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

Методические указания

по выполнению лабораторных работ
по дисциплине «Управление проектами по защите информации и экономика защиты информации»
для студентов направления подготовки /специальности
10.03.01 Информационная безопасность
шифр и наименование направления подготовки/ специальности

(ЭЛЕКТРОННЫЙ ДОКУМЕНТ)

ВВЕДЕНИЕ

Основной целью предприятий на современном этапе развития экономики России является создание, защита и поддержание своей информационной инфраструктуры на современном уровне. В соответствии с этой целью можно сформулировать и его задачи: организация эффективного функционирования предприятия за счет интеграции отдельных функций подразделений с помощью информационных технологий; повышение скорости обработки и предоставления информации, необходимой для принятия решения на всех уровнях управления; повышение качества получаемой информации (избавление от шумов) из микросреды; о положении на рынках, состоянии конкурентов, возможностях сбыта, и макросреды; о международном положении, изменении законодательства и т.д. .

Лабораторная работа студента заключается в изучении лекционного материала, основной и дополнительной литературы по темам дисциплины «Управление проектами по защите информации и экономика защиты информации». В результате изучения студент должен знать основные положения и особенности экономики защиты информации, в частности: особенности развития рынка информации, правовые аспекты взаимодействия субъектов на рынке информации, состав интеллектуальной собственности предприятия и способы ее оценки, основные методики определения экономической эффективности и целесообразности организации мероприятий по защите информации. Методические указания к лабораторной работе разработаны в соответствии с программой дисциплины "Управление проектами по защите информации и экономика защиты информации" и предназначены для студентов всех форм обучения по направлению подготовки10.03.01 Информационная безопасность

СОДЕРЖАНИЕ

Лабораторная работа №1.
Тема: Уровень экономической безопасности предприятия, информация как важный ресурс экономики

Необходимость в защите информации от постороннего вмешательства и наблюдения давно осознана. Разработаны и продолжают разрабатываться соответствующие технологии. Однако увлечение отдельными решениями из области информационной безопасности заслоняет сохраняющуюся фундаментальную проблему, а именно достаточность и эффективность систем защиты с точки зрения пользователя. Мерилом потребительских качеств подобных систем может служить соотношение «стоимость/эффективность», т.е., в конечном счете, баланс между возможным ущербом от несанкционированных действий и размером вложений, которые необходимо потратить для обеспечения защищенности информационных ресурсов.

Инвестиции в разработку проектов защиты объекта, закупку необходимых элементов безопасности и эксплуатацию систем защиты для владельца информации есть ни что иное, как материализованный экономический ущерб. Идя на эти траты, пользователь надеется избежать большего ущерба, связанного с возможным нарушением конфиденциальности. Возникает дилемма: внести плату (частично реализовав ущерб) за возможность уклонения с долей вероятности или допустить возможность ущерба в полной мере, не тратя ничего. Разумное решение состоит в определении оптимальных вложений в системы защиты, обеспечивающих минимальные финансовые потери владельца информации при несанкционированных действиях с нею.

Перед пользователем стоит задача создания оптимальной, с экономической точки зрения, системы защиты информации. Эта задача не так характерна для государственных организаций, однако весьма актуальна для хозяйственно самостоятельных субъектов, ориентированных на деятельность в рыночных условиях.

Наиболее надежными системами защиты информации (СЗИ) являются те, в которых комплексно реализованы все возможные и доступные меры — морально-этические, законодательные, организационные, экономические и технические. Однако комплексные решения очень дороги и могут быть реализованы далеко не всегда. Кроме того, ущерб от утраты защищаемой информации или от разного рода несанкционированных действий с ней может быть гораздо меньше стоимости СЗИ. Поэтому уровень финансовых средств, выделяемых на создание и эксплуатацию СЗИ, должен быть сбалансированным и соответствовать масштабу угроз. Если стоимость СЗИ по сравнению с предполагаемым ущербом мала, то основным фактором риска собственника являются экономические потери от несанкционированных действий с принадлежащей ему информацией. В противоположной ситуации основные потери связаны с чрезмерно высокой стоимостью СЗИ. Необходимо при этом отметить, что затраты на СЗИ носят детерминированный характер, поскольку они уже материализованы в конкретные меры, способы и средства защиты, а вот ущерб, который может быть нанесен при несанкционированных действиях, — величина случайная.

Такой качественный анализ позволяет предполагать, что существует область экономически оптимальных СЗИ, обеспечивающих наименьший риск собственника информации. В качестве меры риска понимаются ожидаемые суммарные потери в процессе защиты информации в течение определенного периода времени. Проведенное автором исследование, основанное на количественном моделировании риска, подтвердило это предположение, обеспечив оценку параметров экономически оптимальных СЗИ.

Моделирование риска собственника информации при создании и эксплуатации СЗИ осуществлялось на основе функциональных зависимостей между риском R, стоимостью СЗИ S, вероятностью преодоления СЗИ и нанесения ущерба собственнику p и размером возникающего при этом ущерба U.

Не останавливаясь на конкретных моделях, отметим, что принципиально возможны три случая ($\partial p/\partial s<0$, $\partial p/\partial s=0$ и $\partial p/\partial s>0$), которые во многом предопределяют облик оптимальных решений и соответствующих СЗИ, их реализующих.

