содержание основных элементов системы защиты.
9. Режим защиты, содержание и порядок действий, направленных на защиту информации, организация и технические мероприятия.
10. Технологических процедур учета и контроля, требований защиты организации конфиденциального документооборота.

11. Регламентация специализированных технологических процедур учета и контроля, требований защиты организации конфиденциального документооборота.

Повышенный уровень

1. Виды паразитных связей и наводок, характерные для любых радиоэлектронных средств и проводов, соединяющих их кабелей.
2. Виды угроз безопасности информации.
3. Основные принципы добывания информации.
4. Процедура идентификации, как основа процесса обнаружения объекта.
5. Методы синтеза информации.
6. Методы несанкционированного доступа к информации.
7. Основными способами привлечения сотрудников государственных и коммерческих структур, имеющих доступ к интересующей информации.
8. Способы наблюдения с использованием технических средств.

4.4. Методические рекомендации по написанию научных текстов (докладов, рефератов, эссе, научных статей и т.д.)

Перед тем, как приступить к написанию научного текста, важно разобраться, какова истинная цель вашего научного текста - это поможет вам разумно распределить свои силы и время.

Во-первых, сначала нужно определиться с идеей научного текста, а для этого необходимо научиться либо относиться к разным явлениям и фактам несколько критически (своя идея – как иная точка зрения), либо научиться увлекаться какими-то известными идеями, которые нуждаются в доработке (идея – как оптимистическая позиция и направленность на дальнейшее совершенствование уже известного). Во-вторых, научиться организовывать свое время.

Писать следует ясно и понятно, стараясь основные положения формулировать четко и недвусмысленно (чтобы и самому понятно было), а также стремясь структурировать свой текст.

Систематизация и анализ изученной литературы по проблеме исследования позволяют студенту написать работу.

Рабочий вариант текста доклада предоставляется руководителю на проверку. На основе рабочего варианта текста руководитель вместе со студентом обсуждает возможности доработки текста, его оформление.

Структура доклада:

- Введение (не более 3-4 страниц). Во введении необходимо обосновать выбор темы, ее актуальность, очертить область исследования, объект исследования, основные цели и задачи исследования.
- Основная часть состоит из 2-3 разделов. В них раскрывается суть исследуемой проблемы, проводится обзор мировой литературы и источников Интернет по предмету

исследования, в котором дается характеристика степени разработанности проблемы и авторская аналитическая оценка основных теоретических подходов к ее решению. Изложение материала не должно ограничиваться лишь описательным подходом к раскрытию выбранной темы. Оно также должно содержать собственное видение рассматриваемой проблемы и изложение собственной точки зрения на возможные пути ее решения.

- Заключение (1-2 страницы). В заключении кратко излагаются достигнутые при изучении проблемы цели, перспективы развития исследуемого вопроса
- Список использованной литературы (не меньше 10 источников), в алфавитном порядке, оформленный в соответствии с принятыми правилами. В список использованной литературы рекомендуется включать работы отечественных и зарубежных авторов, в том числе статьи, опубликованные в научных журналах в течение последних 3-х лет и ссылки на ресурсы сети Интернет.
- Приложение (при необходимости).

Требования к оформлению:

- текст с одной стороны листа;
- шрифт Times New Roman;
- кегль шрифта 14;
- межстрочное расстояние 1,5;
- поля: сверху 2,5 см, снизу – 2,5 см, слева - 3 см, справа 1,5 см;
- реферат должен быть представлен в сброшюрованном виде.

Порядок защиты доклада:

На защиту доклада отводится 5-7 минут времени, в ходе которого студент должен показать свободное владение материалом по заявленной теме. При защите доклада приветствуется использование мультимедиа-презентации.

Доклад оценивается по следующим критериям: соблюдение требований к его оформлению; необходимость и достаточность для раскрытия темы приведенной в тексте доклада информации; умение студента свободно излагать основные идеи, отраженные в докладе; способность студента понять суть задаваемых преподавателем и сокурсниками вопросов и сформулировать точные ответы на них.

Критерии оценки:

Оценка «отлично» выставляется студенту, если в докладе студент исчерпывающе, последовательно, четко и логически стройно излагает материал; свободно справляется с задачами, вопросами и другими видами применения знаний; использует для написания доклада современные научные материалы; анализирует полученную информацию; проявляет самостоятельность при написании доклада.

Оценка «хорошо» выставляется студенту, если качество выполнения доклада достаточно высокое. Студент твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопросы по теме доклада.

Оценка «удовлетворительно» выставляется студенту, если материал доклада излагается частично, но пробелы не носят существенного характера, студент допускает неточности и ошибки при защите доклада, дает недостаточно правильные формулировки, наблюдаются нарушения логической последовательности в изложении материала.

Оценка «неудовлетворительно» выставляется студенту, если он не подготовил доклад или допустил существенные ошибки. Студент неуверенно излагает материал доклада, не отвечает на вопросы преподавателя.

Описание шкалы оценивания

Максимально возможный балл за весь текущий контроль устанавливается равным 55. Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл,

выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	**100**
Хороший	**80**
Удовлетворительный	**60**
Неудовлетворительный	**0**

Темы эссе (рефератов, докладов, сообщений)

1. Системы управления физическим доступом. Специальные режимы работы
2. СУФД.
3. Особенности систем управления логическим доступом. Виды удаленного
4. доступа.
5. Защита объектов информатизации, технических средств обработки
6. информации и машинных носителей от дестабилизирующих факторов
7. окружающей среды. Классификация дестабилизирующих воздействий и
8. способов защиты от них.
9. Понятия об информационных и компьютерных преступлениях.
10. Основные причины и особенности компьютерных преступлений.
11. Уголовно наказуемые формы распространения и разглашения информации
12. Уголовно наказуемые формы фальсификации информации
13. Формы законного и незаконного собирания информации.
14. Незаконное хранение, передача, предоставление и использование
15. информации.
16. Компьютерная система как орудие преступления.
17. Компьютерная система как средство совершения преступления и хранилище
18. информации о преступной деятельности.

4.5. Методические рекомендации по подготовке к зачетам

Процедура зачета как отдельное контрольное мероприятие не проводится, оценивание знаний обучающегося происходит по результатам текущего контроля.

Зачет выставляется по результатам работы в семестре, при сдаче всех контрольных точек, предусмотренных текущим контролем успеваемости. Если по итогам семестра обучающийся имеет от 33 до 60 баллов, ему ставится отметка «зачтено». Обучающемуся, имеющему по итогам семестра менее 33 баллов, ставится отметка «не зачтено».

Количество баллов за зачет (Sзач) при различных рейтинговых баллах по дисциплине по результатам работы в семестре

Рейтинговый балл по дисциплине по результатам работы в семестре (*Rсем*)	Количество баллов за зачет (*S*зач)
50 ≤ *Rсем* ≤ 60	**40**
39 ≤ *Rсем*< 50	**35**
33 ≤ *Rсем* < 39	**27**
***Rсем*< 33**	**0**

Контроль самостоятельной работы студентов

Контроль самостоятельной работы проводится преподавателем в аудитории.

Предусмотрены следующие виды контроля: собеседование, оценка выполнения доклада и его презентации.

Подробные критерии оценивания компетенций приведены в Фонде оценочных средств для проведения текущей и промежуточной аттестации.

Список литературы для выполнения СРС

Перечень основной литературы

1. . Информационная безопасность: учебник для вузов/ В.И. Ярочкин – М.: Академический проект, 2012.
2. Семененко В.А. Информационная безопасность: учеб.пособие/ В.А. Семененко – М.: МГИУ, 2013.

Перечень дополнительной литературы

1. Информационная безопасность: учебник для вузов/ В.И. Ярочкин – М.: Академический проект, 2012.

2. Семененко В.А. Информационная безопасность: учеб.пособие/ В.А. Семененко – М.: МГИУ, 2013.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические рекомендации по выполнению лабораторных работ по дисциплине «Основы управления информационной безопасности».

2. Методические рекомендации по организации самостоятельной работы студентов по дисциплине « Основы управления информационной безопасности»

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование
5. https://urait.ru/bcode/449575 – Зенкина, С. В. Сетевая проектно-исследовательская деятельность обучающихся : учебное пособие для вузов / С. В. Зенкина, Е. К. Герасимова, О. П. Панкратова. — Москва : Издательство Юрайт, 2020. — 152 с. — (Высшее образование). — ISBN 978-5-534-13229-8. — Текст : электронный // ЭБС Юрайт [сайт].

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по выполнению практических работ
по дисциплине
«ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ для
направления подготовки 10.03.01 Информационная безопасность
направленность (профиль) **Безопасность компьютерных систем**

Пятигорск
2024 г.

Содержание

ВВЕДЕНИЕ

1. Цель и задачи изучения дисциплины

Целью освоения дисциплины «Основы управления информационной безопасностью» является формирование набора профессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01 «Информационная безопасность».

В соответствии с указанной целью при изучении данной дисциплины ставятся следующие задачи:

- анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов;
- разработка предложений по совершенствованию системы управления информационной безопасностью;
- формирование комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью.

2. Наименование практических занятий

№ Темы дисциплины	Наименование тем дисциплины, их краткое содержание	Обьем часов	Из них практическая подготовка, часов
	8 семестр		
1	**Практическая работа №1 «Основополагающие документы в области информационной безопасности»** *изучить основополагающие документы в области информационной безопасности и российские и международные, которые используются в России*	2	2
2	Практическая работа №2 **Обеспечение информационной безопасности в ведущих зарубежных странах** *ознакомление с основными принципами обеспечения информационной безопасности в ведущих зарубежных странах*	2	2
3	Практическая работа № 3 **«Требования и показатели защищенности автоматизированных средств обработки информации»** *ознакомиться с требованиями и показателями защищенности автоматизированных средств обработки информации*	4	4
4	Практическая работа № 4 **«Алгоритмы поведения вирусных и других вредоносных программ»** *Знакомство с некоторыми алгоритмами поведения вирусных и других вредоносных программ.*	2	2
5	Практическая работа № 5 ***«Процедура аутентификации пользователя на основе пароля»***	2	2

	изучение технологии аутентификации пользователя на основе пароля.		
6	Практическая работа № 6 **«Анализ рисков информационной безопасности»** *ознакомиться с алгоритмами оценки риска информационной безопасности*	4	4
7	Практическая работа № 7 **«Типовые» каналы утечки информации объектов информатизации ОВД. Условия и факторы, способствующие утечке информации ограниченного доступа. Модели возможных нарушителей»** *ознакомиться с условиями и факторами, способствующими утечке информации ограниченного доступа*	2	2
8	Практическая работа №8 **«Предварительный анализ информационной безопасности предприятия»** *Изучить деятельность определенной организации и провести предварительный анализ ее информационной безопасности*	2	2
	Практическая работа № 9 **«Построение концепции информационной безопасности предприятия»** *: знакомство с основными принципами построения концепции ИБ предприятия, с учетом особенностей его информационной инфраструктуры*	4	4
	Итого за 8семестр	24	24
	Итого	24	24

СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Практическое занятие 1. «Основополагающие документы в области информационной безопасности»

Цель работы: *изучить основополагающие документы в области информационной безопасности и российские и международные, которые используются в России*

1. Теоретическая часть

1. Рекомендации X.800.

Основополагающим документом в области защиты распределенных систем стали рекомендации X.800 — документ довольно обширный.

Основная особенность этого документа – распределение функций обеспечения ИБ по уровням OSI/

Распределение функций безопасности по уровням эталонной семиуровневой модели OSI

Функции безопасности	Уровень модели OSI						
	1	2	3	4	5	6	7
Аутентификация	-	-	+	+	-	-	+
Управление доступом	-	-	+	+	-	-	+
Конфиденциальность соединения	+	+	+	+	-	+	+
Конфиденциальность вне соединений	-	+	+	+	-	+	+
Выборочная конфиденциальность	-	-	-	-	-	+	+
Конфиденциальность трафика	+	-	+	-	-	-	+
Целостность с восстановлением	-	-	-	+	-	-	+
Целостность без восстановления	-	-	+	+	-	-	+
Избирательная целостность	-	-	-	-	-	-	+
Целостность вне соединения	-	-	+	+	-	-	+
Неотказуемость	-	-	-	-	-	-	+

Механизмы безопасности

- Шифрование;
- Электронная (цифровая) подпись;
- Механизмы управления доступом;
- Механизмы контроля целостности данных;

- Механизмы аутентификации;
- Механизмы дополнения трафика;
- Механизмы управления маршрутизацией;
- Механизмы подтверждения подлинности;

2. Критерии оценки надежных компьютерных систем ("Оранжевая книга" Министерства обороны США).

Данный труд, называемый чаще всего по цвету обложки "Оранжевой книгой", был впервые опубликован в августе 1983 года.

"Оранжевая книга" поясняет понятие безопасной системы, которая "управляет, посредством соответствующих средств, доступом к информации, так что только должным образом авторизованные лица или процессы, действующие от их имени, получают право читать, писать, создавать и удалять информацию".

Очевидно, что абсолютно безопасных систем не существует, что это абстракция. Любую систему можно "взломать", если располагать достаточно большими материальными и временными ресурсами.

Есть смысл оценивать лишь степень доверия, которое разумно оказать той или иной системе.

Надежность системы

В "Оранжевой книге" надежная система определяется как "система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа".

Степень доверия, или надежность систем, оценивается по двум основным критериям:

- Политика безопасности
- Гарантированность

Политика безопасности

Это набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. В частности, правила определяют, в каких случаях пользователь имеет право оперировать с определенными наборами данных. Чем надежнее система, тем строже и многообразнее должна быть политика безопасности. В зависимости от сформулированной политики можно выбирать конкретные механизмы, обеспечивающие безопасность системы. Политика безопасности — это активный компонент защиты, включающий в себя анализ возможных угроз и выбор мер противодействия.

Основными элементами политики безопасности являются

- Произвольное управление доступом;

- Безопасность повторного использования объектов;
- Метки безопасности;
- Принудительное управление доступом;
- Подотчетность.

Гарантированность

Это мера доверия, которая может быть оказана архитектуре и реализации системы. Гарантированность показывает, насколько корректны механизмы, отвечающие за проведение в жизнь политики безопасности. Гарантированность можно считать пассивным компонентом защиты, надзирающим за самими защитниками.

Важным средством обеспечения безопасности является механизм подотчетности (протоколирования). Надежная система должна фиксировать все события, касающиеся безопасности. Ведение протоколов должно дополняться аудитом, то есть анализом регистрационной информации.

Концепция надежной вычислительной базы является центральной при оценке степени гарантированности, с которой систему можно считать надежной. Надежная вычислительная база — это совокупность защитных механизмов системы (включая аппаратное и программное обеспечение), отвечающих за проведение в жизнь политики безопасности.

Классы безопасности

В "Оранжевой книге" определяется четыре уровня безопасности (надежности) — D, C, B и A. Уровень D предназначен для систем, признанных неудовлетворительными. В настоящее время он содержит две подсистемы управления доступом для ПК.

По мере перехода от уровня C к A к надежности систем предъявляются все более жесткие требования. Уровни C и B подразделяются на классы (C1, C2, B1, B2, B3) с постепенным возрастанием надежности. Таким образом, всего имеется шесть классов безопасности — C1, C2, B1, B2, B3, A1.

Чтобы система в результате процедуры сертификации могла быть отнесена к некоторому классу, ее политика безопасности и гарантированность должны удовлетворять приводимым ниже требованиям.

Оранжевая книга	Классы безопасности					
Надежность системы	C1	C2	B1	B2	B3	A1
1. Политика безопасности						
1.1 Произвольное управление доступом	+	+	=	=	+	=
1.2 Повторное использование объектов		+	=	=	=	=
1.3.1 Метки безопасности			+	+	=	=
1.3.2 Целостность меток безопасности			+	+	=	=

1.4 Принудительное управление доступом			+	+	=	=
1.5 Подотчетность						
1.5.1 Идентификация и аутентификация	+	+	+	=	=	=
1.5.2 Предоставление надежного пути				+	+	=
1.5.3 Аудит		+	+	+	+	=

3. Интерпретация "Оранжевой книги" для сетевых конфигураций.

Вводится новое понятие — сетевая надежная вычислительная база, распределенный аналог надежной вычислительной базы изолированных систем. Сетевая надежная вычислительная база формируется из всех частей всех компонентов сети, обеспечивающих информационную безопасность. Надежная сетевая система должна обеспечивать такое распределение защитных механизмов, чтобы общая политика безопасности проводилась в жизнь несмотря на уязвимость коммуникационных путей и на параллельную, асинхронную работу компонентов.

Интерпретация предусматривает различные варианты распределения сетевой надежной вычислительной базы по компонентам и, соответственно, различные варианты распределения механизмов управления доступом.

В частности, некоторые компоненты, закрытые от прямого доступа пользователей (например, коммутаторы пакетов, оперирующие на третьем уровне семиуровневой модели OSI), могут вообще не содержать подобных механизмов.

Идентификация групп пользователей может строиться на основе сетевых адресов хостов или (под)сетей. В то же время регистрационный журнал должен содержать достаточно информации для ассоциирования действий с конкретным пользователем. Сетевой адрес может являться частью глобального идентификатора пользователя.

В принципе возможен централизованный контроль доступа, когда решения принимает специальный сервер авторизации. Возможен и смешанный вариант, когда сервер авторизации разрешает соединение двух хостов, а дальше в дело вступают локальные механизмы хоста, содержащего объект доступа.

Аналогично, идентификация и аутентификация пользователей может производиться как централизованно (соответствующим сервером), так и локально — той системой, с которой пользователь непосредственно взаимодействует. Возможна передача идентификационной и аутентификационной информации между хостами (чтобы избавить пользователя от многократной аутентификации). При передаче аутентификационная информация должна быть защищена не слабее, чем на каждом из компонентов сетевой конфигурации.

В качестве еще одного отличительного момента Интерпретации нужно отметить повышенное внимание к целостности информации вообще и меток безопасности в частности. Для контроля целостности меток и для их защиты от нелегального изменения в Интерпретации рекомендуется широкое использование криптографических методов. Далее, чтобы принудительное управление доступом в распределенной конфигурации имело смысл,

совокупность уровней секретности и категорий должна поддерживаться централизованно. В этом одно из принципиальных отличий от произвольного управления доступом.

Новым по сравнению с Оранжевой книгой является рассмотрение вопросов доступности. Сетевой сервис перестает быть доступным, когда пропускная способность коммуникационных каналов падает ниже минимально допустимого уровня или сервис не в состоянии обслуживать запросы. Удаленный ресурс может стать недоступным и вследствие нарушения равноправия в обслуживании пользователей. Надежная система должна быть в состоянии обнаруживать ситуации недоступности, уметь возвращаться к нормальной работе и противостоять атакам на доступность.

4. Гармонизированные критерии Европейских стран.

Европейские страны приняли согласованные критерии оценки безопасности информационных технологий (Information Technology Security Evaluation Criteria, ITSEC). опубликованные в июне 1991 года от имени соответствующих органов четырех стран — Франции, Германии, Нидерландов и Великобритании.

Принципиально важной чертой Европейских Критериев является отсутствие априорных требований к условиям, в которых должна работать информационная система.

Так называемый спонсор, то есть организация, запрашивающая сертификационные услуги, формулирует цель оценки, то есть описывает условия, в которых должна работать система, возможные угрозы ее безопасности и предоставляемые ею защитные функции. Задача органа сертификации — оценить, насколько полно достигаются поставленные цели, то есть насколько корректны и эффективны архитектура и реализация механизмов безопасности в описанных спонсором условиях.