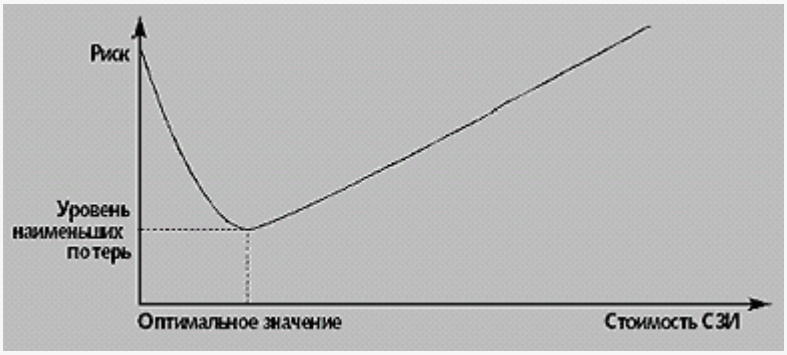

Рис. 1. Зависимость уровня риска от стоимости СЗИ ($\partial p/\partial s<0$)

Типичная зависимость уровня риска от стоимости СЗИ, полученная при условии того, что вероятность нанесения ущерба p уменьшается с ростом стоимости системы S (т.е. соответствующая производная отрицательна, $\partial p/\partial s<0$) приведена на рис. 1. Ее анализ показывает, что применение даже недорогих способов и средств защиты информации резко снижает суммарные потери собственника. Таким образом, вложение средств в СЗИ уже в сравнительно небольших размерах является очень эффективным. При некоторой стоимости СЗИ риск имеет наименьшее значение. Эта стоимость является оптимальной. Дальнейший, сверх оптимального значения, рост затрат на СЗИ будет вести к увеличению экономических потерь собственника информации. Его выигрыш в повышении надежности системы защиты и соответствующем снижении вероятности ущерба от несанкционированных действий будет нивелироваться и обесцениваться чрезвычайно высокой стоимостью самой СЗИ. Поэтому наилучшей стратегией собственника информации будет, очевидно, использование СЗИ, обеспечивающих минимум риска. Эффективность такого решения подтверждается результатами численного моделирования, в соответствии с которыми использование экономически оптимальных СЗИ приводит к снижению суммарных ожидаемых потерь примерно на порядок по сравнению с базовыми решениями.

Чем больше оценка размера вероятного ущерба, тем выше и оптимальная стоимость СЗИ, однако эта зависимость достаточно гладкая, особенно в диапазоне больших значений ожидаемого ущерба. Следовательно, даже если ценность защищаемой информации возросла, то это отнюдь не означает необходимости пропорционального наращивания технических возможностей и соответствующего удорожания СЗИ.

Результаты численного моделирования подтвердили, что экономически оптимальная СЗИ не является самой безопасной. Более того, вероятность ущерба от несанкционированных действий при реализации такой системы может превышать в несколько раз минимально возможные значения показателей безопасности защиты информации. Поэтому применение изложенного подхода ограничено областью экономической целесообразности. В случаях, когда доминирующим требованием является обеспечение абсолютной безопасности информации, реализация концепции экономически оптимальной СЗИ не применима. Это относится, например, к сведениям, составляющим государственную тайну. Тем не менее,

оптимальные СЗИ обеспечивают адаптацию требований безопасности к размеру возможного ущерба. На рис. 2 приведена зависимость вероятности несанкционированных действий с защищаемой информацией при оптимальной СЗИ от величины ущерба.

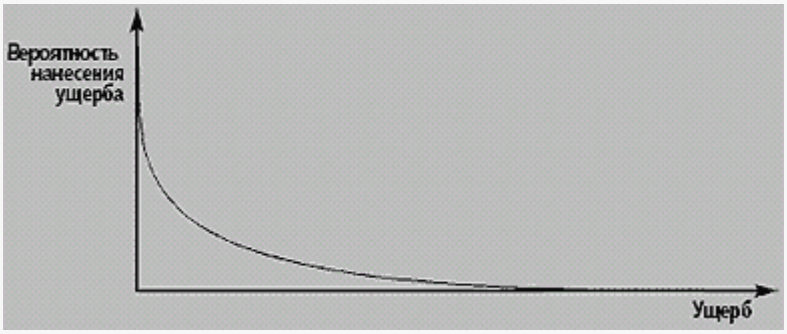

Рис. 2. Зависимость вероятности несанкционированных действий в оптимальной СЗИ от размера возможного ущерба

Изложенные результаты базируются на вполне логичном предположении о том, что более высокий уровень безопасности достигается за счет увеличения стоимости СЗИ. Для придания завершенности, рассмотрим и два других случая.

1. Уровень универсальной обобщенной характеристики безопасности СЗИ — вероятности нанесения ущерба не зависит от стоимости системы защиты ($\partial p/\partial s=0$). К сожалению, такой случай правдоподобен. Например, если организация-подрядчик, осуществляющая проектирование СЗИ, предлагает своему заказчику более дорогое решение, хотя такой же уровень безопасности может быть достигнут и за меньшую плату. Оказывается, что такое недобросовестное решение приводит к зависимости риска владельца защищаемой информации от стоимости СЗИ, показанной на рис. 3, где p — вероятность нанесения ущерба, а стрелкой показано направление изменения риска при увеличении этой вероятности. Подобная зависимость технических характеристик СЗИ от ее стоимости может реализовываться и в случае монополизма поставщика, инфляционных процессах, недобросовестной конкуренции и т.д.

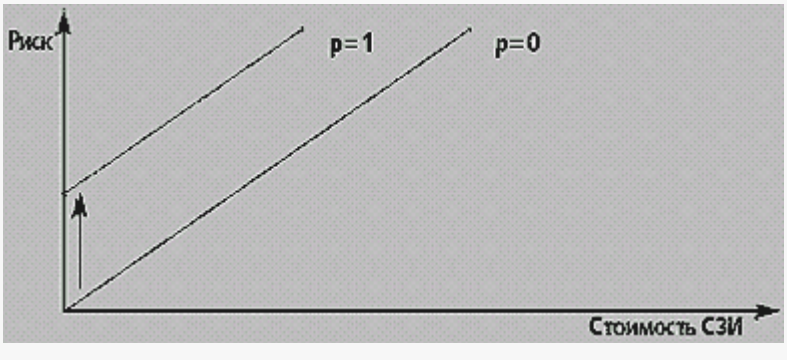

Рис. 3. Зависимость уровня риска от стоимости СЗИ ($\partial p/\partial s=0$)

Если СЗИ фактически обладает высокими характеристиками безопасности, то для снижения своего риска владельцу информационного ресурса необходимо добиваться снижения стоимости системы. Если же изначально характеристики безопасности СЗИ неудовлетворительны, то единственно разумным решением является отказ от нее.

2. Уровень универсальной характеристики безопасности СЗИ имеет тенденцию в некотором ценовом диапазоне к снижению с ростом ее стоимости ($\partial p/\partial s>0$). Такая ситуация также возможна — например, когда элементы защиты содержат невыявленные ошибки, а

СЗИ «совершенствуется» путем наращивания из таких элементов. В этом случае зависимость риска владельца защищаемой информации от стоимости СЗИ показана на рис. 4, где для сравнения пунктиром дан риск при $\partial p/\partial s<0$. В связи с тем, что общий уровень риска возрастает во всем стоимостном диапазоне, необходимо провести тщательный анализ и поиск оптимального решения.

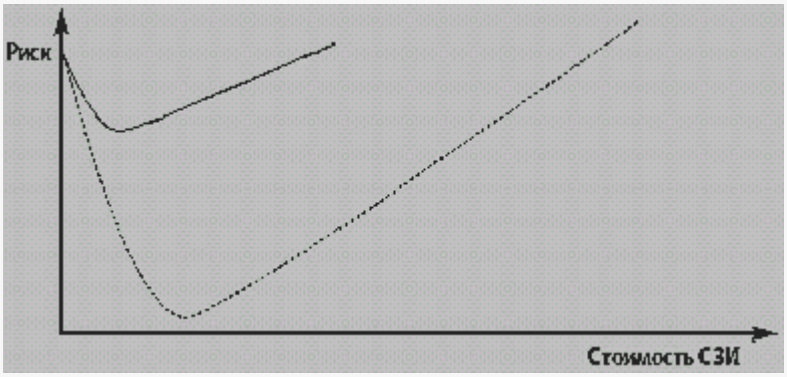

Рис. 4. Зависимость вероятности нанесения ущерба от стоимости СЗИ ($\partial p/\partial S>0$)

Стоимость СЗИ можно существенно снизить при использовании страховых инструментов. Эффективность этого метода во многом зависит от точности определения страховой стоимости защищаемых информационных ресурсов, а также степени соответствия тарифной ставки вероятности несанкционированных действий. Реализации страхования информации мешает фундаментальная проблема отсутствия достаточно точных практических методик по определению ее стоимости и обоснованию тарифов. Сколь сложен этот вопрос, можно судить хотя бы по дискуссиям по смежной теме — концепции общей стоимости владения информационной системой (TCO — totalcostofownership). ИТ-специалисты отмечают множество проблем при практическом использовании данной концепции, хотя в основе информационных систем и лежат вполне материальные вещи, имеющие известную стоимость. Поэтому попытки использования экспертного метода или декларируемого рыночного подхода, основанного на оценке популярности и востребованности информационного ресурса, во многих случаях заведомо неприемлемы. Необходимо приложение дополнительных усилий для разработки практических методик оценки стоимости информации.

В заключение отметим, что оптимальные СЗИ наиболее целесообразны для экономически самостоятельных субъектов, которые в своей деятельности вынуждены соблюдать баланс между затратами на СЗИ и возможным ущербом. Реализация таких систем защиты информации возможна при тщательном учете всех аспектов, включая количественную оценку безопасности и размера ожидаемых потерь. Оценка экономически оптимальных параметров должна являться основой формирования конкретного технического облика СЗИ. К сожалению, сегодня проектирование СЗИ обычно осуществляется с ориентацией на произвольно выделяемый бюджет, не имеющий объективного обоснования по системе критериев «стоимость информации — размер возможного ущерба — риски». При этом владелец информационных ресурсов, если не проводит тщательногоанализа и не оптимизирует размер выделяемых на СЗИ средств, практически всегда оказывается в экономическом проигрыше.