Европейские Критерии рассматривают следующие составляющие информационной безопасности:

1. конфиденциальность, то есть защиту от несанкционированного получения информации;

2. целостность, то есть защиту от несанкционированного изменения информации;

3. доступность, то есть защиту от несанкционированного удержания информации и ресурсов.

В Критериях проводится различие между системами и продуктами. Система — это конкретная аппаратно-программная конфигурация, построенная с вполне определенными целями и функционирующая в известном окружении. Продукт — это аппаратно-программный "пакет", который можно купить и по своему усмотрению встроить в ту или иную систему. Таким образом, с точки зрения информационной безопасности основное отличие между системой и продуктом состоит в том, что система имеет конкретное окружение, которое можно определить и изучить сколь угодно детально, а продукт должен быть рассчитан на использование в различных условиях.

В Европейских Критериях средства, имеющие отношение к информационной безопасности, рассматриваются на трех уровнях детализации. Наиболее абстрактный взгляд касается лишь целей безопасности. На этом уровне мы получаем ответ на вопрос, зачем нужны функции безопасности. Второй уровень содержит спецификации функций безопасности. Мы узнаем, какая функциональность на самом деле обеспечивается. Наконец, на третьем уровне содержится информация о механизмах безопасности. Мы видим, как реализуется декларированная функциональность.

Спецификации функций безопасности — важнейшая часть описания объекта оценки. Критерии рекомендуют выделить в этих спецификациях разделы со следующими заголовками:

1. Идентификация и аутентификация.
2. Управление доступом.
3. Подотчетность.
4. Аудит.
5. Повторное использование объектов.
6. Точность информации.
7. Надежность обслуживания.
8. Обмен данными.

Набор функций безопасности может специфицироваться с использованием ссылок на заранее определенные классы функциональности.

В Европейских Критериях таких классов десять. Пять из них (F-C1, F-C2, F-B1, F-B2, F-B3) соответствуют классам безопасности "Оранжевой книги".

5. Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий".

Этот международный стандарт стал итогом почти десятилетней работы специалистов нескольких стран, он вобрал в себя опыт существовавших к тому времени документов национального и межнационального масштаба. Данный стандарт часто называют "Общими критериями" (ОК).

"Общие критерии" на самом деле являются метастандартом, определяющим инструменты оценки безопасности ИС и порядок их использования.

В отличие от "Оранжевой книги", ОК не содержат предопределенных "классов безопасности". Такие классы можно строить, исходя из требований безопасности, существующих для конкретной организации и/или конкретной информационной системы.

ОК содержат два основных вида требований безопасности:

1. функциональные, соответствующие активному аспекту защиты, предъявляемые к функциям безопасности и реализующим их механизмам;

2. требования доверия, соответствующие пассивному аспекту, предъявляемые к технологии и процессу разработки и эксплуатации.

Требования безопасности предъявляются, а их выполнение проверяется для определенного объекта оценки - аппаратно-программного продукта или информационной системы.

Очень важно, что безопасность в ОК рассматривается не статично, а в привязке к жизненному циклу объекта оценки. Выделяются следующие этапы:

1. определение назначения, условий применения, целей и требований безопасности;

2. проектирование и разработка;

3. испытания, оценка и сертификация;

4. внедрение и эксплуатация.

В ОК объект оценки рассматривается в контексте среды безопасности, которая характеризуется определенными условиями и угрозами.

В свою очередь, угрозы характеризуются следующими параметрами:

1. источник угрозы;

2. метод воздействия;

3. уязвимые места, которые могут быть использованы;

4. ресурсы (активы), которые могут пострадать.

Уязвимые места могут возникать из-за недостатка:

1. в требованиях безопасности;

2. в проектировании;

3. в эксплуатации.

Слабые места по возможности следует устранить, минимизировать или хотя бы постараться ограничить возможный ущерб от их преднамеренного использования или случайной активизации.

С точки зрения технологии программирования в ОК использован устаревший библиотечный (не объектный) подход. Чтобы, тем не менее, структурировать пространство требований, в "Общих критериях" введена иерархия класс – семейство – компонент - элемент.

Классы определяют наиболее общую, "предметную" группировку требований (например, функциональные требования подотчетности).

Семейства в пределах класса различаются по строгости и другим нюансам требований.

Компонент - минимальный набор требований, фигурирующий как целое.

Элемент - неделимое требование.

Между компонентами ОК могут существовать зависимости. Они возникают, когда компонент сам по себе недостаточен для достижения цели безопасности. Вообще говоря, не все комбинации компонентов имеют смысл, и понятие зависимости в какой-то степени компенсирует недостаточную выразительность библиотечной организации, хотя и не заменяет объединение функций в содержательные объектные интерфейсы.

Формируется два вида нормативных документов: профиль защиты и задание по безопасности.

Профиль защиты (ПЗ) представляет собой типовой набор требований, которым должны удовлетворять продукты и/или системы определенного класса (например, операционные системы на компьютерах в правительственных организациях).

Задание по безопасности содержит совокупность требований к конкретной разработке, выполнение которых обеспечивает достижение поставленных целей безопасности.

В ОК нет готовых классов защиты. Сформировать классификацию в терминах "Общих критериев" - значит определить несколько иерархически упорядоченных (содержащих усиливающиеся требования) профилей защиты, в максимально возможной степени использующих стандартные функциональные требования и требования доверия безопасности.

Выделение некоторого подмножества из всего множества профилей защиты во многом носит субъективный характер. По целому ряду соображений (одним из которых является желание придерживаться объектно-ориентированного подхода) целесообразно, на наш взгляд, сформировать сначала отправную точку классификации, выделив базовый (минимальный) ПЗ, а дополнительные требования компоновать в функциональные пакеты.

Функциональный пакет - это неоднократно используемая совокупность компонентов, объединенных для достижения определенных целей безопасности. "Общие критерии" не регламентируют структуру пакетов, процедуры верификации, регистрации и т.п., отводя им роль технологического средства формирования ПЗ.

Базовый профиль защиты должен включать требования к основным (обязательным в любом случае) возможностям. Производные профили получаются из базового путем добавления необходимых пакетов расширения, то есть подобно тому, как создаются производные классы в объектно-ориентированных языках программирования.

Функциональные требования сгруппированы на основе выполняемой ими роли или обслуживаемой цели безопасности. Всего в "Общих критериях" представлено 11 функциональных классов, 66 семейств, 135 компонентов. Это, конечно, значительно больше, чем число аналогичных сущностей в "Оранжевой книге".

Перечислим классы функциональных требований ОК:

1. идентификация и аутентификация;

2. защита данных пользователя;

3. защита функций безопасности (требования относятся к целостности и контролю данных сервисов безопасности и реализующих их механизмов);

4. управление безопасностью (требования этого класса относятся к управлению атрибутами и параметрами безопасности);

5. аудит безопасности (выявление, регистрация, хранение, анализ данных, затрагивающих безопасность объекта оценки, реагирование на возможное нарушение безопасности);

6. доступ к объекту оценки;

7. приватность (защита пользователя от раскрытия и несанкционированного использования его идентификационных данных);

8. использование ресурсов (требования к доступности информации);

9. криптографическая поддержка (управление ключами);

10. связь (аутентификация сторон, участвующих в обмене данными);

11. доверенный маршрут/канал (для связи с сервисами

безопасности).

"Общие критерии" - очень продуманный и полный документ с точки зрения функциональных требований. В то же время, хотелось бы обратить внимание и на некоторые недостатки.

Первый - это отсутствие объектного подхода. Функциональные требования не сгруппированы в осмысленные наборы (объектные интерфейсы), к которым могло бы применяться наследование. Подобное положение, как известно из технологии программирования, чревато появлением слишком большого числа комбинаций функциональных компонентов, несопоставимых между собой.

В современном программировании ключевым является вопрос накопления и многократного использования знаний. Стандарты - одна из форм накопления знаний. Подход в ОК сужает круг фиксируемых знаний, усложняет их корректное использование.

К сожалению, в "Общих критериях" отсутствуют архитектурные требования, что является естественным следствием программистского подхода "снизу вверх". Технологичность средств безопасности, следование общепризнанным рекомендациям по протоколам и программным интерфейсам, а также апробированным архитектурным решениям, таким как менеджер/агент, - необходимые качества изделий информационных технологий, предназначенных для поддержки критически важных функций, к числу которых, безусловно, относятся функции безопасности. Без рассмотрения интерфейсных аспектов системы оказываются нерасширяемыми и изолированными. С практической точки зрения это недопустимо.

Каждый элемент требований доверия принадлежит одному из трех типов:

1. действия разработчиков;

2. представление и содержание свидетельств;

3. действия оценщиков.

Всего в ОК 10 классов, 44 семейства, 93 компонента требований доверия безопасности. Перечислим классы:

1. разработка (требования для поэтапной детализации функций безопасности от краткой спецификации до реализации);

2. поддержка жизненного цикла (требования к модели жизненного цикла, включая порядок устранения недостатков и защиту среды разработки);

3. тестирование;

4. оценка уязвимостей (включая оценку стойкости функций безопасности);

5. поставка и эксплуатация;

6. управление конфигурацией;

7. руководства (требования к эксплуатационной документации);

8. поддержка доверия (для поддержки этапов жизненного цикла после сертификации);

9. оценка профиля защиты;

10. оценка задания по безопасности.

6. Руководящие документы по защите от несанкционированного доступа Гостехкомиссии при Президенте РФ.

Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения СВТ или АС.

В Концепции формулируются следующие основные принципы защиты от НСД к информации:

1. Защита СВТ обеспечивается комплексом программно-технических средств.

2. Защита АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер.

3. Защита АС должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

4. Программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики АС (надежность, быстродействие, возможность изменения конфигурации АС).

5. Неотъемлемой частью работ по защите является оценка эффективности средств защиты, осуществляемая по методике, учитывающей всю совокупность технических характеристик оцениваемого объекта, включая технические решения и практическую реализацию средств защиты.

6. Защита АС должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем АС или контролирующими органами.

В качестве главного средства защиты от НСД к информации в Концепции рассматривается система разграничения доступа (СРД) субъектов к объектам доступа.

Основными функциями СРД являются:

1. реализация правил разграничения доступа (ПРД) субъектов и их процессов к данным;

2. реализация ПРД субъектов и их процессов к устройствам создания твердых копий;

3. изоляция программ процесса, выполняемого в интересах субъекта, от других субъектов;

4. управление потоками данных с целью предотвращения записи данных на носители несоответствующего грифа;

5. реализация правил обмена данными между субъектами для АС и СВТ, построенных по сетевым принципам.

Кроме того, Концепция предусматривает наличие обеспечивающих средств для СРД, которые выполняют следующие функции:

1. идентификацию и опознание (аутентификацию) субъектов и поддержание привязки субъекта к процессу, выполняемому для субъекта;

2. регистрацию действий субъекта и его процесса;

3. предоставление возможностей исключения и включения новых субъектов и объектов доступа, а также изменение полномочий субъектов;

4. реакцию на попытки НСД, например, сигнализацию, блокировку, восстановление после НСД;

5. тестирование;

6. очистку оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователя с защищаемыми данными;

7. учет выходных печатных и графических форм и твердых копий в АС;

8. контроль целостности программной и информационной части как СРД, так и обеспечивающих ее средств.

Технические средства защиты от НСД, согласно Концепции, должны оцениваться по следующим основным параметрам:

1. степень полноты охвата ПРД реализованной СРД и ее качество;

2. состав и качество обеспечивающих средств для СРД;

3. гарантии правильности функционирования СРД и обеспечивающих ее средств.

Устанавливается семь классов защищенности СВТ от НСД к информации.

Самый низкий класс — седьмой, самый высокий — первый. Классы подразделяются на четыре группы, отличающиеся качественным уровнем защиты:

1. первая группа содержит только один седьмой класс;

2. вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;

3. третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;

4. четвертая группа характеризуется верифицированной защитой и содержит только первый класс.

Седьмой класс присваивают СВТ, к которым предъявлялись требования по защите от НСД к информации, но при оценке защищенность СВТ оказалась ниже уровня требований шестого класса.

2. Практическое задание

Изучить в интернете один из основополагающих документов, рассмотренных выше и составить краткий конспект этого документа.

3. Содержание отчета

1. Титульный лист
2. Содержание
3. Практическое задание
4. Конспект документа
5. Выводы

Перечень основной литературы

1. Информационная безопасность: учебник для вузов/ В.И. Ярочкин – М.: Академический проект, 2012.

2. Семененко В.А. Информационная безопасность: учеб.пособие/ В.А. Семененко – М.: МГИУ, 2013.

Перечень дополнительной литературы

1. Информационная безопасность: учебник для вузов/ В.И. Ярочкин – М.: Академический проект, 2012.

2. Семененко В.А. Информационная безопасность: учеб.пособие/ В.А. Семененко – М.: МГИУ, 2013.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

Методические рекомендации по выполнению лабораторных работ по дисциплине «Основы управления информационной безопасности ".

2. Методические рекомендации по организации самостоятельной работы студентов по дисциплине " Основы управления информационной безопасности ".

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://el.ncfu.ru/ – система управления обучением ФГАОУ ВО СКФУ. Дистанционная поддержка дисциплины «Информационные технологии в профессиональной деятельности»
2. http://www.un.org - Сайт ООН Информационно-коммуникационные технологии
3. http://www.intuit.ru – Интернет-Университет Компьютерных технологий.

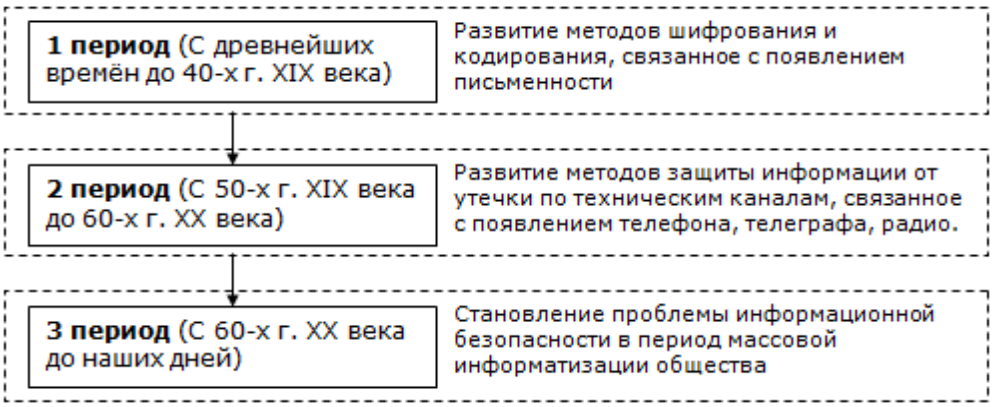
Практическое занятие 2. Обеспечение информационной безопасности в ведущих зарубежных странах

Цель работы: *ознакомление с основными принципами обеспечения информационной безопасности в ведущих зарубежных странах*

1. Теоретическая часть

Обеспечение защиты информации волновало человечество всегда. В процессе эволюции цивилизации менялись виды информации, для её защиты применялись различные методы и средства.

Процесс развития средств и методов защиты информации можно разделить на три относительно самостоятельных периода:



Наблюдаемые в последние годы тенденции в развитии информационных технологий могут уже в недалеком будущем привести к появлению качественно новых

(информационных) форм борьбы, в том числе и на межгосударственном уровне, которые могут принимать форму информационной войны, а сама информационная война станет одним из основных инструментов внешней политики, включая защиту государственных интересов и реализацию любых форм агрессии. Это является одной из причин, почему полезно ознакомиться с основными принципами обеспечения ИБ в ведущих зарубежных странах.

Другая причина заключается в том, что большинство применяемых на территории РФ средств и методов обеспечения ИБ основаны на импортных методиках и строятся из импортных компонентов, которые были разработаны в соответствии с нормами и требованиями по обеспечению ИБ стран-изготовителей. В связи с этим, прежде чем приступить к изучению непосредственно технологий и средств обеспечения ИБ, следует познакомиться с политикой ИБ ведущих зарубежных стран.

2. Практическое задание

1. Подготовить краткий доклад по заданному вопросу (см. вариант), используя учебное пособие Аверченкова, В.И. «Системы защиты информации в ведущих зарубежных странах» и другие доступные источники информации.
2. Заполнить таблицу «Системы обеспечения ИБ в ведущих зарубежных странах» (см. вариант) на основе подготовленного материала, а также докладов других студентов.
3. Провести анализ собранной информации и сделать выводы.

3. Содержание отчета

1. Титульный лист
2. Содержание
3. Практическое задание
4. Таблица «Системы обеспечения ИБ в ведущих зарубежных странах»
5. Выводы

4. Варианты

Вариант – номер по списку в журнале.

Вариант	Страна	Основные принципы обеспечения ИБ	Основные документы в области обеспечения ИБ	Структура государственных органов обеспечения национальной ИБ
1	**США**			
2	**Италия**			
3	**Великобритания**			
4	**Швеция**			

5	**Франция**			
6	**Германия**			
7	**Китай**			
8	**Япония**			
9	**Швейцария**			
10	**Испания**			
11	**Канада**			
12	**Австралия**			
13	**Бразилия**			
14	**Аргентина**			
15	**Корея**			

Перечень основной литературы

1. Информационная безопасность: учебник для вузов/ В.И. Ярочкин – М.: Академический проект, 2012.

2. Семененко В.А. Информационная безопасность: учеб.пособие/ В.А. Семененко – М.: МГИУ, 2013.

Перечень дополнительной литературы

1. Информационная безопасность: учебник для вузов/ В.И. Ярочкин – М.: Академический проект, 2012.

2. Семененко В.А. Информационная безопасность: учеб.пособие/ В.А. Семененко – М.: МГИУ, 2013.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

Методические рекомендации по выполнению лабораторных работ по дисциплине «Основы управления информационной безопасности ".

2. Методические рекомендации по организации самостоятельной работы студентов по дисциплине " Основы управления информационной безопасности ".

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://el.ncfu.ru/ – система управления обучением ФГАОУ ВО СКФУ. Дистанционная поддержка дисциплины «Информационные технологии в профессиональной деятельности»
2. http://www.un.org - Сайт ООН Информационно-коммуникационные технологии
3. http://www.intuit.ru – Интернет-Университет Компьютерных технологий.

Практическое занятие 3. «Требования и показатели защищенности автоматизированных средств обработки информации»

Цель работы: *ознакомиться с требованиями и показателями защищенности автоматизированных средств обработки информации*

1. Теоретическая часть

Защита информации от несанкционированного доступа (НСД) является составной частью общей проблемы обеспечения безопасности информации. Мероприятия по защите информации от НСД должны осуществляться взаимосвязано с мероприятиями по специальной защите основных и вспомогательных средств вычислительной техники, средств и систем связи от технических средств разведки и промышленного шпионажа.

В общем случае, комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД реализуется в рамках системы защиты информации от НСД (СЗИ НСД), условно состоящей из следующих четырех подсистем:

- управления доступом;
- регистрации и учета;
- криптографической;
- обеспечения целостности.

В зависимости от класса автоматизированной системы (АС) в рамках этих подсистем должны быть реализованы следующие требования.

Требования к АС третьей группы представлены в табл. 1.

Обозначения:

- " - " - нет требований к данному классу;
- " + " - есть требования к данному классу.