Информация и страховые тарифы

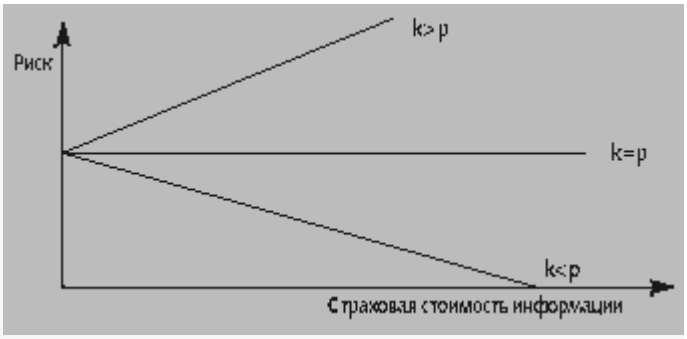

Рис. Зависимость риска от размера страховой стоимости при различных тарифах

Задание:

1.Провести анализ способов и средств защиты информации

2.Проланализировать снижение суммарных потерь собственника в результате применения средств защиты информации

Ответить на вопросы:

1.Структура управленческой информации

2. Виды экономической информации

3.Характеристика документов: нормативные, плановые, учетные, расчетные, аналитические и другие виды.

Лабораторная работа 2.
Этапы построения и экономическое обоснование создания системы защиты информации

Информация в настоящее время является товаром, который можно покупать и продавать на рынке, иногда – за достаточно большие деньги. Как и любой товар, информация имеет свою цену, за которую она покупается и продается, и как любой ценный ресурс – подлежит защите.

Отечественный ИТ-рынок в последние несколько лет динамично развивается, по оценкам экспертов его рост превышает 10% в год. При этом сектор информационной безопасности (ИБ) развивается еще более быстрыми темпами — более чем на 25% в год. Такой рост определяется в основном двумя факторами: возросшим вниманием руководства к обеспечению ИБ и недостаточным уровнем ИБ в существующих информационных системах (ИС). Понятно, что долго такие темпы роста сектора ИБ

сохраняться не смогут, они замедлятся, и вопросы оценки эффективности затрат в области ИБ встанут весьма остро. Уже сейчас в отечественных ИС с повышенными требованиями в области ИБ (банковские системы, ответственные производства, и т.д.) затраты на обеспечение режима ИБ составляют до 30% всех затрат на ИС, и владельцы информационных ресурсов серьезно рассматривают экономические аспекты обеспечения ИБ. Даже в тех ИС, уровень ИБ которых явно не достаточен, у технических специалистов зачастую возникают проблемы обоснования перед руководством (владельцами информационных ресурсов) затрат на повышение этого уровня. Начальники служб автоматизации, исполнительные директора, начальники служб информационной безопасности должны иметь понятные для бизнеса аргументы для обоснования инвестиций в ИБ, т.е., по сути, представлять обоснование стоимости системы ИБ для бизнеса.

Таким образом, в настоящее время комплексное управление процессами обеспечения информационной безопасностью (ИБ) подразумевает не просто бесцельное внедрение совокупности средств и систем защиты. ИБ превратилась в науку о реализации адекватного и эффективного по качеству и стоимости подхода к обеспечению защищенности всех элементов ИТ. Такой взгляд на проблему ИБ неизбежно требует определения показателей и метрик, позволяющих сравнивать защищенность различных систем ИТ, сравнивать эффективность контрмер, ранжировать угрозы и уязвимости по своей важности.

Для любых компаний очень важно деньги в ЗИ вкладывать обоснованно. В информационной безопасности известен принцип разумной достаточности, который гласит следующее:

Создание 100% надежной системы защиты информации невозможно в принципе, в любых случаях остается ненулевая возможность реализации какой-либо угрозы либо уязвимости. Любая система защиты информации может быть взломана, это вопрос только времени и потраченных злоумышленником средств. Поэтому бесконечно вкладывать деньги в обеспечение ИБ бессмысленно, необходимо когда-то остановиться (вопрос только в выборе этого порога). Согласно принципу разумной достаточности, стойкость СЗИ считается достаточной, если время взлома злоумышленником СЗИ превосходит время старения информации (либо некоторый разумный предел), либо стоимость взлома системы защиты информации превосходит стоимость полученной злоумышленником выгоды от взлома. В последнем случае, если злоумышленник является нормальным экономическим субъектом (не фанат, с психикой все в порядке), то он конечно не будет работать себе в убыток.

Пример

Возьмем парольную систему идентификации и аутентификации пользователей ОС Windows 2000. Предположим, что пользовательские пароли выбираются длиной 10 символов и используется следующий алфавит символов (наиболее распространенный):

1. Английские малые и большие буквы.
2. Цифры.
3. Специальные знаки (13 штук).

Пространство атаки хэша NTLM в этом случае = $(26+26+10+13)^{10}=75^{10}$

Пространство атаки хэша LANMAN в этом случае = $(26+10+13)^{7}+(26+10+13)^{3}=49^{7}+49^{3}$.

Скорость перебора паролей программой SAMInsidecоставляет около $7*10^{6}$ паролей в секунду.

Тогда гарантированное время взлома составляет $(49^{7}+49^{3})$ / $(7*10^{6})$ секунд = 96889 секунд = 27 часов. В этом случае, даже если пароли менять каждый день, то вероятность взлома будет близка к единице.

Если к алфавиту символов добавить русские буквы, то гарантированное время взлома составляет 41 сутки. Если пароли менять каждую неделю, то вероятность взлома будет составлять 1/7. В обоих случаях, стойкость – недостаточна, время взлома ненамного превосходит время старения информации (смена пароля).

Однако, если выбрать пароль 15 символов (хеша LANMAN не будет), то гарантированное время взлома при первом наборе символов будет составлять $75^{15}/10^7$ секунд = 42375 млрд. лет, в этом случае даже меняя пароль один раз в год, мы получим достаточную стойкость системы защиты.