Таблица 1 Требования к АС третьей группы

1. Подсистемы и требования	2. Классы	
	4. 3 Б	5. 3 А
6. **1. Подсистема управления доступом**	7.	8.
9. 1.1. Идентификация, проверка подлинности и контроль доступа субъектов:	10.	11.
12. в систему	13. +	14. +
15. к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	16. -	17. -
18. к программам	19. -	20. -
21. к томам, каталогам, файлам, записям, полям записей	22. -	23. -
24. 1.2. Управление потоками информации	25.	26.
27. **2. Подсистема регистрации и учета**	28.	29.
30. 2.1. Регистрация и учет:	31.	32.
33. входа (выхода) субъектов доступа в (из) систему(ы) (узел сети)	34. +	35. +
36. выдачи печатных (графических) выходных документов	37. -	38. +

39. запуска (завершения) программ и процессов (заданий, задач)	40. -	41. -
42. доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	43. -	44. -
45. доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	46. -	47. -
48. изменения полномочий субъектов доступа	49. -	50. -
51. создаваемых защищаемых объектов доступа	52. -	53. -
54. 2.2. Учет носителей информации	55. +	56. +
57. 2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	58. -	59. +
60. 2.4. Сигнализация попыток нарушения защиты	61. -	62. -
63. **3. Криптографическая подсистема**	64.	65.
66. 3.1. Шифрование конфиденциальной информации	67. -	68. -
69. 3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	70. -	71. -
72. 3.3. Использование аттестованных (сертифицированных) криптографических средств	73. -	74. -
75. **4. Подсистема обеспечения целостности**	76.	77.
78. 4.1. Обеспечение целостности программных средств и обрабатываемой информации	79. +	80. +
81. 4.2. Физическая охрана средств вычислительной техники и носителей информации	82. +	83. +
84. 4.3. Наличие администратора (службы) защиты информации в АС	85. -	86. -
87. 4.4. Периодическое тестирование СЗИ НСД	88. +	89. +
90. 4.5. Наличие средств восстановления СЗИ НСД	91. +	92. +
93. 4.6. Использование сертифицированных	94. -	95. +

средств защиты		

Требования к АС второй группы представлены в табл. 2.
Обозначения:
" - " - нет требований к данному классу;
" + " - есть требования к данному классу.

Таблица 2 Требования к АС второй группы

96. Подсистемы и требования	97. Классы	
	99. 2 Б	100. 2 А
101. 1. Подсистема управления доступом	102.	103.
104. 1.1. Идентификация, проверка подлинности и контроль доступа субъектов:	105.	106.
107. в систему	108. +	109. +
110. к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	111. -	112. +
113. к программам	114. -	115. +
116. к томам, каталогам, файлам, записям, полям записей	117. -	118. +
119. 1.2. Управление потоками информации	120. -	121. +
122. 2. Подсистема регистрации и учета	123.	124.
125. 2.1. Регистрация и учет:	126.	127.
128. входа (выхода) субъектов доступа в (из) систему (узел сети)	129. +	130. +
131. выдачи печатных (графических) выходных документов	132. -	133. +
134. запуска (завершения) программ и процессов (заданий, задач)	135. -	136. +
137. доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	138. -	139. +
140. доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	141. -	142. +
143. изменения полномочий субъектов доступа	144. -	145. -

146. создаваемых защищаемых объектов доступа	147. -	148. +
149. 2.2. Учет носителей информации	150. +	151. +
152. 2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	153. -	154. +
155. 2.4. Сигнализация попыток нарушения защиты	156. -	157. -
158. 3. Криптографическая подсистема	159.	160.
161. 3.1. Шифрование конфиденциальной информации	162. -	163. +
164. 3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	165. -	166. -
167. 3.3. Использование аттестованных (сертифицированных) криптографических средств	168. -	169. +
170. 4. Подсистема обеспечения целостности	171.	172.
173. 4.1. Обеспечение целостности программных средств и обрабатываемой информации	174. +	175. +
176. 4.2. Физическая охрана средств вычислительной техники и носителей информации	177. +	178. +
179. 4.3. Наличие администратора (службы) защиты информации в АС	180. -	181. +
182. 4.4. Периодическое тестирование СЗИ НСД	183. +	184. +
185. 4.5. Наличие средств восстановления СЗИ НСД	186. +	187. +
188. 4.6. Использование сертифицированных средств защиты	189. -	190. +

Требования к АС первой группы представлены в табл. 3.
Обозначения:
" - " - нет требований к данному классу;
" + " - есть требования к данному классу.

Таблица 3 Требования к АС первой группы

191. Подсистемы и требования	192. Классы				
	194. 1 Д	195. 1 Г	196. 1 В	197. 1 Б	198. 1 А
199. 1. Подсистема управления доступом	200.	201.	202.	203.	204.

205. 1.1. Идентификация, проверка подлинности и контроль доступа субъектов:	206.	207.	208.	209.	210.
211. в систему	212. +	213. +	214. +	215. +	216. +
217. к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	218. -	219. +	220. +	221. +	222. +
223. к программам	224. -	225. +	226. +	227. +	228. +
229. к томам, каталогам, файлам, записям, полям записей	230. -	231. +	232. +	233. +	234. +
235. 1.2. Управление потоками информации	236. -	237. -	238. +	239. +	240. +
241. 2. Подсистема регистрации и учета	242.	243.	244.	245.	246.
247. 2.1. Регистрация и учет:	248.	249.	250.	251.	252.
253. входа (выхода) субъектов доступа в (из) систему (узел сети)	254. +	255. +	256. +	257. +	258. +
259. выдачи печатных (графических) выходных документов	260. -	261. +	262. +	263. +	264. +
265. запуска (завершения) программ и процессов (заданий, задач)	266. -	267. +	268. +	269. +	270. +
271. доступа программ субъектов доступа к защищаемым	272. -	273. +	274. +	275. +	276. +

файлам, включая их создание и удаление, передачу по линиям и каналам связи					
277. доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	278. -	279. +	280. +	281. +	282. +
283. изменения полномочий субъектов доступа	284. -	285. -	286. +	287. +	288. +
289. создаваемых защищаемых объектов доступа	290. -	291. -	292. +	293. +	294. +
295. 2.2. Учет носителей информации	296. +	297. +	298. +	299. +	300. +
301. 2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	302. -	303. +	304. +	305. +	306. +
307. 2.4. Сигнализация попыток нарушения защиты	308. -	309. -	310. +	311. +	312. +
313. 3. Криптографическая	314.	315.	316.	317.	318.

подсистема					
319. 3.1. Шифрование конфиденциальной информации	320. -	321. -	322. -	323. +	324. +
325. 3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	326. -	327. -	328. -	329. -	330. +
331. 3.3. Использование аттестованных (сертифицированных) криптографических средств	332. -	333. -	334. -	335. +	336. +
337. 4. Подсистема обеспечения целостности	338.	339.	340.	341.	342.
343. 4.1. Обеспечение целостности программных средств и обрабатываемой информации	344. +	345. +	346. +	347. +	348. +
349. 4.2. Физическая охрана средств вычислительной техники и носителей информации	350. +	351. +	352. +	353. +	354. +
355. 4.3. Наличие администратора	356. -	357. -	358. +	359. +	360. +

(службы) защиты информации в АС					
361. 4.4. Периодическое тестирование СЗИ НСД	362. +	363. +	364. +	365. +	366. +
367. 4.5. Наличие средств восстановления СЗИ НСД	368. +	369. +	370. +	371. +	372. +
373. 4.6. Использование сертифицированных средств защиты	374. -	375. -	376. +	377. +	378. +

Организационные мероприятия в рамках средств защиты информации от несанкционированного доступа в АС, обрабатывающих или хранящих информацию, являющуюся собственностью государства и отнесенную к категории секретной, должны отвечать государственным требованиям по обеспечению режима секретности проводимых работ.

При обработке или хранении в АС информации, не отнесенной к категории секретной, в рамках СЗИ НСД государственным, коллективным, частным и совместным предприятиям, а также частным лицам рекомендуются следующие организационные мероприятия:

- выявление конфиденциальной информации и ее документальное оформление в виде перечня сведений, подлежащих защите;
- определение порядка установления уровня полномочий субъекта доступа, а также круга лиц, которым это право предоставлено;
- установление и оформление правил разграничения доступа, т.е. совокупности правил, регламентирующих права доступа субъектов к объектам;
- ознакомление субъекта доступа с перечнем защищаемых сведений и его уровнем полномочий, а также с организационно-распорядительной и рабочей документацией, определяющей требования и порядок обработки конфиденциальной информации;
- получение от субъекта доступа расписки о неразглашении доверенной ему конфиденциальной информации;
- обеспечение охраны объекта, на котором расположена защищаемая АС, (территория, здания, помещения, хранилища информационных носителей) путем установления соответствующих постов, технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими хищение средств вычислительной техники (СВТ), информационных носителей, а также НСД к СВТ и линиям связи;
- выбор класса защищенности АС в соответствии с особенностями обработки информации (технология обработки, конкретные условия эксплуатации АС) и уровнем ее конфиденциальности;
- организация службы безопасности информации (ответственные лица, администратор АС), осуществляющей учет, хранение и выдачу информационных носителей, паролей, ключей, ведение служебной информации СЗИ НСД (генерацию паролей, ключей, сопровождение правил разграничения доступа), приемку включаемых в АС новых программных средств, а

также контроль за ходом технологического процесса обработки конфиденциальной информации и т.д.;
- разработка СЗИ НСД, включая соответствующую организационно-распорядительную и эксплуатационную документацию;
- осуществление приемки СЗИ НСД в составе АС.
При разработке АС, предназначенной для обработки или хранения информации, являющейся собственностью государства и отнесенной к категории секретной, необходимо ориентироваться в соответствии с РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» на классы защищенности АС не ниже (по группам) 3А, 2А, 1А, 1Б, 1В и использовать сертифицированные СВТ:
- не ниже 4 класса - для класса защищенности АС 1В;
- не ниже 3 класса - для класса защищенности АС 1Б;
- не ниже 2 класса - для класса защищенности АС 1А.

2. задание

Изучить и описать требования по обеспечению информационной безопасности для конкретного предприятия (см. вариант).

3. Содержание отчета

1. Титульный лист
2. Содержание
3. Лабораторное задание
4. Описание требований и выбор класса защищенности АС
5. Оценка рисков
6. Выводы

4. Варианты

Вариант – номер по списку в журнале.

Номер варианта	**Организация**	**Метод оценки риска (см. Приложение Е ГОСТа)**
1	Отделение коммерческого банка	1
2	Поликлиника	2
3	Университет	3
4	Офис страховой компании	4
5	Интернет-магазин	1
6	Центр оказания государственных услуг	2
7	Отделение полиции	3

8	Аудиторская компания	4
9	Дизайнерская фирма	1
10	Офис адвоката	2
11	Агентство недвижимости	3
12	Туристическое агентство	4
13	Издательство	1
14	Рекламное агентство	2
15	Отделение налоговой службы	3
16	Гостиница	4
17	Городской архив	1
18	Офис нотариуса	2
19	Диспетчерская служба такси	3
20	Железнодорожная касса	4

Перечень основной литературы

1. Информационная безопасность: учебник для вузов/ В.И. Ярочкин – М.: Академический проект, 2012.

2. Семененко В.А. Информационная безопасность: учеб.пособие/ В.А. Семененко – М.: МГИУ, 2013.

Перечень дополнительной литературы

1. Информационная безопасность: учебник для вузов/ В.И. Ярочкин – М.: Академический проект, 2012.

2. Семененко В.А. Информационная безопасность: учеб.пособие/ В.А. Семененко – М.: МГИУ, 2013.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

Методические рекомендации по выполнению лабораторных работ по дисциплине «Основы управления информационной безопасности ".

2. Методические рекомендации по организации самостоятельной работы студентов по дисциплине " Основы управления информационной безопасности ".

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://el.ncfu.ru/ – система управления обучением ФГАОУ ВО СКФУ. Дистанционная поддержка дисциплины «Информационные технологии в профессиональной деятельности»
2. http://www.un.org - Сайт ООН Информационно-коммуникационные технологии
3. http://www.intuit.ru – Интернет-Университет Компьютерных технологий.

Практическое занятие 4. «Алгоритмы поведения вирусных и других вредоносных программ»

Цель работы: *изучение технологии аутентификации пользователя на основе пароля*

1. Теоретическая часть

На сегодняшний день перечень доступных антивирусных программ весьма обширен. Они различаются как по цене, так и по своим функциональным возможностям. Наиболее мощные (и, как правило, наиболее дорогие) антивирусные программы представляют собой на самом деле пакеты специализированных утилит, способных при совместном их использовании обеспечить разностороннюю защиту компьютерной системы.

Большинство современных антивирусных пакетов выполняют следующие функции:

- сканирование памяти и содержимого дисков;
- сканирование в реальном режиме времени с помощью резидентного модуля;
- распознавание поведения, характерного для компьютерных вирусов;
- блокировка и/или удаление выявленных вирусов;
- восстановление зараженных информационных объектов;
- принудительная проверка подключенных к корпоративной сети компьютеров;
- удаленное обновление антивирусного программного обеспечения и баз данных через Интернет;
- фильтрация трафика Интернета на предмет выявления вирусов в передаваемых программах и документах;
- выявление потенциально опасных Java-апплетов и модулей ActiveX;
- ведение протоколов, содержащих информацию о событиях, касающихся антивирусной защиты и др.

2. Практическое задание

1. Подготовить краткий доклад по заданному вопросу (см. вариант), используя любые доступные источники информации.

Рекомендация: Собранный материал будет наиболее актуальным, если включить в него данные, полученные практическим путем. Для этого при возможности, установите демонстрационную версию заданного пакета ПО и протестируйте ее в течении нескольких дней.

2. Заполнить таблицу «Пакеты антивирусных программ» на основе подготовленного материала, а также докладов других студентов.
3. Провести анализ собранной информации и сделать выводы.

3. Содержание отчета

1. Титульный лист
2. Содержание
3. Практическое задание
4. Таблица "Пакеты антивирусных программ"
5. Выводы

4. Варианты

Вариант – номер по списку в журнале.

Пакет антивирусного ПО	Основные функции	Достоинства	Недостатки
Антивирус Касперского			
Антивирус Dr.Web для Windows			
Panda Antivirus			
ESET NOD32 Антивирус			
avast! Free Antivirus			
Avira AntiVir Personal			
Norton AntiVirus			
Trend Micro Internet Security			
Microsoft Security Essentials			
McAfee VirusScan			

Перечень основной литературы

1. Информационная безопасность: учебник для вузов/ В.И. Ярочкин – М.: Академический проект, 2012.

2. Семененко В.А. Информационная безопасность: учеб.пособие/ В.А. Семененко – М.: МГИУ, 2013.

Перечень дополнительной литературы

1. Информационная безопасность: учебник для вузов/ В.И. Ярочкин – М.:

Академический проект, 2012.

2. Семененко В.А. Информационная безопасность: учеб.пособие/ В.А. Семененко – М.: МГИУ, 2013.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

Методические рекомендации по выполнению лабораторных работ по дисциплине «Основы управления информационной безопасности ".

2. Методические рекомендации по организации самостоятельной работы студентов по дисциплине " Основы управления информационной безопасности ".

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://el.ncfu.ru/ – система управления обучением ФГАОУ ВО СКФУ. Дистанционная поддержка дисциплины «Информационные технологии в профессиональной деятельности»
2. http://www.un.org - Сайт ООН Информационно-коммуникационные технологии
3. http://www.intuit.ru – Интернет-Университет Компьютерных технологий.

Практическое занятие 5. ***Тема: «Процедура аутентификации пользователя на основе пароля»***

Цель работы: *изучение технологии аутентификации пользователя на основе пароля.*

Теоретическая часть

Идентификация — это заявление о том, кем вы являетесь. В зависимости от ситуации, это может быть имя, адрес электронной почты, номер учетной записи, итд.
Аутентификация — предоставление доказательств, что вы на самом деле есть тот, кем идентифицировались (от слова “authentic” — истинный, подлинный).
Авторизация — проверка, что вам разрешен доступ к запрашиваемому ресурсу.

Аутентификация по паролю

Этот метод основывается на том, что пользователь должен предоставить username и password для успешной идентификации и аутентификации в системе. Пара username/password задается пользователем при его регистрации в системе, при этом в качестве username может выступать адрес электронной почты пользователя.
Применительно к веб-приложениям, существует несколько стандартных протоколов для аутентификации по паролю, которые мы рассмотрим ниже.

HTTP authentication

Этот протокол, описанный в стандартах HTTP 1.0/1.1, существует очень давно и до сих пор активно применяется в корпоративной среде. Применительно к веб-сайтам работает следующим образом:

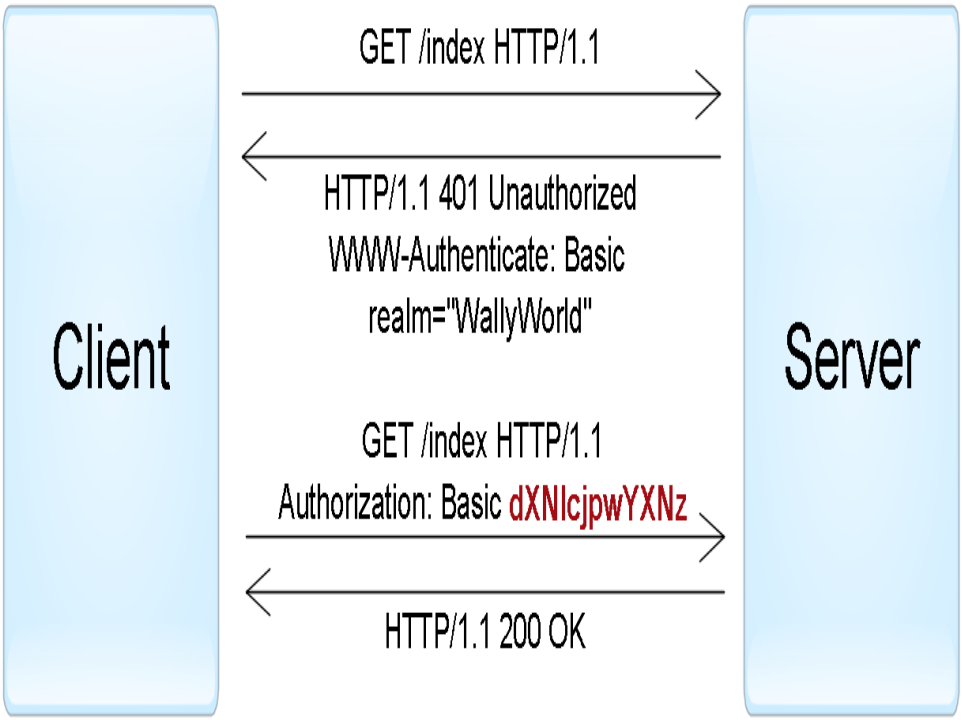
1. Сервер, при обращении неавторизованного клиента к защищенному ресурсу, отсылает HTTP статус “401 Unauthorized” и добавляет заголовок “WWW-Authenticate” с указанием схемы и параметров аутентификации.

2. Браузер, при получении такого ответа, автоматически показывает диалог ввода username и password. Пользователь вводит детали своей учетной записи.
3. Во всех последующих запросах к этому веб-сайту браузер автоматически добавляет HTTP заголовок “Authorization”, в котором передаются данные пользователя для аутентификации сервером.
4. Сервер аутентифицирует пользователя по данным из этого заголовка. Решение о предоставлении доступа (авторизация) производится отдельно на основании роли пользователя, ACL или других данных учетной записи.

Весь процесс стандартизирован и хорошо поддерживается всеми браузерами и веб-серверами. Существует несколько схем аутентификации, отличающихся по уровню безопасности:

Технология работы

1. **Basic** — наиболее простая схема, при которой username и password пользователя передаются в заголовке Authorization в незашифрованном виде (base64-encoded). Однако при использовании HTTPS (HTTP over SSL) протокола, является относительно безопасной.