Второй вариант – использовать аппаратные ключи и аппаратные устройства (однако, придется принимать во внимание их стоимость, и стоимость защищаемой информации).

Существует, как минимум, два подхода к обоснованию стоимости корпоративной системы защиты.

Первый подход – (наукообразный) - заключается в том, чтобы применить на практике необходимый инструментарий получения *метрики и меры безопасности*, а для этого привлечь руководство компании (как ее собственника) к оценке стоимости защищаемой информации, определений возможностей реализации потенциальных угроз и уязвимостей, а также потенциального ущерба. Наиболее известный показатель, позволяющий характеризовать меру безопасности, сравнивать защищенность различных систем ИТ, сравнивать эффективность контрмер – есть риск ИБ. Через риск достаточно эффективно считается наиболее экономичный вариант реализации контрмер.

Второй подход (практический) состоит в следующем: можно попробовать найти инвариант разумной стоимости корпоративной системы защиты информации. Ведь существуют аналогичные инварианты в других областях, где значимые для бизнеса события носят вероятностный характер. Например, на рынке автострахования некоторая общая оценка разумной стоимости такой услуги, как страхование собственного автомобиля, составляет от 5 до 15% его рыночной цены - в зависимости от локальных условий эксплуатации, культуры и опыта вождения водителя, интенсивности движения, состояния дорог и т.д. Эксперты-практики в области защиты информации нашли некий оптимум, позволяющий чувствовать себя относительно уверенно, - стоимость системы ИБ должна составлять примерно 10-20% от стоимости КИС - в зависимости от уровня конфиденциальности информации (но надо их еще правильно вложить). Это и есть та самая оценка на основе практического опыта (bestpractice), на которую можно положиться. И на вопрос «А почему для создания адекватной целям и задачам бизнеса корпоративной системы защиты информации требуется сто тысяч долларов?» отвечать «Потому что на сегодняшний день стоимость нашей КИС составила один миллион долларов!». Очевидно, что второй подход не лишен недостатков. Здесь, скорее всего, не удастся заставить руководство глубоко осознать проблемы ИБ. Но зато можно смело прогнозировать объем бюджета на ИБ и существенно сэкономить на услугах внешних консультантов.

Ответить на вопросы

1.Этапы построения системы информационной безопасности предприятия
2.Метод получения количественной оценки риска
3. Комплексное управление процессами обеспечения информационной безопасностью

Лабораторная работа 3.
Методы оценки и планирования производственных затрат. Производственные ресурсы фирмы

Под риском информационной безопасности будем понимать возможные потери собственника или пользователя информации и поддерживающей инфраструктуры связанные с реализацией некоторой угрозы.

1. Риск нарушения конфиденциальности информации (информация - товар).
2. Риск нарушения целостности информации (Магнитогорск, DrPaper).
3. Риск нарушения доступности информации, доступности сервисов – Владивосток. Организации сейчас жестко завязаны на автоматизацию, на сервисы, несут огромные потери от их простаивания (это ущерб). Недаром сейчас вводят такого рода процессы, как управление доступностью сервисов, управление непрерывностью и т.д.

Порядок определения затрат на защиту информации

4.1. Прямые и косвенные затраты на защиту информации предприятия (организации)

Как уже отмечалось, безопасность предприятия обеспечивается комплексом мер на всех этапах его жизненного цикла, его информационной системы и в общем случае складывается из стоимости:

1) проектных работ;
2) закупки и настройки программно-технических средств защиты,

включающих следующие основные группы: межсетевые экраны, средства криптографии, антивирусы и ААА (средства аутентификации, авторизации и администрирования);

3) затрат на обеспечение физической безопасности;
4) обучения персонала;
5) управления и поддержки системы (администрирование безопасности);
6) аудита защиты информации;
7) периодической модернизации системы защиты информации и т.д.

Стоимостным показателем экономической эффективности комплексной системы защиты информации будет сумма прямых и косвенных затрат на организацию (модернизации), эксплуатацию и сопровождение системы защиты информации в течение года.

Он может рассматриваться как ключевой количественный показатель эффективности организации защиты информации в компании, так как позволит не только оценить совокупные затраты на защиту, но управлять этими затратами для достижения требуемого уровня защищенности предприятия.

При этом прямые затраты включают как капитальные компоненты затрат (ассоциируемые с фиксированными активами или «собственностью»), так и трудозатраты, которые учитываются в категориях операций и административного управления. Сюда же относят затраты на услуги удаленных пользователей и др., связанные с поддержкой деятельности организации.

В свою очередь косвенные затраты отражают влияние комплексной системы безопасности и подсистемы защиты информации на служащих посредством таких измеримых показателей, как простои и «»зависания» корпоративной системы защиты

информации и комплексной системы безопасности в целом, затраты на операции и поддержку (не относящиеся к прямым затратам).

Очень часто косвенные затраты играют значительную роль, так как они обычно изначально не отражаются в бюджете на комплексную систему безопасности, а выявляются явно при анализе затрат в последствии, что в конечном счете приводит к росту «скрытых» затрат компании. Рассмотрим, как можно определить прямые (бюджетные) и косвенные затраты на комплексную систему безопасности.