Пример HTTP аутентификации с использованием Basic схемы.

2. **Digest** — challenge-response-схема, при которой сервер посылает уникальное значение nonce, а браузер передает MD5 хэш пароля пользователя, вычисленный с использованием указанного nonce. Более безопасная альтернативв Basic схемы при незащищенных соединениях, но подвержена man-in-the-middle attacks (с заменой схемы на basic). Кроме того, использование этой схемы не позволяет применить современные хэш-функции для хранения паролей пользователей на сервере.
3. **NTLM** (известная как Windows authentication) — также основана на challenge-response подходе, при котором пароль не передается в чистом виде. Эта схема не является стандартом HTTP, но поддерживается большинством браузеров и веб-серверов.

Преимущественно используется для аутентификации пользователей Windows Active Directory в веб-приложениях. Уязвима к pass-the-hash-атакам.

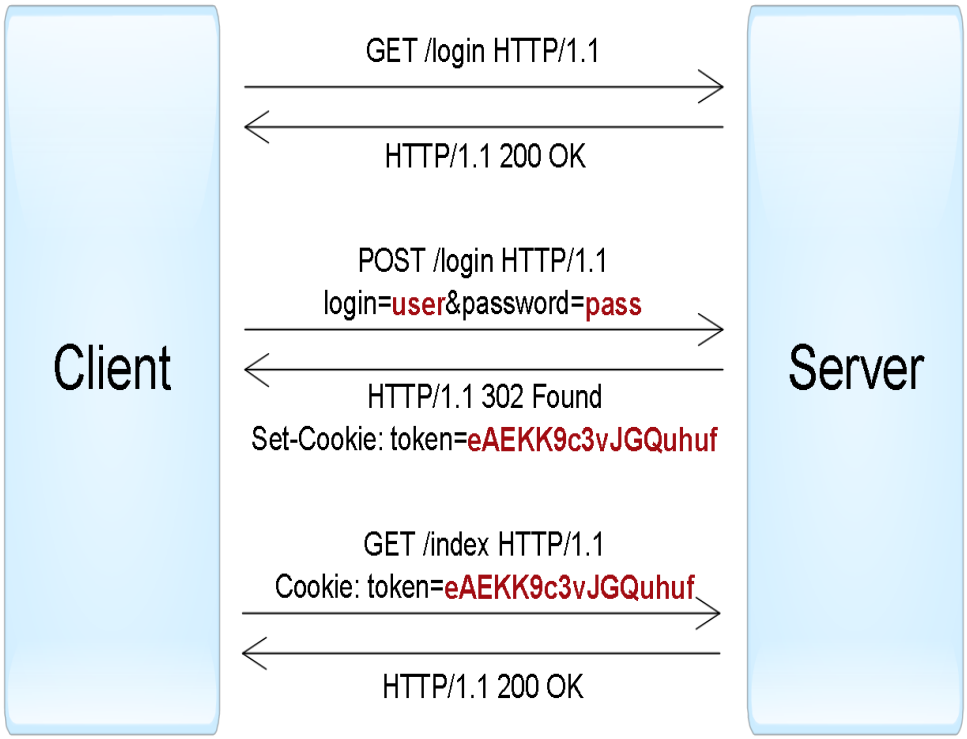
4. **Negotiate** — еще одна схема из семейства Windows authentication, которая позволяет клиенту выбрать между NTLM и Kerberos аутентификацией. Kerberos — более безопасный протокол, основанный на принципе Single Sign-On. Однако он может функционировать, только если и клиент, и сервер находятся в зоне intranet и являются частью домена Windows.

Стоит отметить, что при использовании HTTP-аутентификации у пользователя нет стандартной возможности выйти из веб-приложения, кроме как закрыть все окна браузера.

Forms authentication

Для этого протокола нет определенного стандарта, поэтому все его реализации специфичны для конкретных систем, а точнее, для модулей аутентификации фреймворков разработки.

Работает это по следующему принципу: в веб-приложение включается HTML-форма, в которую пользователь должен ввести свои username/password и отправить их на сервер через HTTP POST для аутентификации. В случае успеха веб-приложение создает session token, который обычно помещается в browser cookies. При последующих веб-запросах *session token* автоматически передается на сервер и позволяет приложению получить информацию о текущем пользователе для авторизации запроса.



Пример forms authentication.

Приложение может создать session token двумя способами:

1. Как идентификатор аутентифицированной сессии пользователя, которая хранится в памяти сервера или в базе данных. Сессия должна содержать всю необходимую информацию о пользователе для возможности авторизации его запросов.
2. Как зашифрованный и/или подписанный объект, содержащий данные о пользователе, а также период действия. Этот подход позволяет реализовать stateless-архитектуру сервера, однако требует механизма обновления сессионного токена по истечении срока действия. Несколько стандартных форматов таких токенов рассматриваются в секции «Аутентификация по токенам».

Необходимо понимать, что перехват session token зачастую дает аналогичный уровень доступа, что и знание username/password. Поэтому все коммуникации между клиентом и сервером в случае forms authentication должны производиться только по защищенному соединению HTTPS.

Другие протоколы аутентификации по паролю

Два протокола, описанных выше, успешно используются для аутентификации пользователей на веб-сайтах. Но при разработке клиент-серверных приложений с использованием веб-сервисов (например, iOS или Android), наряду с HTTP аутентификацией, часто применяются нестандартные протоколы, в которых данные для аутентификации передаются в других частях запроса.

Существует всего несколько мест, где можно передать username и password в HTTP запросах:

1. **URL query** — считается небезопасным вариантом, т. к. строки URL могут запоминаться браузерами, прокси и веб-серверами.
2. **Request body** — безопасный вариант, но он применим только для запросов, содержащих тело сообщения (такие как POST, PUT, PATCH).
3. **HTTP header** —оптимальный вариант, при этом могут использоваться и стандартный заголовок Authorization (например, с Basic-схемой), и другие произвольные заголовки.

Распространенные уязвимости и ошибки реализации

Аутентификации по паролю считается не очень надежным способом, так как пароль часто можно подобрать, а пользователи склонны использовать простые и одинаковые пароли в разных системах, либо записывать их на клочках бумаги. Если злоумышленник смог выяснить пароль, то пользователь зачастую об этом не узнает. Кроме того, разработчики приложений могут допустить ряд концептуальных ошибок, упрощающих взлом учетных записей.

Ниже представлен список наиболее часто встречающихся уязвимостей в случае использования аутентификации по паролю:

- Веб-приложение позволяет пользователям создавать простые пароли.
- Веб-приложение не защищено от возможности перебора паролей (brute-force attacks).
- Веб-приложение само генерирует и распространяет пароли пользователям, однако не требует смены пароля после первого входа (т.е. текущий пароль где-то записан).

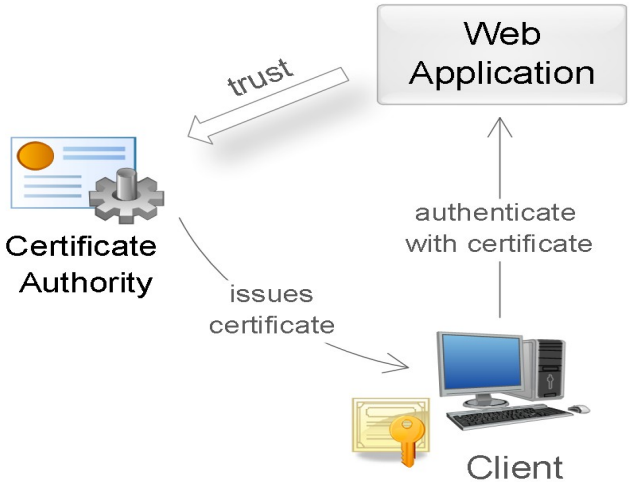
- Веб-приложение допускает передачу паролей по незащищенному HTTP-соединению, либо в строке URL.
- Веб-приложение не использует безопасные хэш-функции для хранения паролей пользователей.
- Веб-приложение не предоставляет пользователям возможность изменения пароля либо не нотифицирует пользователей об изменении их паролей.
- Веб-приложение использует уязвимую функцию восстановления пароля, которую можно использовать для получения несанкционированного доступа к другим учетным записям.
- Веб-приложение не требует повторной аутентификации пользователя для важных действий: смена пароля, изменения адреса доставки товаров и т. п.
- Веб-приложение создает session tokens таким образом, что они могут быть подобраны или предсказаны для других пользователей.
- Веб-приложение допускает передачу session tokens по незащищенному HTTP-соединению, либо в строке URL.
- Веб-приложение уязвимо для session fixation-атак (т. е. не заменяет session token при переходе анонимной сессии пользователя в аутентифицированную).
- Веб-приложение не устанавливает флаги HttpOnly и Secure для browser cookies, содержащих session tokens.
- Веб-приложение не уничтожает сессии пользователя после короткого периода неактивности либо не предоставляет функцию выхода из аутентифицированной сессии.

Аутентификация по сертификатам

Сертификат представляет собой набор атрибутов, идентифицирующих владельца, подписанный *certificate authority* (CA). CA выступает в роли посредника, который гарантирует подлинность сертификатов (по аналогии с ФМС, выпускающей паспорта). Также сертификат криптографически связан с закрытым ключом, который хранится у владельца сертификата и позволяет однозначно подтвердить факт владения сертификатом.

На стороне клиента сертификат вместе с закрытым ключом могут храниться в операционной системе, в браузере, в файле, на отдельном физическом устройстве (smart card, USB token). Обычно закрытый ключ дополнительно защищен паролем или PIN-кодом.

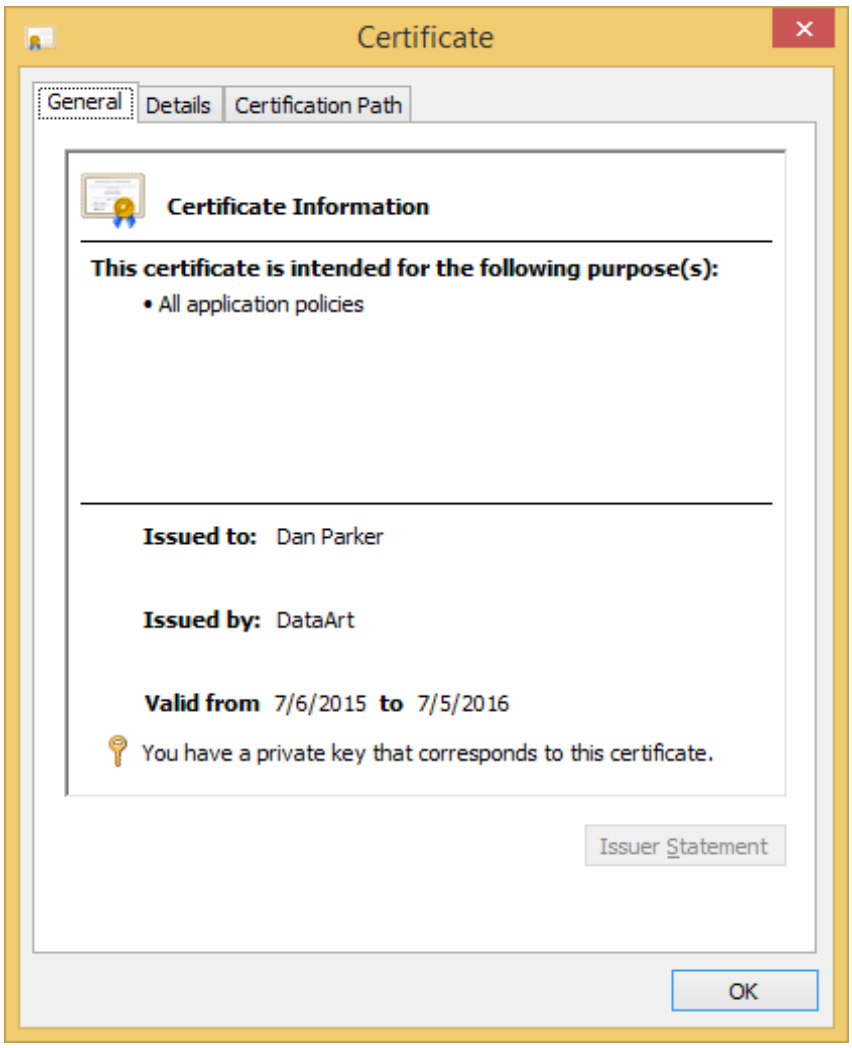
В веб-приложениях традиционно используют сертификаты стандарта X.509. Аутентификация с помощью X.509-сертификата происходит в момент соединения с сервером и является частью протокола SSL/TLS. Этот механизм также хорошо поддерживается браузерами, которые позволяют пользователю выбрать и применить сертификат, если веб-сайт допускает такой способ аутентификации.



Использование сертификата для аутентификации.

Во время аутентификации сервер выполняет проверку сертификата на основании следующих правил:

1. Сертификат должен быть подписан доверенным certification authority (проверка цепочки сертификатов).
2. Сертификат должен быть действительным на текущую дату (проверка срока действия).
3. Сертификат не должен быть отозван соответствующим CA (проверка списков исключения).



Пример X.509 сертификата. После успешной аутентификации веб-приложение может выполнить авторизацию запроса на основании таких данных сертификата, как subject (имя владельца), issuer (эмитент), serial number (серийный номер сертификата) или thumbprint (отпечаток открытого ключа сертификата). Использование сертификатов для аутентификации — куда более надежный способ, чем аутентификация посредством паролей. Это достигается созданием в процессе аутентификации цифровой подписи, наличие которой доказывает факт применения закрытого ключа в конкретной ситуации (non-repudiation). Однако трудности с распространением и поддержкой сертификатов делает такой способ аутентификации малодоступным в широких кругах.

Аутентификация по одноразовым паролям

Аутентификация по одноразовым паролям обычно применяется дополнительно к аутентификации по паролям для реализации *two-factor authentication* (2FA). В этой концепции пользователю необходимо предоставить данные двух типов для входа в систему: что-то, что он знает (например, пароль), и что-то, чем он владеет (например, устройство для генерации одноразовых паролей). Наличие двух факторов позволяет в значительной степени увеличить уровень безопасности, что м. б. востребовано для определенных видов веб-приложений.

Другой популярный сценарий использования одноразовых паролей — дополнительная аутентификация пользователя во время выполнения важных действий: перевод денег, изменение настроек и т. п.

Существуют разные источники для создания одноразовых паролей. Наиболее популярные:

1. Аппаратные или программные токены, которые могут генерировать одноразовые пароли на основании секретного ключа, введенного в них, и текущего времени. Секретные ключи пользователей, являющиеся фактором владения, также хранятся на сервере, что позволяет выполнить проверку введенных одноразовых паролей. Пример аппаратной реализаций токенов — RSA SecurID; программной — приложение Google Authenticator.
2. Случайно генерируемые коды, передаваемые пользователю через SMS или другой канал связи. В этой ситуации фактор владения — телефон пользователя (точнее — SIM-карта, привязанная к определенному номеру).
3. Распечатка или scratch card со списком заранее сформированных одноразовых паролей. Для каждого нового входа в систему требуется ввести новый одноразовый пароль с указанным номером.

Аппаратный токен RSA SecurID генерирует новый код каждые 30 секунд.

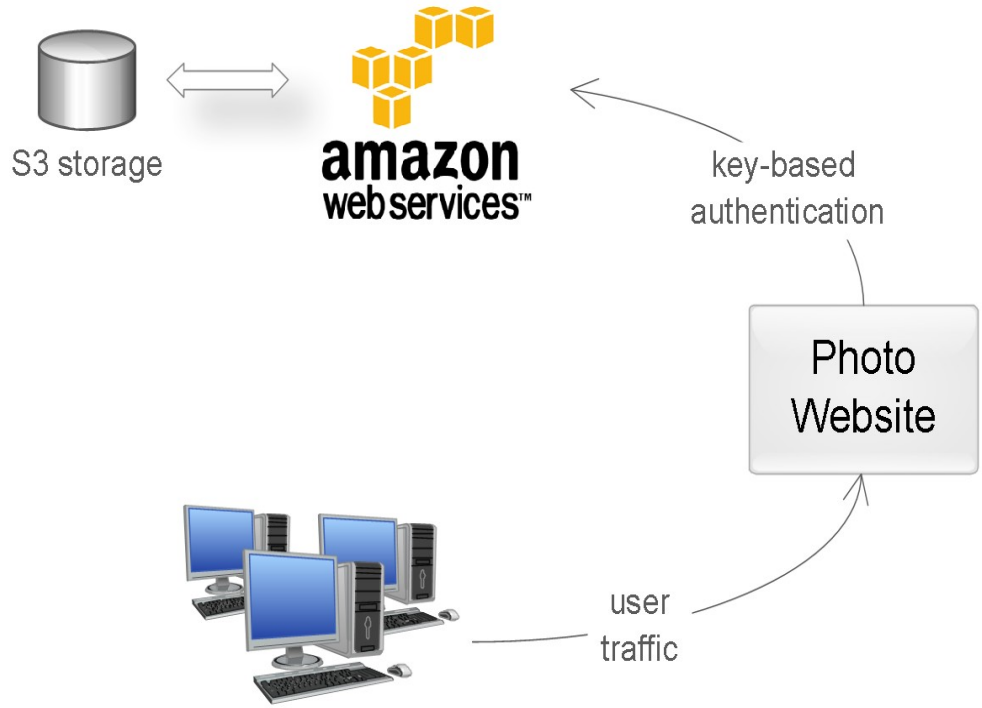
В веб-приложениях такой механизм аутентификации часто реализуется посредством расширения forms authentication: после первичной аутентификации по паролю, создается сессия пользователя, однако в контексте этой сессии пользователь не имеет доступа к приложению до тех пор, пока он не выполнит дополнительную аутентификацию по одноразовому паролю.

Аутентификация по ключам доступа

Этот способ чаще всего используется для аутентификации устройств, сервисов или других приложений при обращении к веб-сервисам. Здесь в качестве секрета применяются ключи доступа (*access key, API key*) — длинные уникальные строки, содержащие произвольный набор символов, по сути заменяющие собой комбинацию username/password.

В большинстве случаев, сервер генерирует ключи доступа по запросу пользователей, которые далее сохраняют эти ключи в клиентских приложениях. При создании ключа также возможно ограничить срок действия и уровень доступа, который получит клиентское приложение при аутентификации с помощью этого ключа.

Хороший пример применения аутентификации по ключу — облако Amazon Web Services. Предположим, у пользователя есть веб-приложение, позволяющее загружать и просматривать фотографии, и он хочет использовать сервис Amazon S3 для хранения файлов. В таком случае, пользователь через консоль AWS может создать ключ, имеющий ограниченный доступ к облаку: только чтение/запись его файлов в Amazon S3. Этот ключ в результате можно применить для аутентификации веб-приложения в облаке AWS.



Пример применения аутентификации по ключу.

Использование ключей позволяет избежать передачи пароля пользователя сторонним приложениям (в примере выше пользователь сохранил в веб-приложении не свой пароль, а ключ доступа). Ключи обладают значительно большей энтропией по сравнению с паролями, поэтому их практически невозможно подобрать. Кроме того, если ключ был раскрыт, это не приводит к компрометации основной учетной записи пользователя — достаточно лишь аннулировать этот ключ и создать новый. С технической точки зрения, здесь не существует единого протокола: ключи могут передаваться в разных частях HTTP-запроса: URL query, request body или HTTP header. Как и в случае аутентификации по паролю, наиболее оптимальный вариант — использование HTTP header. В некоторых случаях используют HTTP-схему Bearer для передачи токена в заголовке (Authorization: Bearer [token]). Чтобы избежать перехвата ключей, соединение с сервером должно быть обязательно защищено протоколом SSL/TLS.

Пример аутентификации по ключу доступа, переданного в HTTP заголовке.

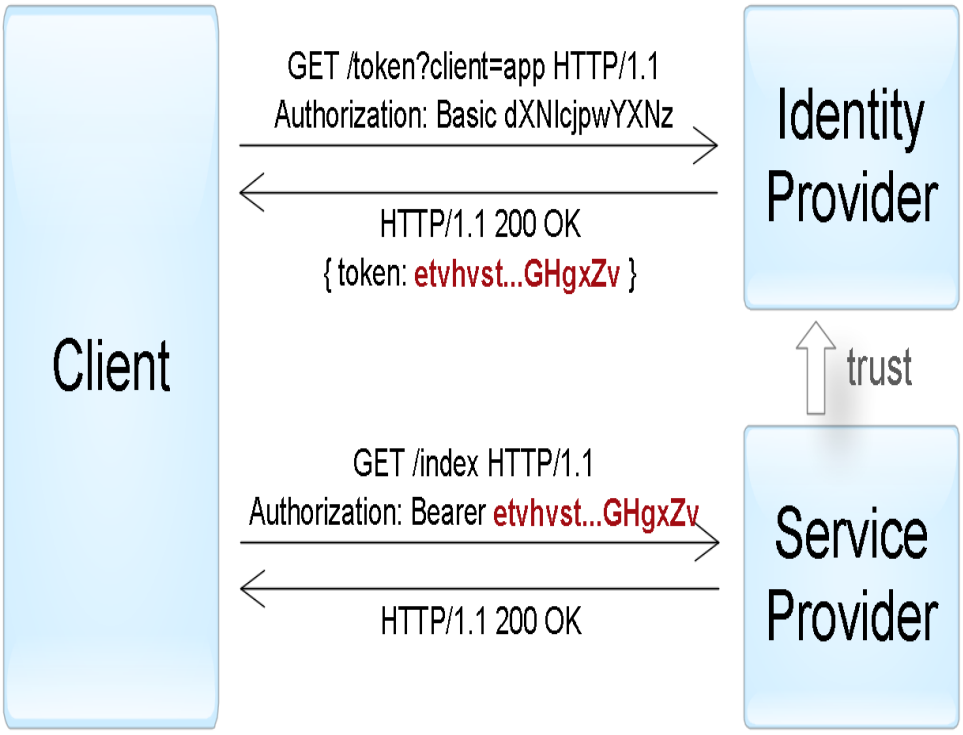
Кроме того, существуют более сложные схемы аутентификации по ключам для незащищенных соединений. В этом случае, ключ обычно состоит их двух частей: публичной и секретной. Публичная часть используется для идентификации клиента, а секретная часть позволяет сгенерировать подпись. Например, по аналогии с digest authentication схемой, сервер может послать клиенту уникальное значение nonce или timestamp, а клиент — возвратить хэш или HMAC этого значения, вычисленный с использованием секретной части ключа. Это позволяет избежать передачи всего ключа в оригинальном виде и защищает от replay attacks.

Аутентификация по токенам

Такой способ аутентификации чаще всего применяется при построении распределенных систем *Single Sign-On* (SSO), где одно приложение (*service provider* или *relying party*) делегирует функцию аутентификации пользователей другому приложению (*identity provider* или *authentication service*). Типичный пример этого способа — вход в приложение через учетную запись в социальных сетях. Здесь социальные сети являются сервисами аутентификации, а приложение доверяет функцию аутентификации пользователей социальным сетям.

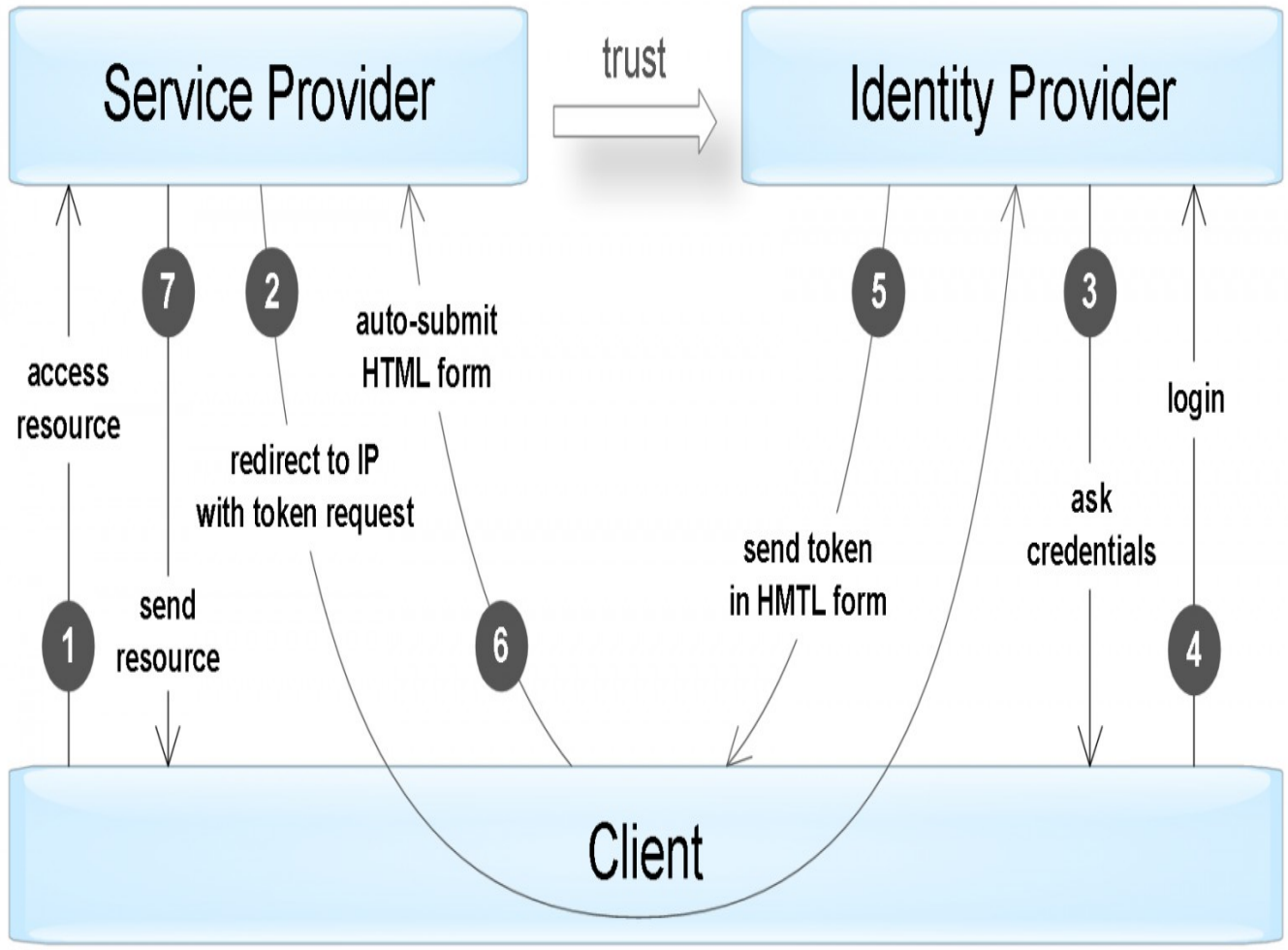
Реализация этого способа заключается в том, что identity provider (IP) предоставляет достоверные сведения о пользователе в виде токена, а service provider (SP) приложение использует этот токен для идентификации, аутентификации и авторизации пользователя. На общем уровне, весь процесс выглядит следующим образом:

1. Клиент аутентифицируется в identity provider одним из способов, специфичным для него (пароль, ключ доступа, сертификат, Kerberos, итд.).
2. Клиент просит identity provider предоставить ему токен для конкретного SP-приложения. Identity provider генерирует токен и отправляет его клиенту.
3. Клиент аутентифицируется в SP-приложении при помощи этого токена.



Пример аутентификации «активного» клиента при помощи токена, переданного посредством Bearer схемы.

Процесс, описанный выше, отражает механизм аутентификации *активного* клиента, т. е. такого, который может выполнять запрограммированную последовательность действий (например, iOS/Android приложения). Браузер же — *пассивный* клиент в том смысле, что он только может отображать страницы, запрошенные пользователем. В этом случае аутентификация достигается посредством автоматического перенаправления браузера между веб-приложениями identity provider и service provider.



Пример аутентификации «пассивного» клиента посредством перенаправления запросов.
Существует несколько стандартов, в точности определяющих протокол взаимодействия между клиентами (активными и пассивными) и IP/SP-приложениями и формат поддерживаемых токенов. Среди наиболее популярных стандартов — OAuth, OpenID Connect, SAML, и WS-Federation. Сам токен обычно представляет собой структуру данных, которая содержит информацию, кто сгенерировал токен, кто может быть получателем токена, срок действия, набор сведений о самом пользователе (claims). Кроме того, токен дополнительно подписывается для предотвращения несанкционированных изменений и гарантий подлинности. При аутентификации с помощью токена SP-приложение должно выполнить следующие проверки: Токен был выдан доверенным identity provider приложением (проверка поля *issuer*).

1. Токен предназначается текущему SP-приложению (проверка поля *audience*).
2. Срок действия токена еще не истек (проверка поля *expiration date*).
3. Токен подлинный и не был изменен (проверка подписи).

В случае успешной проверки SP-приложение выполняет авторизацию запроса на основании данных о пользователе, содержащихся в токене.

Форматы токенов

Существует несколько распространенных форматов токенов для веб-приложений:

1. **Simple Web Token** (SWT) — наиболее простой формат, представляющий собой набор произвольных пар имя/значение в формате кодирования HTML form. Стандарт определяет несколько зарезервированных имен: Issuer, Audience, ExpiresOn и

HMACSHA256. Токен подписывается с помощью симметричного ключа, таким образом оба IP- и SP-приложения должны иметь этот ключ для возможности создания/проверки токена. *Пример SWT токена (после декодирования).*

Issuer=http://auth.myservice.com&
Audience=http://myservice.com&
ExpiresOn=1435937883&
UserName=John Smith&
UserRole=Admin&
HMACSHA256=KOUQRPSpy64rvT2KnYyQKtFFXUIggnesSpE7ADA4o9w

2. **JSON Web Token (JWT)** — содержит три блока, разделенных точками: заголовок, набор полей (claims) и подпись. Первые два блока представлены в JSON-формате и дополнительно закодированы в формат base64. Набор полей содержит произвольные пары имя/значения, притом стандарт JWT определяет несколько зарезервированных имен (iss, aud, exp и другие). Подпись может генерироваться при помощи и симметричных алгоритмов шифрования, и асимметричных. Кроме того, существует отдельный стандарт, отписывающий формат зашифрованного JWT-токена.

   Пример подписанного JWT токена (после декодирования 1 и 2 блоков).

{ «alg»: «HS256», «typ»: «JWT» }.
{ «iss»: «auth.myservice.com», «aud»: «myservice.com», «exp»: «1435937883», «userName»: «John Smith», «userRole»: «Admin» }.
S9Zs/8/uEGGTVVtLggFTizCsMtwOJnRhjaQ2BMUQhcY

3. **Security Assertion Markup Language (SAML)** — определяет токены (SAML assertions) в XML-формате, включающем информацию об эмитенте, о субъекте, необходимые условия для проверки токена, набор дополнительных утверждений (statements) о пользователе. Подпись SAML-токенов осуществляется при помощи ассиметричной криптографии. Кроме того, в отличие от предыдущих форматов, SAML-токены содержат механизм для подтверждения владения токеном, что позволяет предотвратить перехват токенов через man-in-the-middle-атаки при использовании незащищенных соединений.

Стандарт SAML

Стандарт Security Assertion Markup Language (SAML) описывает способы взаимодействия и протоколы между identity provider и service provider для обмена данными аутентификации и авторизации посредством токенов. Изначально версии 1.0 и 1.1 были выпущены в 2002 – 2003 гг., в то время как версия 2.0, значительно расширяющая стандарт и обратно несовместимая, опубликована в 2005 г.
Этот основополагающий стандарт — достаточно сложный и поддерживает много различных сценариев интеграции систем. Основные «строительные блоки» стандарта:

1. **Assertions** — собственный формат SAML токенов в XML формате.
2. **Protocols** — набор поддерживаемых сообщений между участниками, среди которых — запрос на создание нового токена, получение существующих токенов, выход из системы (logout), управление идентификаторами пользователей, и другие.
3. **Bindings** — механизмы передачи сообщений через различные транспортные протоколы. Поддерживаются такие способы, как HTTP Redirect, HTTP POST, HTTP Artifact (ссылка на сообщения), SAML SOAP, SAML URI (адрес получения сообщения) и другие.

4. **Profiles** — типичные сценарии использования стандарта, определяющие набор assertions, protocols и bindings необходимых для их реализации, что позволяет достичь лучшей совместимости. Web Browser SSO — один из примеров таких профилей.

Кроме того, стандарт определяет формат обмена метаинформацией между участниками, которая включает список поддерживаемых ролей, протоколов, атрибутов, ключи шифрования и т. п. Рассмотрим краткий пример использования SAML для сценария Single Sign-On. Пользователь хочет получить доступ на защищенный ресурс сервис-провайдера (шаг № 1 на диаграмме аутентификации пассивных клиентов). Т. к. пользователь не был аутентифицирован, SP отправляет его на сайт identity provider'а для создания токена (шаг № 2). Ниже приведен пример ответа SP, где последний использует SAML HTTP Redirect binding для отправки сообщения с запросом токена:

```
HTTP/1.1 302 Found
Location: https://idp.example.com/SAML/SSO/Browser?SAMLRequest=aQC5kAsTB...3QIX3
f7M&RelayState=kzdeP2qmdr576&SigAlg=http%3A%2F%2Fwww.w3.org%2F200%2F09%2Fxmldsig
%23rsa-sha1&Signature=OPqCEvoc8Vz0WsQdctKbzLBNj74
```

- URI соответствующего сервиса identity provider'а берется из его метаданных.
- SAMLRequest — XML-запрос на создание нового токена (кодировка deflate + base64).
- RelayState — произвольная строка, описывающая состояние SP (будет возвращена в ответе).
- SigAlg — алгоритм подписи сообщения.
- Signature — подпись сообщения (кодировка base64)

В случае такого запроса, identity provider аутентифицирует пользователя (шаги №3-4), после чего генерирует токен. Ниже приведен пример ответа IP с использованием HTTP POST binding (шаг № 5):

```
...
<body onload="document.forms[0].submit()">
<form method="post" action="https://sp.example.com/SAML/SSO/POST">
    <input type="hidden" name="SAMLResponse" value="XHU2KeRbb... 94X/rX4" />
    <input type="hidden" name="RelayState" value="kzdeP2qmdr576" />
    <input type="submit" value="Submit" />
</form>
...
```

- URI соответствующего сервиса service provider'а берется из его метаданных.
- SAMLResponse — XML-ответ, содержащий SAML assertion (кодировка base64).
- RelayState — строка, переданная в параметре RelayState-запроса.

После того как браузер автоматически отправит эту форму на сайт service provider'а (шаг № 6), последний декодирует токен и аутентифицирует пользователя. По результатам успешной авторизации запроса пользователь получает доступ к запрошенному ресурсу (шаг № 7).

Стандарты WS-Trust и WS-Federation

WS-Trust и WS-Federation входят в группу стандартов WS-*, описывающих SOAP/XML-веб сервисы. Эти стандарты разрабатываются группой компаний, куда входят Microsoft, IBM, VeriSign и другие. Наряду с SAML, эти стандарты достаточно сложные, используются преимущественно в корпоративных сценариях.

Стандарт **WS-Trust** описывает интерфейс сервиса авторизации, именуемого Secure Token Service (STS). Этот сервис работает по протоколу SOAP и поддерживает создание,

обновление и аннулирование токенов. При этом стандарт допускает использование токенов различного формата, однако на практике в основном используются SAML-токены.

Стандарт **WS-Federation** касается механизмов взаимодействия сервисов между компаниями, в частности, протоколов обмена токенов. При этом WS-Federation расширяет функции и интерфейс сервиса STS, описанного в стандарте WS-Trust. Среди прочего, стандарт WS-Federation определяет:
Формат и способы обмена метаданными о сервисах.

- Функцию единого выхода из всех систем (single sign-out).
- Сервис атрибутов, предоставляющий дополнительную информацию о пользователе.
- Сервис псевдонимов, позволяющий создавать альтернативные имена пользователей.
- Поддержку пассивных клиентов (браузеров) посредством перенаправления.

Перечень основной литературы

1. Информационная безопасность: учебник для вузов/ В.И. Ярочкин – М.: Академический проект, 2012.

2. Семененко В.А. Информационная безопасность: учеб.пособие/ В.А. Семененко – М.: МГИУ, 2013.

Перечень дополнительной литературы

1. Информационная безопасность: учебник для вузов/ В.И. Ярочкин – М.: Академический проект, 2012.

2. Семененко В.А. Информационная безопасность: учеб.пособие/ В.А. Семененко – М.: МГИУ, 2013.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

Методические рекомендации по выполнению лабораторных работ по дисциплине «Основы управления информационной безопасности ".

2. Методические рекомендации по организации самостоятельной работы студентов по дисциплине " Основы управления информационной безопасности ".

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://el.ncfu.ru/ – система управления обучением ФГАОУ ВО СКФУ. Дистанционная поддержка дисциплины «Информационные технологии в профессиональной деятельности»
2. http://www.un.org - Сайт ООН Информационно-коммуникационные технологии
3. http://www.intuit.ru – Интернет-Университет Компьютерных технологий.

Практическое занятие 6. «Анализ рисков информационной безопасности»

Цель работы: *ознакомиться с алгоритмами оценки риска информационной безопасности*

Рассматриваемые вопросы

- защита коммерческой тайны;
- внутренняя работа с сотрудниками;
- внутренняя контрразведка;

- служебные расследования;
- экономичная безопасность;
- техническая и физическая защита.

1. .

Теоретическая часть

Прежде чем приступать к построению эффективной системы информационной безопасности, необходимо тщательно проанализировать уже существующую на предприятии систему хранения и обработки данных. Есть три основных шага, которые необходимо для этого сделать:

1. Выявление критически важной информации.

2. Выявление слабых мест в корпоративной безопасности.

3. Оценка возможностей защиты этой информации.

Все эти действия можно выполнить либо силами своих сотрудников, либо заказать у специалистов аудит информационной безопасности компании. Преимущества первого способа – более низкая стоимость и, что немаловажно, отсутствие доступа к корпоративным данным для третьих лиц. Однако если в организации нет хороших штатных специалистов по аудиту безопасности, то лучше всего прибегнуть к помощи сторонних компаний – результат будет надежнее. Это поможет избежать наиболее распространенных ошибок в обеспечении информационной безопасности.

При переоценке угроз система безопасности не только тяжким бременем ложится на бюджет предприятия, но и неоправданно затрудняет работникам организации исполнение возложенных на них обязанностей. Это грозит потерями возможной прибыли и утратой конкурентоспособности».

Выявление критически важной информации. На этом этапе происходит определение тех документов и данных, безопасность которых имеет огромное значение для компании, а утечка – несет огромные убытки. Чаще всего к такой информации относятся сведения, составляющие коммерческую тайну, но не только.