Предположим, что руководство предприятия проводит работы по внедрению на предприятии комплексной системы защиты информации (КСЗИ). Уже определены объекты и цели защиты, угрозы информационной безопасности и меры по противодействию им, приобретены и установлены необходимые средства защиты информации. Для того, чтобы требуемый уровень защиты ресурсов реально достигался и соответствовал ожиданиям руководства предприятия, необходимо ответить на следующие основные вопросы, связанные с затратами на информационную безопасность:

1) Неизбежны ли затраты на информационную безопасность?

2) Какова зависимость между затратами на информационную безопасность и достигаемым уровнем информационной безопасности?

3) Представляют ли затраты на информационную безопасность существенную часть от оборота компании?

4) Какую пользу можно извлечь из анализа затрат на информационную безопасность?

Как правило, затраты на информационную безопасность подразделяются на следующие категории:

1) Затраты на формирование и поддержание звена управления системой защиты информации (организационные затраты).

2) Затраты на контроль, то есть на определение и подтверждение достигнутого уровня защищенности ресурсов предприятия.

3) Внутренние затраты на ликвидацию последствий нарушения информационной безопасности – затраты, понесенные организацией в результате того, что требуемый уровень защищенности не был достигнут.

4) Внешние затраты на ликвидацию последствий нарушения информационной безопасности – компенсация потерь при нарушениях политики безопасности в случаях, связанных с утечкой информации, потерей имиджа компании, утратой доверия партнеров и потребителей и т. п.

5) Затраты на техническое обслуживание системы защиты информации и мероприятия по предотвращению нарушений политики безопасности предприятия (затраты на предупредительные мероприятия).

При этом обычно выделяют единовременные и систематические затраты.

Единовременные – затраты на формирование безопасности предприятия: организационные затраты и затраты на приобретение и установку средств защиты.

Систематические – затраты на эксплуатацию и обслуживание.

Классификация затрат условна, так как сбор, классификация и анализ затрат на информационную безопасность – внутренняя деятельность предприятий, и детальная разработка перечня зависят от особенностей конкретной организации.

Главное при определении затрат на систему безопасности – взаимопонимание и согласие по статьям расходов внутри предприятия. Кроме того, категории затрат должны

быть постоянными и не должны дублировать друг друга. Неизбежны ли затраты на информационную безопасность?

Невозможно полностью исключить затраты на безопасность, однако они могут быть приведены к приемлемому уровню. Некоторые виды затрат на безопасность являются абсолютно необходимыми, а некоторые могут быть существенно уменьшены или исключены. Последние – это те, которые могут исчезнуть при отсутствии нарушений безопасности или сократятся, если количество и разрушающее воздействие нарушений уменьшатся.

При соблюдении безопасности и проведении профилактики нарушений можно исключить или существенно уменьшить следующие затраты:

1) на восстановление системы безопасности до соответствия требованиям безопасности;

2) на восстановление ресурсов информационной среды предприятия;

3) на переделки внутри системы безопасности;

4) на юридические споры и выплаты компенсаций;

5) на выявление причин нарушения безопасности.

Необходимые затраты – это те, которые необходимы даже если уровень угроз безопасности достаточно низкий. Это затраты на поддержание достигнутого уровня защищенности информационной среды предприятия. Неизбежные затраты могут включать:

1) обслуживание технических средств защиты;

2) конфиденциальное делопроизводство;

3) функционирование и аудит системы безопасности;

4) минимальный уровень проверок и контроля с привлечением специализированных организаций;

5) обучение персонала методам информационной безопасности.

Какова зависимость между затратами на информационную безопасность и уровнем защищенности предприятия?

Сумма всех затрат на повышение уровня защищенности предприятия от угроз информационной безопасности составляет общие затраты на безопасность. Взаимосвязь между всеми затратами на безопасность, общими затратами на безопасность и уровнем защищенности информационной среды предприятия обычно имеет вид функции Общие затраты на безопасность складываются из затрат на предупредительные мероприятия, затрат на контроль и восполнение потерь (внешних и внутренних). С изменением уровня защищенности информационной среды изменяются величины составляющих общих затрат и, соответственно, их сумма – общие затраты на безопасность. Мы не включаем в данном случае единовременные затраты на формирование информационной безопасности предприятия, так как предполагаем, что такая система уже выработана Снижение общих затрат В примере показано, что достигаемый уровень защищенности измеряется в категориях «большой риск»» и «риск отсутствует» («совершенная защита»).

Рассматривая левую сторону графика («большой риск»), мы видим, что общие затраты на безопасность высоки в основном потому, что высоки потери на компенсацию при нарушениях политики безопасности. Затраты на обслуживание системы безопасности очень малы.

Если мы будем двигаться вправо по графику, то достигаемый уровень защищенности будет увеличиваться (снижение информационного риска). Это происходит за счет

увеличения объема предупредительных мероприятий, связанных с обслуживанием системы защиты. Затраты на компенсацию НПБ уменьшаются в результате предупредительных действий. Как показано на графике, на этой стадии затраты на потери падают быстрее, нежели возрастают затраты на предупредительные мероприятия.

Как результат – общие затраты на безопасность уменьшаются. Изменения объема затрат на контроль незначительны. Взаимосвязь между затратами на безопасность и достигаемым уровнем защищенности.

Увеличение общих затрат

Если двигаться по графику вправо за точку экономического равновесия (т.е. достигаемый уровень защищенности увеличивается), ситуация начинает меняться. Добиваясь устойчивого снижения затрат на компенсацию нарушений политики безопасности, мы видим, что затраты на предупредительные мероприятия возрастают все быстрее и быстрее. Получается, что значительное количество средств должно быть затрачено на достижение достаточно малого снижения уровня риска.