Например, после принятия новой редакции федерального закона «О персональных данных» в охране нуждаются и все сведения, собираемые организацией о своих сотрудниках и клиентах. Серия прошлогодних утечек из Мегафона, интернет-магазинов и «РЖД», а также штрафы, полученные виновниками этих инцидентов – лучшее доказательство необходимости защиты такой информации.

Важно помнить: сторонние специалисты-аудиторы не могут самостоятельно составить список всех документов, которые необходимо защищать. Работа аудитора должна выполняться совместно с сотрудником предприятия, хорошо знающим особенности документооборота.

Выявление слабых мест в корпоративной безопасности. Эта задача выполняется непосредственно специалистами, проводящими аудит. От результатов этой работы зависит выбор схемы построения информационной безопасности.

При выявлении брешей в информационной и, как следствие, корпоративной безопасности оцениваются не только технические средства. Очень важный момент – наличие разграничения прав доступа сотрудников к той или иной информации, соглашения о неразглашении корпоративной информации. Важно также оценить лояльность работников к руководству и взаимоотношения в коллективе – всё это входит в обязанности отдела по работе с персоналом.

Недавний пример ситуации, когда штатный сотрудник воспользовался своим положением и похитил информацию – кража кенийским представительством Google сведений о стартапе Mocality (онлайн-база бизнес-информации). Google был вынужден принести официальные извинения пострадавшим, а глава представительства, по вине которого произошёл инцидент, был смещен со своей должности.

Оценка возможностей защиты информации. Это завершающий этап аудита, в ходе которого на основании проведенного анализа составляется список конкретных мер, которые необходимо принять для охраны корпоративных секретов компании. Рекомендации могут носить как технический, так и организационный характер.

Кроме того, на этом этапе анализируются и финансовые возможности компании по защите информации, поскольку многие средства защиты информации могут оказаться слишком дорогими для предприятия. А некоторые из этих мер попросту не целесообразны для малого бизнеса. Особая необходимость в DLP-системе возникает, если в организации используется 50 и более компьютеров.

Установку DLP-системы всегда предваряет технический аудит. После заказа 30-дневного бесплатного триала заказчика консультируют инженеры «СёрчИнформ», которые оценивают ИТ-инфраструктуру компании и определяют, сколько мощностей потребуется для установки программы.

Двусторонняя защита

Информационная безопасность – лишь один из многих способов (пусть и самый важный) обеспечить корпоративную защиту. Необходим комплекс мер – технических и организационных.

К техническим решениям по защите корпоративных секретов относится установка DLP-системы (от англ. Data Leak Prevention – предотвращение утечек данных). Этот комплекс программных средств отслеживает все информационные потоки в организации – от электронной почты до программ, использующих алгоритмы шифрования, (к примеру, Skype) или протокол HTTPS. Под контролем также находятся все съемные носители информации, корпоративные компьютеры и ноутбуки.

Важная особенность DLP-систем – их автономность. Компании нет необходимости содержать целый отдел, который занимался бы информационной безопасностью. Достаточно всего нескольких специалистов.

Последние исследования SearchInform, ведущего игрока на российском рынке информационной безопасности, показали, что сейчас в России и странах СНГ DLP-системы не пользуются большой популярностью. Только чуть более половины организаций (58%) планируют в скором времени установку комплексной защиты. Остальные не считают нужным ее внедрение либо полагают, что достаточно и частичной защиты. Однако, информационная безопасность только тогда будет на оптимальном уровне, когда обеспечена комплексная защита.

DLP-система позволяет не только обеспечить надежную защиту секретов. Их функции намного шире: при правильном подходе можно получить информацию о настроениях сотрудников в коллективе, проследить движение ключевых документов, входящие и исходящие сообщения. Как следствие, использование DLP-систем – это еще и эффективное подспорье в таких важных для корпоративной безопасности мероприятиях, как внутренняя контрразведка или служебное расследование.

Впрочем, одной лишь технической безопасности данных и отслеживания действий сотрудников недостаточно. Важны и организационные мероприятия, работа с сотрудниками, разработка внутренней документации.

«Система корпоративной безопасности должна быть комплексной, иначе будет как в анекдоте: на проходной охранник строго проверяет у работников предприятия пропуска, а через двадцать метров от проходной имеется дырка, через которую на территорию фирмы может проникнуть любой желающий», –делится опытом ***Александр Доронин****.*

Организационная работа включает в себя информирование персонала о наличии в организации систем информационной безопасности, о необходимости соблюдать коммерческую тайну и возможных последствиях ее разглашения, как для компании, так и для самого сотрудника. Создание благоприятной рабочей атмосферы – еще один ключевой момент организационных мер. Корпоративная безопасность невозможна, если сотрудники недоверчиво косятся один на одного. Такая «холодная война» будет изрядно тормозить бизнес-процессы. Поэтому ещё раз стоит напомнить о важной роли отдела по работе с персоналом.

Что касается разработки внутренней документации, то должны быть четко прописаны обязанности работников, а также их права доступа к тем или иным документам. Каждый отдел должен выполнять возложенные на него задачи – не больше, но и не меньше.

Нельзя забывать и о таких, казалось бы, элементарных вещах, как работа службы безопасности. Физическая защита сотрудников на рабочих местах – тоже немаловажная часть корпоративной безопасности.

Только добившись такой двусторонней – технической и организационной – защиты, не преувеличив и не преуменьшив угрозы, можно создать надежную корпоративную защиту компании.

Перечень основной литературы

1. Информационная безопасность: учебник для вузов/ В.И. Ярочкин – М.: Академический проект, 2012.

2. Семененко В.А. Информационная безопасность: учеб.пособие/ В.А. Семененко – М.: МГИУ, 2013.

Перечень дополнительной литературы

1. Информационная безопасность: учебник для вузов/ В.И. Ярочкин – М.: Академический проект, 2012.

2. Семененко В.А. Информационная безопасность: учеб.пособие/ В.А. Семененко – М.: МГИУ, 2013.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

Методические рекомендации по выполнению лабораторных работ по дисциплине «Основы управления информационной безопасности ".

2. Методические рекомендации по организации самостоятельной работы студентов по дисциплине " Основы управления информационной безопасности ".

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://el.ncfu.ru/ – система управления обучением ФГАОУ ВО СКФУ. Дистанционная поддержка дисциплины «Информационные технологии в профессиональной деятельности»
2. http://www.un.org - Сайт ООН Информационно-коммуникационные технологии
3. http://www.intuit.ru – Интернет-Университет Компьютерных технологий.

Практическое занятие 7. «Типовые» каналы утечки информации объектов информатизации ОВД. Условия и факторы, способствующие утечке информации ограниченного доступа. Модели возможных нарушителей».

Цель работы: *ознакомиться с условиями и факторами, способствующими утечке информации ограниченного доступа*

Теоретическая часть

Реализация угроз нарушения информационной безопасности является следствием одного из следующих действий и событий: разглашения конфиденциальной информации, утечки конфиденциальной информации и несанкционированный доступ к защищаемой информации (106). При разглашении или утечке происходит нарушение конфиденциальности информации с ограниченным доступом Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. - М.: Горячая линия-Телеком, 2011..

Утечка конфиденциальной информации - это бесконтрольный выход конфиденциальной информации за пределы ИС или круга лиц, которым она была доверена по службе или стала известна в процессе работы. Эта утечка может быть следствием:

- - разглашения конфиденциальной информации;
- - ухода информации по различным, главным образом техническим, каналам;
- - несанкционированного доступа к конфиденциальной информации различными способами.

Разглашение информации ее владельцем или обладателем есть умышленные или неосторожные действия должностных лиц и пользователей, которым соответствующие сведения в установленном порядке были доверены по службе или по работе, приведшие к ознакомлению с ним лиц, не допущенных к этим сведениям.

Возможен бесконтрольный уход конфиденциальной информации по визуально-оптическим, акустическим, электромагнитным и другим каналам.

К факторам утечки могут, например, относиться:

- - недостаточное знание работниками предприятия правил защиты информации и непонимание (или недопонимание) необходимости их тщательного соблюдения;
- - использование неаттестованных технических средств обработки конфиденциальной информации;
- - слабый контроль за соблюдением правил защиты информации правовыми, организационными и инженерно-техническими мерами.

Несанкционированный доступ (НСД). Это наиболее распространенный вид информационных угроз заключается в получении пользователем доступа к объекту, на который у него нет разрешения в соответствии с принятой в организации политикой безопасности. Обычно самая главная проблема определить, кто и к каким наборам данных должен иметь доступ, а кто нет. Другими словами, необходимо определить термин «несанкционированный».

По характеру, воздействия НСД является активным воздействием, использующим ошибки системы. НСД обращается обычно непосредственно к требуемому набору данных, либо

воздействует на информацию о санкционированном доступе с целью легализации НСД. НСД может быть подвержен любой объект системы. НСД может быть осуществлен как стандартными, так и специально разработанными программными средствами к объектам. защищенность автоматизированный утечка информатизация

Есть и достаточно примитивные пути несанкционированного доступа:

- - хищение носителей информации и документальных отходов;
- - инициативное сотрудничество;
- - склонение к сотрудничеству со стороны взломщика;
- - выпытывание;
- - подслушивание;
- - наблюдение и другие пути.

Любые способы утечки конфиденциальной информации могут привести к значительному материальному и моральному ущербу как для организации, где функционирует ИС, так и для ее пользователей.

Менеджерам следует помнить, что довольно большая часть причин и условий, создающих предпосылки и возможность неправомерного овладения конфиденциальной информацией, возникает из-за элементарных недоработок руководителей организаций и их сотрудников. Например, к причинам и условиям, создающим предпосылки для утечки коммерческих секретов, могут относиться:

- - недостаточное знание работниками организации правил защиты конфиденциальной информации и непонимание необходимости их тщательного соблюдения;
- - использование неаттестованных технических средств обработки конфиденциальной информации;
- - слабый контроль за соблюдением правил защиты информации правовыми организационными и инженерно- техническими мерами и др.

Разглашение и утечка приводит к неправомерному ознакомлению с конфиденциальной информацией при минимальных затратах усилий со стороны злоумышленника. Этому способствуют некоторые не лучшие личностно-профессиональные характеристики и действия сотрудников фирмы, представленные на рис.2 Мандиа К. Защита от вторжений. Расследование компьютерных преступлений. - СПб.: Лори, 2010

И даже если сотрудник не является злоумышленником, он может ошибаться не намеренно вследствие усталости, болезненного состояния и пр.

Ошибочное использование информационных ресурсов, будучи санкционированным, тем не менее, может привести к разрушению, раскрытию. или компрометации указанных ресурсов. Данная угроза, чаще всего, является следствием ошибок в программном обеспечении АИС.

Уничтожение компьютерной информации - это стирание ее в памяти ЭВМ, удаление с физических носителей, а также несанкционированные изменения составляющих ее данных, кардинально меняющие содержание (например, введение ложной информации, добавление, изменение, удаление записей). Одновременный перевод информации на другой машинный носитель не считается в контексте уголовного закона уничтожением компьютерной информации лишь в том случае, если в результате этих действий доступ правомерных пользователей к информации не оказался существенно затруднен либо исключен.

Имеющаяся у пользователя возможность восстановить уничтоженную информацию с помощью средств программного обеспечения или получить данную информацию от другого пользователя не освобождает виновного от ответственности.

Уничтожением информации не является переименование файла, где она содержится, а также само по себе автоматическое "вытеснение" старых версий файлов последними по времени.

Блокирование компьютерной информации - это искусственное затруднение доступа пользователей к компьютерной информации, не связанное с ее уничтожением. Другими словами, это совершение с информацией действий, результатом которых является невозможность получения или использование ее по назначению при полной сохранности самой информации.

Компрометация информации, как правило, реализуется посредством внесения несанкционированных изменений в базы данных, в результате чего ее потребитель вынужден либо отказаться от нее, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений. В случае использования скомпрометированной информации потребитель подвергается опасности принятия неверных решений со всеми вытекающими последствиями.

Отказ от информации, в частности, непризнание транзакции (операции в банке) состоит в непризнании получателем или отправителем информации фактов ее получения или отправки. В условиях маркетинговой деятельности это, в частности, позволяет одной из сторон расторгать заключенные финансовые соглашения "техническим" путем, формально не отказываясь от них и нанося тем самым второй стороне значительный ущерб.

Модификация компьютерной информации - это внесение в нее любых изменений, кроме связанных с адаптацией программы для ЭВМ или базы данных. Адаптация программы для ЭВМ или базы данных - «это внесение изменений, осуществляемых исключительно в целях обеспечения функционирования программы для ЭВМ или базы данных на конкретных технических средствах пользователя или под управлением конкретных программ пользователя» (ч.1 ст.1 Закона РФ от 23 сентября 1992 года "О правовой охране программ для электронных вычислительных машин и баз данных"). Другими словами это означает изменение ее содержания по сравнению с той информацией, которая первоначально (до совершения деяния) была в распоряжении собственника или законного пользователя.

Копирование компьютерной информации - изготовление и устойчивое запечатление второго и последующих экземпляров базы данных, файлов в любой материальной форме, а также их запись на машинный носитель, в память ЭВМ.

Отказ в обслуживании представляет собой весьма существенную и распространенную угрозу, источником которой является сама АИС. Подобный отказ особенно опасен в ситуациях, когда задержка с предоставлением ресурсов абоненту может привести к тяжелым для него последствиям. Так, отсутствие у пользователя данных, необходимых для принятия решения, в течение периода, когда это решение еще может быть эффективно реализовано, может стать причиной его нерациональных действий.

Основными типовыми путями несанкционированного доступа к информации, являются:

- - перехват электронных излучений;
- - принудительное электромагнитное облучение (подсветка) линий связи с целью получения паразитной модуляции;
- - применение подслушивающих устройств (закладок);
- - дистанционное фотографирование;
- - перехват акустических излучений и восстановление текста принтера;

- - хищение носителей информации и документальных отходов;
- - чтение остаточной информации в памяти системы после выполнения санкционированных запросов;
- - копирование носителей информации с преодолением мер защиты;
- - маскировка под зарегистрированного пользователя;
- - мистификация (маскировка под запросы системы);
- - использование программных ловушек;
- - использование недостатков языков программирования и операционных систем;
- - включение в библиотеки программ специальных блоков типа "Троянский конь";
- - незаконное подключение к аппаратуре и линиям связи;
- - злоумышленный вывод из строя механизмов защиты;
- - внедрение и использование компьютерных вирусов.

Необходимо отметить, что особую опасность в настоящее время представляет проблема компьютерных вирусов, ибо эффективной защиты против них разработать не удалось. Остальные пути несанкционированного доступа поддаются надежной блокировке при правильно разработанной и реализуемой на практике системе обеспечения безопасности

Ниже перечисляются наиболее распространенные технические угрозы и причины, в результате которых они реализуются:

- - несанкционированный доступ к информационной системе - происходит в результате получения нелегальным пользователем доступа к информационной системе;
- - раскрытие данных - наступает в результате получения доступа к информации или ее чтения человеком и возможного раскрытия им информации случайным или намеренным образом;
- - несанкционированная модификация данных и программ - возможна в результате модификации, удаления или разрушения человеком данных и программного обеспечения локальных вычислительных сетей случайным или намеренным образом;
- - раскрытие трафика локальных вычислительных сетей - произойдет в результате доступа к информации или ее чтения человеком и возможного ее разглашения случайным или намеренным образом тогда, когда информация передается через локальные вычислительные сети;
- - подмена трафика локальных вычислительных сетей - это его использование легальным способом, когда появляются сообщения, имеющие такой вид, будто они посланы законным заявленным отправителем, а на самом деле это не так;
- - неработоспособность локальных вычислительных сетей - это следствие осуществления угроз, которые не позволяют ресурсам локальных вычислительных сетей быть своевременно доступными.

Способы воздействия угроз на информационные объекты подразделяются на:

- - информационные;
- - программно-математические;
- - физические;
- - радиоэлектронные;
- - организационно-правовые.

Реализация угроз нарушения информационной безопасности является следствием одного из следующих действий и событий: разглашения конфиденциальной информации, утечки конфиденциальной информации и несанкционированный доступ к защищаемой информации (106). При разглашении или утечке происходит нарушение конфиденциальности информации с ограниченным доступом Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. - М.: Горячая линия-Телеком, 2011..

Утечка конфиденциальной информации - это бесконтрольный выход конфиденциальной информации за пределы ИС или круга лиц, которым она была доверена по службе или стала известна в процессе работы. Эта утечка может быть следствием:

- - разглашения конфиденциальной информации;
- - ухода информации по различным, главным образом техническим, каналам;
- - несанкционированного доступа к конфиденциальной информации различными способами.

Разглашение информации ее владельцем или обладателем есть умышленные или неосторожные действия должностных лиц и пользователей, которым соответствующие сведения в установленном порядке были доверены по службе или по работе, приведшие к ознакомлению с ним лиц, не допущенных к этим сведениям.

Возможен бесконтрольный уход конфиденциальной информации по визуально-оптическим, акустическим, электромагнитным и другим каналам.

К факторам утечки могут, например, относиться:

- - недостаточное знание работниками предприятия правил защиты информации и непонимание (или недопонимание) необходимости их тщательного соблюдения;
- - использование неаттестованных технических средств обработки конфиденциальной информации;
- - слабый контроль за соблюдением правил защиты информации правовыми, организационными и инженерно-техническими мерами.

Несанкционированный доступ (НСД). Это наиболее распространенный вид информационных угроз заключается в получении пользователем доступа к объекту, на который у него нет разрешения в соответствии с принятой в организации политикой безопасности. Обычно самая главная проблема определить, кто и к каким наборам данных должен иметь доступ, а кто нет. Другими словами, необходимо определить термин «несанкционированный».

По характеру, воздействия НСД является активным воздействием, использующим ошибки системы. НСД обращается обычно непосредственно к требуемому набору данных, либо воздействует на информацию о санкционированном доступе с целью легализации НСД. НСД может быть подвержен любой объект системы. НСД может быть осуществлен как стандартными, так и специально разработанными программными средствами к объектам. защищенность автоматизированный утечка информатизация

Есть и достаточно примитивные пути несанкционированного доступа:

- - хищение носителей информации и документальных отходов;
- - инициативное сотрудничество;
- - склонение к сотрудничеству со стороны взломщика;
- - выпытывание;
- - подслушивание;
- - наблюдение и другие пути.

Любые способы утечки конфиденциальной информации могут привести к значительному материальному и моральному ущербу как для организации, где функционирует ИС, так и для ее пользователей.

Менеджерам следует помнить, что довольно большая часть причин и условий, создающих предпосылки и возможность неправомерного овладения конфиденциальной информацией, возникает из-за элементарных недоработок руководителей организаций и их сотрудников. Например, к причинам и условиям, создающим предпосылки для утечки коммерческих секретов, могут относиться:

- - недостаточное знание работниками организации правил защиты конфиденциальной информации и непонимание необходимости их тщательного соблюдения;
- - использование неаттестованных технических средств обработки конфиденциальной информации;
- - слабый контроль за соблюдением правил защиты информации правовыми организационными и инженерно- техническими мерами и др.

Разглашение и утечка приводит к неправомерному ознакомлению с конфиденциальной информацией при минимальных затратах усилий со стороны злоумышленника. Этому способствуют некоторые не лучшие личностно-профессиональные характеристики и действия сотрудников фирмы, представленные на рис.2 Мандиа К. Защита от вторжений. Расследование компьютерных преступлений. - СПб.: Лори, 2010

И даже если сотрудник не является злоумышленником, он может ошибаться не намеренно вследствие усталости, болезненного состояния и пр.

Ошибочное использование информационных ресурсов, будучи санкционированным, тем не менее, может привести к разрушению, раскрытию. или компрометации указанных ресурсов. Данная угроза, чаще всего, является следствием ошибок в программном обеспечении АИС.

Уничтожение компьютерной информации - это стирание ее в памяти ЭВМ, удаление с физических носителей, а также несанкционированные изменения составляющих ее данных, кардинально меняющие содержание (например, введение ложной информации, добавление, изменение, удаление записей). Одновременный перевод информации на другой машинный носитель не считается в контексте уголовного закона уничтожением компьютерной информации лишь в том случае, если в результате этих действий доступ правомерных пользователей к информации не оказался существенно затруднен либо исключен.

Имеющаяся у пользователя возможность восстановить уничтоженную информацию с помощью средств программного обеспечения или получить данную информацию от другого пользователя не освобождает виновного от ответственности.

Уничтожением информации не является переименование файла, где она содержится, а также само по себе автоматическое "вытеснение" старых версий файлов последними по времени.

Блокирование компьютерной информации - это искусственное затруднение доступа пользователей к компьютерной информации, не связанное с ее уничтожением. Другими словами, это совершение с информацией действий, результатом которых является невозможность получения или использование ее по назначению при полной сохранности самой информации.

Компрометация информации, как правило, реализуется посредством внесения несанкционированных изменений в базы данных, в результате чего ее потребитель вынужден либо отказаться от нее, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений. В случае использования скомпрометированной информации потребитель подвергается опасности принятия неверных решений со всеми вытекающими последствиями.

Отказ от информации, в частности, непризнание транзакции (операции в банке) состоит в непризнании получателем или отправителем информации фактов ее получения или отправки. В условиях маркетинговой деятельности это, в частности, позволяет одной из сторон расторгать заключенные финансовые соглашения "техническим" путем, формально не отказываясь от них и нанося тем самым второй стороне значительный ущерб.

Модификация компьютерной информации - это внесение в нее любых изменений, кроме связанных с адаптацией программы для ЭВМ или базы данных. Адаптация программы для ЭВМ или базы данных - «это внесение изменений, осуществляемых исключительно в целях обеспечения функционирования программы для ЭВМ или базы данных на конкретных технических средствах пользователя или под управлением конкретных программ пользователя» (ч.1 ст.1 Закона РФ от 23 сентября 1992 года "О правовой охране программ для электронных вычислительных машин и баз данных"). Другими словами это означает изменение ее содержания по сравнению с той информацией, которая первоначально (до совершения деяния) была в распоряжении собственника или законного пользователя.

Копирование компьютерной информации - изготовление и устойчивое запечатление второго и последующих экземпляров базы данных, файлов в любой материальной форме, а также их запись на машинный носитель, в память ЭВМ.

Отказ в обслуживании представляет собой весьма существенную и распространенную угрозу, источником которой является сама АИС. Подобный отказ особенно опасен в ситуациях, когда задержка с предоставлением ресурсов абоненту может привести к тяжелым для него последствиям. Так, отсутствие у пользователя данных, необходимых для принятия решения, в течение периода, когда это решение еще может быть эффективно реализовано, может стать причиной его нерациональных действий.

Основными типовыми путями несанкционированного доступа к информации, являются:

- - перехват электронных излучений;
- - принудительное электромагнитное облучение (подсветка) линий связи с целью получения паразитной модуляции;
- - применение подслушивающих устройств (закладок);
- - дистанционное фотографирование;
- - перехват акустических излучений и восстановление текста принтера;
- - хищение носителей информации и документальных отходов;
- - чтение остаточной информации в памяти системы после выполнения санкционированных запросов;
- - копирование носителей информации с преодолением мер защиты;
- - маскировка под зарегистрированного пользователя;
- - мистификация (маскировка под запросы системы);
- - использование программных ловушек;
- - использование недостатков языков программирования и операционных систем;
- - включение в библиотеки программ специальных блоков типа "Троянский конь";
- - незаконное подключение к аппаратуре и линиям связи;
- - злоумышленный вывод из строя механизмов защиты;
- - внедрение и использование компьютерных вирусов.

Необходимо отметить, что особую опасность в настоящее время представляет проблема компьютерных вирусов, ибо эффективной защиты против них разработать не удалось. Остальные пути несанкционированного доступа поддаются надежной блокировке при правильно разработанной и реализуемой на практике системе обеспечения безопасности

Ниже перечисляются наиболее распространенные технические угрозы и причины, в результате которых они реализуются:

- - несанкционированный доступ к информационной системе - происходит в результате получения нелегальным пользователем доступа к информационной системе;
- - раскрытие данных - наступает в результате получения доступа к информации или ее чтения человеком и возможного раскрытия им информации случайным или намеренным образом;
- - несанкционированная модификация данных и программ - возможна в результате модификации, удаления или разрушения человеком данных и программного обеспечения локальных вычислительных сетей случайным или намеренным образом;
- - раскрытие трафика локальных вычислительных сетей - произойдет в результате доступа к информации или ее чтения человеком и возможного ее разглашения случайным или намеренным образом тогда, когда информация передается через локальные вычислительные сети;
- - подмена трафика локальных вычислительных сетей - это его использование легальным способом, когда появляются сообщения, имеющие такой вид, будто они посланы законным заявленным отправителем, а на самом деле это не так;
- - неработоспособность локальных вычислительных сетей - это следствие осуществления угроз, которые не позволяют ресурсам локальных вычислительных сетей быть своевременно доступными.

Способы воздействия угроз на информационные объекты подразделяются на:

- - информационные;
- - программно-математические;
- - физические;
- - радиоэлектронные;
- - организационно-правовые.

Перечень основной литературы

1. Информационная безопасность: учебник для вузов/ В.И. Ярочкин – М.: Академический проект, 2012.

2. Семененко В.А. Информационная безопасность: учеб.пособие/ В.А. Семененко – М.: МГИУ, 2013.

Перечень дополнительной литературы

1. Информационная безопасность: учебник для вузов/ В.И. Ярочкин – М.: Академический проект, 2012.

2. Семененко В.А. Информационная безопасность: учеб.пособие/ В.А. Семененко – М.: МГИУ, 2013.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

Методические рекомендации по выполнению лабораторных работ по дисциплине «Основы управления информационной безопасности ".

2. Методические рекомендации по организации самостоятельной работы студентов по дисциплине " Основы управления информационной безопасности ".

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://el.ncfu.ru/ – система управления обучением ФГАОУ ВО СКФУ. Дистанционная поддержка дисциплины «Информационные технологии в профессиональной деятельности»
2. http://www.un.org - Сайт ООН Информационно-коммуникационные технологии
3. http://www.intuit.ru – Интернет-Университет Компьютерных технологий.

.

Практическое занятие 8. Тема: «Предварительный анализ информационной безопасности предприятия»

Цель работы*: Изучить деятельность определенной организации и провести предварительный анализ ее информационной безопасности*.

Теоретическая часть

Организации, бизнес которых во многом зависит от информационной сферы, для достижения целей бизнеса должны поддерживать на необходимом уровне систему обеспечения ИБ (СОИБ). СОИБ представляет собой совокупность аппаратно-программных, технических и организационных защитных мер (ЗМ), функционирующих под управлением СМИБ и процессов осознания ИБ, инициирующих и поддерживающих деятельность по менеджменту ИБ.

Желание иметь СОИБ, адекватную целям ИБ организации по обеспечению доступности, целостности и конфиденциальности информационных активов, приводит к стремлению совершенствовать СОИБ. Совершенствование, улучшение СОИБ возможно при условии знания состояний характеристик и параметров используемых ЗМ, процессов менеджмента, осознания ИБ и понимания степени их соответствия требуемым результатам. Понять эти аспекты СОИБ можно только по результатам оценки ИБ организации, полученной с помощью модели оценки ИБ на основании свидетельств оценки, критериев оценки и с учетом контекста оценки.

Критерии оценки — это все то, что позволяет установить значения оценки для объекта оценки. В качестве критериев оценки ИБ могут использоваться требования ИБ, процедуры ИБ, сочетание требований и процедур ИБ, уровень инвестиций, затрат на ИБ.

К свидетельствам оценки ИБ относятся записи, изложение фактов или любая информация, которая имеет отношение к критериям оценки ИБ и может быть проверена. Такими свидетельствами оценки ИБ могут быть доказательства выполняемой и выполненной деятельности по обеспечению ИБ в виде отчетных, нормативных, распорядительных документов, результатов опросов, наблюдений.

Контекст оценки ИБ объединяет цели и назначение оценки ИБ, вид оценки (независимая оценка, самооценка), объект и области оценки ИБ, ограничения оценки и роли.

Модель оценки ИБ определяет сферу оценки, отражающую контекст оценки ИБ в рамках критерия оценки ИБ, отображение и преобразование оценки в параметры объекта оценки, а также устанавливает показатели, обеспечивающие оценку ИБ в сфере оценки.

В общем виде процесс проведения оценки ИБ (рисунок 1) представлен основными компонентами процесса: контекст, свидетельства, критерии и модель оценки — необходимыми для реализации процесса оценки.

Оценка ИБ заключается в выработке оценочного суждения относительно пригодности (зрелости) процессов обеспечения ИБ, адекватности используемых защитных мер или целесообразности (достаточности) инвестиций (затрат) для обеспечения необходимого уровня ИБ на основе измерения и оценивания критических элементов (факторов) объекта оценки.

Рисунок 1 — Общий вид процесса оценки ИБ организации

Наряду с важнейшим назначением оценки ИБ — создание информационной потребности для совершенствования ИБ, возможны и другие цели проведения оценки ИБ, такие как:

– определение степени соответствия установленным критериям отдельных областей обеспечения ИБ, процессов обеспечения ИБ, защитных мер;

– выявление влияния критических элементов (факторов) и их сочетания на ИБ организации;

– сравнение зрелости различных процессов обеспечения ИБ и сравнение степени соответствия различных защитных мер установленным требованиям.

Результаты оценки ИБ организации могут также использоваться заинтересованной стороной для сравнения уровня ИБ организаций с одинаковым бизнесом и сопоставимым масштабом.

Способ оценки ИБ по эталону сводится к сравнению деятельности и мер по обеспечению ИБ организации с требованиями, закрепленными в эталоне. По сути дела проводится оценка соответствия СОИБ организации установленному эталону. Под оценкой соответствия ИБ организации установленным критериям понимается деятельность, связанная с прямым или косвенным определением выполнения или невыполнения соответствующих требований ИБ в организации. С помощью оценки соответствия ИБ измеряется правильность реализации процессов системы обеспечения ИБ организации и идентифицируются недостатки такой реализации.

В результате проведения оценки ИБ должна быть сформирована оценка степени соответствия СОИБ эталону, в качестве которого могут быть приняты (в совокупности и отдельно):

– требования законодательства Российской Федерации в области ИБ;

– отраслевые требования по обеспечению ИБ;

– требования нормативных, методических и организационно-распорядительных документов по обеспечению ИБ;

– требования национальных и международных стандартов в области ИБ.

Основные этапы оценки информационной безопасности по эталону включают выбор эталона и формирование на его основе критериев оценки ИБ, сбор свидетельств оценки и измерение критических элементов (факторов) объекта оценки, формирование оценки ИБ.

Риск-ориентированная оценка ИБ организации представляет собой способ оценки, при котором рассматриваются риски ИБ, возникающие в информационной сфере организации, и сопоставляются существующие риски ИБ и принимаемые меры по их обработке. В результате должна быть сформирована оценка способности организации эффективно управлять рисками ИБ для достижения своих целей.

Основные этапы риск-ориентированной оценки информационной безопасности включают идентификацию рисков ИБ, определение адекватных процессов менеджмента рисков и ключевых индикаторов рисков ИБ, формирование на их основе критериев оценки ИБ, сбор свидетельств оценки и измерение риск-факторов, формирование оценки ИБ.

Способ оценки ИБ на основе экономических показателей оперирует понятными для бизнеса аргументами о необходимости обеспечения и совершенствования ИБ. Для проведения оценки в качестве критериев эффективности СОИБ используются, например, [**2**], показатели совокупной стоимости владения (Total Cost of Ownership — TCO).

Под показателем TCO понимается сумма прямых и косвенных затрат на внедрение, эксплуатацию и сопровождение СОИБ. Под прямыми затратами понимаются все материальные затраты, такие как покупка оборудования и программного обеспечения, трудозатраты соответствующих категорий сотрудников. Косвенными являются все затраты на обслуживание СОИБ, а также потери от произошедших инцидентов. Сбор и анализ статистики по структуре прямых и косвенных затрат проводится, как правило, в течение года. Полученные данные оцениваются по ряду критериев с показателями TCO аналогичных организаций отрасли.

Оценка на основе показателя TCO позволяет оценить затраты на информационную безопасность и сравнить ИБ организации с типовым профилем защиты, а также управлять затратами для достижения требуемого уровня защищенности.

Основные этапы оценки эффективности СОИБ на основе модели ТСО включают сбор данных о текущем уровне ТСО, анализ областей обеспечения ИБ, выбор сравнимой модели ТСО в качестве критерия оценки, сравнение показателей с критерием оценки, формирование оценки ИБ.

Однако этот способ оценки требует создания общей информационной базы данных об эффективности СОИБ организаций схожего бизнеса и постоянной поддержки базы данных в актуальном состоянии. Такое информационное взаимодействие организаций, как правило, не соответствует целям бизнеса. Поэтому оценка ИБ на основе показателя ТСО практически не применяется.

Далее рассмотрим подробнее способ оценки ИБ на основе эталона и способ риск-ориентированной оценки ИБ.

Процесс оценки информационной безопасности

Основные элементы процесса оценки

Процесс оценки ИБ включает следующие элементы проведения оценки:

– контекст оценки, который определяет входные данные: цели и назначение оценки ИБ, вид оценки (независимая оценка, самооценка), объект и области оценки ИБ, ограничения оценки и роли;

– критерии оценки;

– модель оценки;

– мероприятия процесса оценки: сбор свидетельств оценки и проверка их достоверности, измерение и оценивание атрибутов объекта оценки;

– выходные данные оценки.

Основные элементы процесса оценки ИБ [3] представлены на рисунке 3 в виде процессной модели.

Прежде чем рассмотреть особенности способов оценки ИБ организации, необходимо описать общие для любой оценки ИБ компоненты: контекст оценки, сбор свидетельств оценки и проверка их достоверности, измерение и оценивание атрибутов при проведении оценки различного вида (независимая оценка, самооценка) и выходные данные оценки. Модель оценки и критерии оценки, определяющие особенности способов оценки, будут рассмотрены в других разделах.

Контекст оценки информационной безопасности организации

Контекст оценки ИБ включает цели и назначение оценки ИБ, вид оценки, объект и области оценки ИБ, ограничения оценки, роли.

К ролям, участвующим в реализации процесса оценки, относятся организатор, аналитик, руководитель группы оценки, оценщик, владелец активов, представитель объекта оценки.

Организатор (заказчик) оценки ИБ формирует цель оценки (совершенствование объекта оценки, определение соответствия объекта оценки установленным критериям и т.д.) и определяет критерий оценки, объект и область оценки. Под организатором оценки понимается лицо или организация, являющиеся внутренними или внешними по отношению к оцениваемому объекту оценки, которые организуют проведения оценки и предоставляют финансовые и другие ресурсы, необходимые для ее проведения. Организатор должен обеспечить доступ группы оценки (руководитель группы оценки, оценщик) к активам объекта оценки для изучения, к персоналу для проведения опросов, к инфраструктуре, необходимой во время оценивания. Хотя руководство объекта оценки напрямую не имеет никаких конкретных обязанностей по проведению оценивания, осознание важности оценки имеет очень большое значение. Это особенно актуально в том случае, когда организатор оценки не является членом руководства объекта оценки.

По завершении оценки организатор передает отчетные документы по оценке заинтересованным сторонам для использования их в соответствии с заявленной целью оценки.

Аналитик оценки ИБ выбирает способ оценки ИБ, модель оценки и определяет методическое и информационное обеспечение оценки, т.е. методики, данные для оценки. Аналитик оценки анализирует результаты оценки и формирует отчет и рекомендации по результатам оценки ИБ.

Руководитель группы оценки и оценщик измеряют и оценивают свидетельства оценки, предоставленные владельцами активов, и формируют результаты оценки. Руководитель группы должен распределить ответственность между членами группы за оценивание конкретных процессов, подразделений, областей или видов деятельности объекта оценки. Такое распределение должно учитывать потребность в независимости, компетентности специалистов по оценке и результативном использовании ресурсов. Мероприятия по измерению и оцениванию выполняются исключительно руководителем группы оценки и оценщиком, входящими в группу оценки. Другой персонал (представитель объекта оценки, технический эксперт) может участвовать в работе группы оценки для обеспечения специализированных знаний или консультаций. Они могут обсуждать с оценщиком формулировки суждений, но не будут нести ответственность за окончательную оценку.

Важным аспектом при определении контекста оценки является вид оценки: независимая или самооценка. В зависимости от вида оценки различается отношение ролей процесса оценки и объекта оценки.

Независимая оценка достигается путем проведения оценки группой оценки, члены которой независимы от объекта оценки. Организатор оценки может относиться к той же организации, к которой относится объект оценки, но не обязательно к оцениваемому объекту оценки. Степень независимости может варьироваться в соответствии с целью и областью оценки. В случае внешнего организатора оценки предполагается наличие взаимного соглашения между организатором оценки и организацией, к которой относится объект оценки. Представитель объекта оценки принимает участие в формировании свидетельств оценки, обеспечивает взаимодействие группы оценки с владельцами активов. Их участие в проведении оценки дает возможность определить и учесть особенности объекта оценки, обеспечить достоверность результатов оценки.

Самооценка выполняется организацией с целью оценки собственной СОИБ. Организатор самооценки обычно входит в состав объекта оценки, как и члены группы оценки.

Область оценки может включать, например, один или несколько процессов объекта оценки, например, организатор может сосредоточить внимание на одном или нескольких критических процессах и/или защитных мерах. Выбор объекта оценки должен отражать намеченное использование организатором выходных данных оценки. Например, если выходные данные предназначены для использования при совершенствовании деятельности по обеспечению ИБ, то область оценки должна соответствовать области намеченных работ по совершенствованию. Область оценки может быть любой: от отдельного процесса до всей организации. В контексте оценки должно быть представлено подробное описание объекта оценки, включающее размеры объекта оценки, область применения продуктов или услуг объекта оценки, основные характеристики (например, объем, критичность, сложность и качество) продуктов или услуг объекта оценки.

К ограничениям оценки можно отнести возможную недоступность основных активов, используемых в обычной деловой деятельности организации; недостаточный временной интервал, выделенный для проведения оценивания; необходимость исключения определенных частей объекта оценки из-за стадии жизненного цикла. Кроме того, могут быть наложены ограничения на количество и вид данных, которые должны быть собраны и изучены.

Содержание контекста оценки должно быть согласовано руководителем группы оценки с организатором и уполномоченным представителем объекта оценки и задокументировано до начала процесса оценки. Фиксирование контекста оценки важно, так как он содержит исходные элементы процесса оценки.

Во время выполнения оценки могут происходить изменения в контексте оценки. Изменения должны быть одобрены организатором оценки и уполномоченным представителем объекта оценки. Если эти изменения оказывают влияние на временной график и ресурсы проведения оценки, то планирование оценки должно быть соответствующим образом пересмотрено.

Мероприятия и выходные данные процесса оценки

Сбор свидетельств оценки и проверка их достоверности.

Назначение мероприятия: сбор свидетельств оценки с соблюдением условий обеспечения достоверной оценки ИБ.