График (рис. 4.1.) отражает только общий случай, так как построен с учетом некоторых допущений, которые не всегда соответствуют реальным ситуациям.

Первое допущение заключается в том, что предупредительная деятельность по техническому обслуживанию комплекса программно-технических средств защиты информации и предупреждению нарушений политики безопасности предприятия соответствует следующему правилу: в первую очередь рассматриваются те проблемы, решение которых дает наибольший эффект по снижению информационного риска. Если не следовать этой модели, то вид графика станет совсем иным.

Второе допущение заключается в том, что точка экономического равновесия не изменяется во времени. На практике это допущение часто не выполняется.

Основные факторы:

1) эффективность предупредительной деятельности невелика.

В рассматриваемой модели предполагается, что такая деятельность позволяет не повторять допущенные ранее ошибки. На практике это не так, и для достижения должного эффекта требуются большие затраты. В результате точка экономического равновесия сдвигается вправо;

2) устаревшие системы ИБ;

3) разработчики средств защиты не успевают за активностью злоумышленников, которые находят все новые и новые бреши в системах защиты.

Кроме того, информатизация предприятия может породить новые проблемы, решение которых потребует дополнительных предупредительных затрат.

После того, как уже установлена система классификации и кодирования различных элементов затрат на безопасность, необходимо выявить источники данных о затратах.

Такая информация уже может существовать, часть ее достаточно легко получить, в то время как другие данные определить будет значительно труднее, а некоторые могут быть недоступны.

Затраты на контроль.

Основной объем затрат составляет оплата труда персонала службы безопасности и прочего персонала предприятия, занятого проверками и испытаниями. Эти затраты могут быть определены весьма точно.

Оставшиеся затраты в основном связаны со стоимостью конкретных специальных работ и услуг внешних организаций и материально-техническим обеспечением системы безопасности. Они могут быть определены напрямую.

Внутренние затраты на компенсацию нарушений безопасности. Определение элементов затрат этой группы намного сложнее, но большую часть установить достаточно легко:

1) установка патчей или приобретение последних версий программных средств защиты информации;

2) приобретение технических средств взамен пришедших в негодность;

3) затраты на восстановление баз данных и прочих информационных массивов;

4) затраты на обновление планов обеспечения непрерывности деятельности службы безопасности;

5) затраты на внедрение дополнительных средств защиты, требующих существенной перестройки системы безопасности.

Труднее выявить объемы заработной платы и накладных расходов:

1) по проведению дополнительных испытаний и проверок технологических информационных систем;

2) по утилизации скомпрометированных ресурсов;

3) по проведению повторных проверок и испытаний системы защиты информации;

4) по проведению мероприятий по контролю достоверности данных, подвергшихся атаке на целостность;

5) по проведению расследований нарушений безопасности;

Выяснение затрат на эти виды деятельности связаны с различными отделами:

1) отделом информационных технологий;

2) контрольно-ревизионным и финансовым отделами;

3) службой безопасности.

Поскольку каждый вовлеченный сотрудник вряд ли в течение всего рабочего дня решает проблемы, связанные только лишь с внутренними потерями от нарушений политики безопасности, оценка потерь должна быть произведена с учетом реально затраченного на эту деятельность времени.

Таким образом, мы опять видим, что основные виды затрат в этой категории могут быть определены с достаточной степенью точности.

Внешние затраты на компенсацию нарушений безопасности Часть внешних затрат на компенсацию нарушений политики безопасности связана с тем, что были скомпрометированы коммерческие данные партнеров и персональные данные пользователей услуг предприятия. Затраты, связанные с восстановлением доверия, определяются таким же образом, как и в случае внутренних потерь. Однако существуют и другие затраты, которые определить достаточно сложно. В их числе:

1) затраты на проведение дополнительных исследований и разработку новой рыночной стратегии;

2) потери от снижения приоритета в научных исследованиях и невозможности патентования и продажи лицензий на научно-технические достижения;

3) затраты, связанные с ликвидацией «узких мест» в снабжении, производстве и сбыте продукции;

4) потери от компрометации производимой предприятием продукции и снижения цен на нее;

5) возникновение трудностей в приобретении оборудования или технологий, в том числе повышение цен на них, ограничение объема поставок.

Перечисленные затраты могут быть вызваны действиями персонала различных отделов, например, проектного, технологического, планово-экономического, юридического, хозяйственного, отдела маркетинга, тарифной политики и ценообразования.

Поскольку сотрудники всех этих отделов вряд ли будут заняты полный рабочий день вопросами внешних потерь, то установление объема затрат необходимо вести с учетом реально затраченного времени.

Один из элементов внешних потерь невозможно точно вычислить – это потери, связанные с подрывом имиджа предприятия, снижением доверия потребителя к продукции и услугам предприятия.

Именно по этой причине многие корпорации скрывают, что их сервис не безопасен. Корпорации боятся обнародования такой информации даже больше, чем атаки в той или иной форме.

Однако многие предприятия игнорируют эти затраты на основании того, что их нельзя установить с какой-либо степенью точности – они только предположительны. Затраты на предупредительные мероприятия. Эти затраты, вероятно, наиболее сложно оценить, поскольку предупредительные мероприятия проводятся в разных отделах и затрагивают многие службы.