Независимая оценка ИБ может быть осуществлена с помощью внутреннего и внешнего аудита ИБ. В [**4**] аудит ИБ определяется как систематический, независимый и документируемый процесс получения свидетельств деятельности организации по обеспечению ИБ, установления степени выполнения в

организации критериев ИБ, а также допускающий возможность формирования профессионального аудиторского суждения об информационной безопасности организации.

Необходимыми условиями обеспечения достоверной оценки ИБ при проведении аудита являются:

– использование доверенного процесса аудита и соблюдение основных принципов аудита;

– менеджмент программы аудита ИБ;

– использование наиболее достоверных источников свидетельств оценки;

– определение объема выборки с учетом заданной достоверности свидетельств оценки;

– учет факторов, влияющих на аудиторский риск, с целью снижения аудиторского риска.

Доверенный процесс аудита ИБ должен отвечать требованиям принятого в организации нормативного документа, описывающего процесс аудита ИБ, либо требованиям признаваемого сообществом международного (национального) нормативного документа (стандарта, рекомендации). Таким нормативным документом для банковской системы РФ является СТО БР ИББС–1.1–2007 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности», принятый и введенный в действие Распоряжением Банка России от 28 апреля 2007 года №Р-345. В стандарте изложены принципы проведения аудита ИБ организации, описана последовательность этапов проведения аудита ИБ, установлены требования к этапам проведения аудита ИБ организаций и к взаимоотношениям представителей аудиторской организации с представителями проверяемой организации.

В СТО БР ИББС–1.1–2007 изложено также содержание программы аудита ИБ, включающей деятельность, необходимую для планирования и организации определенного количества и вида аудитов и обеспечения их ресурсами, необходимыми для эффективного и результативного проведения аудитов в заданные сроки. В стандарте определены процедуры менеджмента программы аудита ИБ, направленные на контроль внедрения программы аудита ИБ, анализ достижения целей программы аудита ИБ и определение возможностей для ее совершенствования. Совершенствование программы аудита ИБ состоит в определении корректирующих и превентивных действий по совершенствованию программы аудита ИБ, включающих в себя пересмотр и корректировку сроков проведения аудитов ИБ и необходимых ресурсов, улучшение методов подготовки свидетельств аудита ИБ.

К основным принципам проведения аудита ИБ [**5**] относятся:

– независимость аудита ИБ.

Аудиторы (группа оценки) независимы в своей деятельности и неответственны за деятельность, которая подвергается аудиту ИБ. Независимость является основанием для беспристрастности при проведении аудита ИБ и объективности при формировании заключения по результатам аудита ИБ;

– полнота аудита ИБ.

Аудит ИБ должен охватывать все области аудита ИБ, соответствующие цели оценки. Кроме того, полнота аудита ИБ определяется достаточностью затребованных и предоставленных материалов, документов и уровнем их соответствия поставленным задачам. Полнота аудита ИБ является необходимым условием для формирования объективных заключений по результатам оценки ИБ;

– оценка на основе свидетельств аудита ИБ.

При периодическом проведении аудита ИБ оценка на основе свидетельств аудита ИБ является единственным способом, позволяющим получить повторяемое заключение по результатам аудита ИБ, что повышает доверие к такому заключению. Для повторяемости заключения свидетельства аудита ИБ должны быть проверяемыми;

– достоверность свидетельств аудита ИБ.

Оценщики должны быть уверены в достоверности свидетельств оценки ИБ. Доверие к документальным свидетельствам оценки ИБ повышается при подтверждении их достоверности третьей стороной или руководством организации. Доверие к фактам, полученным при опросе сотрудников объекта оценки, повышается при подтверждении данных фактов из различных источников. Доверие к фактам, полученным при наблюдении за деятельностью в области ИБ объекта оценки, повышается, если они получены непосредственно при функционировании проверяемых процедур или процессов;

– компетентность и этичность поведения.

Доверие к процессу и результатам оценки ИБ зависит от компетентности тех, кто проводит аудит ИБ, и от этичности их поведения. Компетентность базируется на способности аудитора применять знания и навыки. Этичность поведения подразумевает ответственность, неподкупность, умение хранить тайну, беспристрастность.

Соблюдение принципов проведения аудита ИБ является предпосылкой для объективных заключений по результатам оценки.

Основными методами получения свидетельств оценки должны быть:

– проверка и анализ документов, относящихся к объекту оценки;

– наблюдение за процессами объекта оценки;

– опрос сотрудников объекта оценки и независимой (третьей) стороны.

Наряду с ручными способами сбора информации формирование свидетельств аудита может быть автоматическим или полуавтоматическим в результате применения какого-то инструментального средства или применения нескольких инструментальных средств.

При сборе данных оценщики должны исходить из того, что деятельность по обеспечению ИБ в области оценки осуществляется в соответствии с критериями оценки ИБ, если этому есть доказательства. Оценщики должны проявлять достаточную степень профессионального скептицизма в отношении собираемых свидетельств оценки, принимая во внимание возможность наличия нарушений ИБ.

Проверка и анализ документов позволяют оценщику получить свидетельства оценки, обладающие наибольшей полнотой и удобством восприятия и использования по сравнению с другими методами получения свидетельств аудита. Однако эти свидетельства аудита имеют различную степень достоверности в зависимости от их характера и источника, а также от эффективности контроля за процессом подготовки и обработки представленных документов.

Свидетельствами оценки ИБ, полученными в результате проверки и анализа документов, могут быть, например:

– наличие документа (документов) с релевантным содержанием;

– выдержки из документа (документов), подтверждающие реализацию деятельности по обеспечению ИБ, возложение ответственности и обязанностей на сотрудника (сотрудников) за реализацию деятельности по обеспечению ИБ;

– выдержки из документа (документов), содержащие описания реализованных ЗМ, процессов обеспечения ИБ.

Наблюдение представляет собой отслеживание оценщиком процедур или процессов обеспечения ИБ, выполняемых другими лицами (в т.ч. персоналом организации). Информация считается достоверной только в том случае, если она получена непосредственно в момент функционирования проверяемых процедур или процессов.

Свидетельствами аудита, полученными с помощью наблюдения за деятельностью, могут быть, например, записи, факты или другая информация, имеющие отношение к результатам автоматического контроля техническими средствами, зафиксированные оценщиками в ходе наблюдения.

Устный опрос проводят оценщики среди сотрудников (владельцев активов), утвержденных представителем объекта оценки для предоставления источников свидетельств и свидетельств оценки. Результаты устных опросов должны оформляться в виде протокола или краткого конспекта, в котором обязательно должны быть указаны фамилия, имя, отчество оценщика, проводившего опрос, фамилия, имя, отчество опрашиваемого лица, а также их подписи. Для проведения типовых опросов могут быть подготовлены бланки с перечнями интересующих вопросов. Результаты устного опроса следует проверять, так как опрашиваемый может выражать свое субъективное мнение.

Свидетельствами аудита, полученными при проведении опроса, могут быть, например, описания и разъяснения опрашиваемых лиц по реализации процессов, процедур по обеспечению ИБ.

Для уверенности в достоверности оценки оценщики должны быть уверены в достоверности выявленных свидетельств аудита. Собранные свидетельства оценки, используемые для оценивания показателей, должны быть точным представлением оцениваемого объекта оценки. Для этого следует учитывать достоверность источников свидетельств аудита.

По степени достоверности (от наибольшей к наименьшей) источники свидетельств оценки делятся на:

– документальные источники свидетельств, полученные из различных источников третьей стороны (сведения об использовании лицензионных мер и средств обеспечения ИБ, договора по сопровождению мер и средств обеспечения ИБ и т.д.);

– документальные источники свидетельств, полученные на (от) объекте(та) оценки и подтвержденные третьей стороной (план мероприятий по результатам внешнего аудита ИБ, материалы ведомственных проверок ИБ и т.д.);

– источники свидетельств, полученные в ходе проведения аудиторских процедур, не предусматривающих периодическую документальную отчетность (результаты наблюдения за деятельностью, анализа данных системы мониторинга ИБ и т.д.);

– источники свидетельств, полученные в виде нормативных и распорядительных документов (политики, регламенты, отчеты о деятельности, приказы, распоряжения и т.д.), указывающих на надлежащее применение процессов и мер обеспечения ИБ на практике (наличие разрешительных записей уполномоченных лиц, данных контроля рисков и т.д.);

– свидетельства, полученные в результате устных и письменных опросов о объекте оценки, и наблюдение за применением мер и средств обеспечения ИБ, которые не оставляют документальных свидетельств (выявление ролей процессов, последовательности применения ЗМ и т.д.).

Наряду с достоверностью источников свидетельств следует учитывать временной период получения свидетельств и сочетание источников свидетельств оценки. Например, доверие к фактам, полученным при наблюдении за деятельностью, повышается, если они получены непосредственно при функционировании проверяемых процедур или процессов; доверие к фактам, полученным при опросе сотрудников, повышается при подтверждении данных фактов из различных источников.

Достоверность выявленных свидетельств оценки ИБ зависит также от объема выборки при формировании свидетельств оценки. Соответствующее использование объема выборки тесно связано с доверием, с которым относятся к заключениям по результатам аудита.

Некоторые свидетельства оценки основано на выборках релевантных данных. Например, свидетельства наличия ЗМ для всех систем, степени охвата персонала и сотрудников подразделения процессами обучения и осведомления ИБ и т.д. Выборка производится с целью измерения и оценивания менее чем 100% объектов проверяемой совокупности. Задачей оценщика при проведении выборки является определение наиболее оптимального способа отбора элементов для формирования свидетельств оценки. При этом возможно:

– отобрать все элементы (сплошная проверка);

– отобрать специфические (определенные) элементы;

– отобрать отдельные элементы (сформировать аудиторскую выборку).

Сплошная проверка может быть целесообразна, если:

– генеральная совокупность состоит из небольшого числа элементов большой стоимости;

– риск контроля является высоким, а другие средства не позволяют получить достаточные свидетельства оценки;

– повторяющийся характер расчетов или иных процессов делает сплошную проверку эффективной с точки зрения соотношения затрат и результатов.

Сплошная проверка редко применяется при проведении оценки ИБ.

Оценщик может решить отобрать специфические (определенные) элементы генеральной совокупности, основываясь на следующих факторах.

Отбираемые специфические статьи могут включать:

– элементы с высокой стоимостью или так называемые критические (ключевые) элементы выборки;

– элементы, стоимость которых превышает определенную величину;

– элементы для проверки процедур, позволяющие определить, выполняется ли организацией конкретная процедура.

Выводы по результатам измерения, применяемого к отобранным таким способом элементам, не могут быть распространены на всю генеральную совокупность. При использовании этого метода анализируется потребность в получении свидетельств оценки в отношении оставшейся части генеральной совокупности, если оставшаяся часть является существенной.

Оценщик с учетом имеющихся сведений может принять решение о проведении выборочной проверки путем отбора отдельных элементов, т.е. применить статистический подход. Общее требование в этом случае — репрезентативность, т.е. все элементы изучаемой генеральной совокупности должны иметь равную вероятность быть отобранными в выборку.

При применении методов, связанных со статистической выборкой, объем отобранной совокупности может определяться на основании теории вероятностей и математической статистики либо профессионального суждения аудитора.

Достоверность оценки во многом зависит от того, как будут оценщиками учтены факторы, влияющие на аудиторский риск, который включает:

– риск контроля;

– риск необнаружения.

Риск контроля представляет собой риск того, что внутренний контроль не предотвратит или не выявит существенных нарушений ИБ. Важным фактором для повышения достоверности оценок является оптимизация объема выборки в соответствии с предполагаемым риском контроля.

Риск необнаружения представляет собой риск того, что процедуры и методы аудита, применяемые оценщиками, не выявят существенных нарушений.

Важными факторами для снижения риска необнаружения и, тем самым, повышения достоверности оценок являются:

– увеличение времени проверки;

– проведение опросов, ориентированных на представителей третьих независимых лиц;

– увеличение объема выборки.

Перечень основной литературы

1. Информационная безопасность: учебник для вузов/ В.И. Ярочкин – М.: Академический проект, 2012.

2. Семененко В.А. Информационная безопасность: учеб.пособие/ В.А. Семененко – М.: МГИУ, 2013.

Перечень дополнительной литературы

1. Информационная безопасность: учебник для вузов/ В.И. Ярочкин – М.: Академический проект, 2012.

2. Семененко В.А. Информационная безопасность: учеб.пособие/ В.А. Семененко – М.: МГИУ, 2013.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

Методические рекомендации по выполнению лабораторных работ по дисциплине «Основы управления информационной безопасности ".

2. Методические рекомендации по организации самостоятельной работы студентов по дисциплине " Основы управления информационной безопасности ".

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://el.ncfu.ru/ – система управления обучением ФГАОУ ВО СКФУ. Дистанционная поддержка дисциплины «Информационные технологии в профессиональной деятельности»
2. http://www.un.org - Сайт ООН Информационно-коммуникационные технологии
3. http://www.intuit.ru – Интернет-Университет Компьютерных технологий.

Практическое занятие 9. Построение концепции информационной безопасности предприятия»

Цель работы: *знакомство с основными принципами построения концепции ИБ предприятия, с учетом особенностей его информационной инфраструктуры*

Технология работы

этапы разработки концепции информационной безопасности

Разработка концепции информационной безопасности телекоммуникационной компании в полном объеме является процедурой, требующей значительных трудозатрат, а также значительного финансирования.
Приведенные ниже рекомендации по разработке концепции позволяют оптимизировать затраты на ее создание. Данные рекомендации предусматривают поэтапную разработку концепции с поэтапным финансированием работ.

Этап 1. Принятие решения, формирование рабочей группы. На данном этапе руководство компании должно принять решение о необходимости разработки концепции информационной безопасности, а также о целях, преследуемых данной разработкой.

Цели разработки могут быть следующие:

1. получение целостной системы взглядов на состояние ИБ в компании;
2. сокращение потерь вследствие ненадлежащего состояния системы ИБ;
3. создание новой (реконструкция существующей) системы ИБ;
4. документирование уже существующей системы ИБ;
5. получение конкурентного преимущества перед компаниями, не имеющими концепции.

После определения целей разработки на данном этапе формируется рабочая группа. В состав рабочей группы необходимо включить представителей следующих подразделений:

1. служба безопасности компании;
2. подразделение, ответственное за защиту информации;
3. IT-департамент;
4. служба эксплуатации сети связи;
5. служба развития;

6. отдел экономической безопасности;
7. техническая служба;
8. финансовая служба.

Этап 2. Составление плана разработки концепции. Определение объемов финансирования по сбору исходных данных. На данном этапе формируется календарный план мероприятий по разработке концепции, а также определяются сами мероприятия по разработке и стоимость их проведения.

Перечень мероприятий по разработке включает:

1. сбор исходных данных (возможно вплоть до полного аудита системы ИБ);
2. обработку исходных данных;
3. выбор варианта концепции ИБ
4. формирование подгруппы по разработке КИБ;
5. формирование подгруппы по разработке ПИБ;
6. формирование группы по проектированию системы ИБ.

Наиболее затратным на данном этапе является сбор исходных данных, поэтому прежде чем перейти непосредственно к работам по сбору ИД, необходимо полностью задействовать возможности подразделений Компании по самостоятельному предоставлению исходных данных, необходимых для концепции. После определения объема финансирования работ по сбору исходных данных необходимо приступать к третьему этапу.

Этап 3. Сбор исходных данных. На данном этапе силами рабочей группы или на основе привлечения субподрядных организаций осуществляется сбор исходных данных для разработки концепции. Как отмечено выше, в случае явного морального устаревания системы защиты информации, ее недостаточности или недокументированности на данном этапе необходимо провести полный аудит информационной безопасности компании. Аудит явится источником исходных данных для разработки концепции. Аудит придется проводить также и после реализации мероприятий по концепции, поэтому в целях снижения затрат предварительный аудит желательно производить по упрощенным методикам.

Этап 4. Разработка КИБ. Определение затрат на разработку ПИБ. На основании собранных исходных данных осуществляется разработка КИБ (нормативная часть). В данном документе уже будут отражены основные требования к системе ИБ и требования к ее нормативному обеспечению. Стоимость разработки ПИБ определяется следующими факторами:

1. полнотой собранных исходных данных;
2. уровнем безопасности, который должен быть обеспечен в соответствии с нормативной частью концепции;
3. требованиями к технике и нормативному обеспечению;
4. сложностью инфотелекоммуникационной структуры сети связи и информационной системы.

Этап 5. Разработка ПИБ и нормативных документов. На данном этапе разрабатывается техническая часть концепции — ПИБ. Требования к ПИБ сформулированы в нормативной части, а исходные данные могут уточняться по мере разработки ПИБ.

Параллельно с разработкой ПИБ проводится разработка документов, определенных нормативной частью концепции — положений, инструкций и т.д. Поскольку ПИБ детализирует технические характеристики системы защиты информации, на данном этапе разрабатываемые документы будут наполнены конкретным материалом и оптимизированы под бизнес-процессы компании.

Этап 6. Разработка экономической части концепции. После разработки ПИБ, содержащей детализированные требования к технике, помещениям, условиям эксплуатации, а также инструкции и иные нормативные документы, можно оценить стоимость:

1. реализации КИБ;
2. владения системой информационной безопасности;
3. прочих постоянных и переменных затрат в рамках положений концепции.

На основании предложенной в данной НИР методики (или иной методики) необходимо рассчитать окупаемость вложений, в случае необходимости произвести корректировку концепции.

Этап 7. Корректировка концепции (проводится при необходимости снижения затрат на реализацию). На данном этапе целесообразно выделить два уровня обеспечения безопасности — базовый и повышенный.

В *базовый* уровень необходимо включить те мероприятия и требования концепции, которые минимально необходимы для компании и выгода от реализации которых превышает затраты.

В *повышенный* уровень включаются те мероприятия и требования, которые необходимы только для ограниченного вида информационных ресурсов, а для других желательны. При этом необходимо обеспечить сопоставимость ценности ресурсов, защищаемых по повышенным требованиям, к затратам на защиту.

Коррекция проводится до тех пор, пока стоимость системы информационной безопасности не станет ниже приносимой выгоды. Заметим, что в приносимую выгоду необходимо включать сокращение потерь от рисков нарушения режима безопасности и рисков, ими генерируемых.

Этап 8. Утверждение концепции и ознакомление сотрудников компании. Данный этап является завершающим в разработке концепции. Концепция должна быть обсуждена коллегиальным руководящим органом компании, утверждена и введена приказом по компании.

Сотрудники компании должны быть ознакомлены с концепцией и документами, разработанными в ее рамках (в пределах компетентности сотрудников).

1. Перечень основной литературы

1. Информационная безопасность: учебник для вузов/ В.И. Ярочкин – М.: Академический проект, 2012.

2. Семененко В.А. Информационная безопасность: учеб.пособие/ В.А. Семененко – М.: МГИУ, 2013.

Перечень дополнительной литературы

1. Информационная безопасность: учебник для вузов/ В.И. Ярочкин – М.:

Академический проект, 2012.

2. Семененко В.А. Информационная безопасность: учеб.пособие/ В.А. Семененко – М.: МГИУ, 2013.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

Методические рекомендации по выполнению лабораторных работ по дисциплине «Основы управления информационной безопасности ".

2. Методические рекомендации по организации самостоятельной работы студентов по дисциплине " Основы управления информационной безопасности ".

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://el.ncfu.ru/ – система управления обучением ФГАОУ ВО СКФУ. Дистанционная поддержка дисциплины «Информационные технологии в профессиональной деятельности»
2. http://www.un.org - Сайт ООН Информационно-коммуникационные технологии
3. http://www.intuit.ru – Интернет-Университет Компьютерных технологий.