Эти затраты могут появляться на всех этапах жизненного цикла ресурсов информационной среды предприятия:

1) планирования и организации;

2) приобретения и ввода в действие;

3) доставки и поддержки;

4) мониторинга процессов, составляющих информационную технологию.

В дополнение к этому, большинство затрат данной категории связано с работой персонала службы безопасности.

Затраты на предупредительные мероприятия в основном включают заработную плату и накладные расходы.

Однако точность их определения в большей степени зависит от точности установления времени, затраченного каждым сотрудником в отдельности. Некоторые предупредительные затраты легко выявить напрямую. Они, в частности, могут включать оплату различных работ сторонних организаций, например:

1) обслуживание и настройку программно-технических средств защиты, операционных систем и используемого сетевого оборудования;

2) проведение инженерно-технических работ по установлению сигнализации, оборудованию хранилищ конфиденциальных документов, защите телефонных линий связи, средств вычислительной техники и т. п.;

3) доставку конфиденциальной информации;

4) консультации;

5) курсы обучения.

Источники сведений о рассмотренных затратах. При определении затрат на обеспечение ИБ необходимо помнить, что:

1) затраты на приобретение и ввод в действие программно-технических средств могут быть получены из анализа накладных, записей в складской документации и т. п.;

2) выплаты персоналу могут быть взяты из ведомостей;

3) объемы выплат заработной платы должны быть взяты с учетом реально затраченного времени на проведение работ по обеспечению информационной безопасности если только часть времени сотрудника затрачивается на деятельность по обеспечению информационной безопасности, то целесообразность оценки каждой из составляющих затрат его времени не должна подвергаться сомнению;

4) классификация затрат на безопасность и распределение их по элементам должны стать частью повседневной работы внутри предприятия.

С этой целью персоналу должны быть хорошо известны различные элементы затрат и соответствующие им коды.

Задание.

1. Проработать теоретический материал
2. Разработать примерный перечень затрат предприятия (организации) на обеспечение информационной безопасности с обязательным предположением, что основы безопасности на предприятии сформированы.

Ответить на вопросы:

1.Типовая зависимость уровня риска от стоимости СЗИ

2.Методы снижения стоимости СЗИ

3.Применение принципов размещения и экономного расходования ресурсов предприятия.

4.Оценка ожидаемых результатов эффективности организации ИБ

Лабораторная работа 4.
Затраты на контроль за соблюдением политики ИБ. Затраты на ликвидацию последствий нарушения режима ИБ

Таблица 1. Затраты на обслуживание системы безопасности (затраты на предупредительные мероприятия)

Направления	Вид затрат
Управление системой защиты информации	Затраты на планирование системы защиты информации предприятия.
	Затраты на изучение возможностей информационной инфраструктуры предприятия по обеспечению безопасности информации ограниченного распространения.

Таблица 2. Затраты на осуществление технической поддержки

Направления	Вид затрат
Обучение производственного персонала при внедрении средств защиты и процедур, а также планов по защите информации.	Проверка сотрудников на лояльность, выявление угроз безопасности.
	Организация системы допуска исполнителей и сотрудников конфиденциального делопроизводства

	с соответствующими штатами.

Таблица 3. Обслуживание средств защиты информации

Направления	Вид затрат
Регламентное обслуживание средств защиты информации	Затраты на обслуживание и настройку программно-технических средств защиты, операционных систем, используемого сетевого оборудования.
	Затраты, связанные с организацией сетевого взаимодействия и безопасного использования информационных систем.
	Затраты на поддержание системы резервного копирования и ведение архива данных.
	Проведение инженерно-технических работ по установлению сигнализации, оборудованию хранилищ конфиденциальных документов, защите телефонных линий связи, средств вычислительной техники и т. п.

Таблица 4. Аудит системы безопасности

Направления	Вид затрат
Затраты на контроль изменений состояния информационной среды предприятия.	Обеспечение должного качества информационных технологий
Затраты на систему контроля за действиями исполнителей.	Затраты на обеспечение соответствия требованиям качества информационных технологий, в том числе анализ возможных негативных аспектов информационных технологий, которые влияют на целостность и доступность информации.
	Затраты на доставку (обмен) конфиденциальной информации.
	Удовлетворение субъективных требований пользователей: стиль, удобство интерфейсов и др.
	Удовлетворение субъективных требований пользователей: стиль, удобство интерфейсов и др.
Обеспечение требований стандартов	Затраты на обеспечение соответствия принятым стандартам и требованиям, достоверности информации, действенности средств защиты.

	Затраты на контроль: Плановые проверки и испытания. Затраты на проверки и испытания программно-технических средств защиты информации. Затраты на проверку навыков эксплуатации средств
	Затраты на обеспечение работы лиц, ответственных за реализацию конкретных процедур безопасности по подразделениям.
	Оплата работ по контролю правильности ввода данных в прикладные системы.
	Оплата работ по контролю правильности ввода данных в прикладные системы. Оплата инспекторов по контролю требований, предъявляемых к защитным средствам при разработке любых систем (контроль выполняется на стадии проектирования и спецификации требований).
	Внеплановые проверки и испытания. Оплата работы испытательного персонала специализированных организаций. Обеспечение испытательного персонала (внутреннего и внешнего) материально-техническими средствами. Контроль за соблюдением безопасности Затраты на контроль реализации функций, обеспечивающих управление защитой коммерческой тайны. Затраты на организацию временного взаимодействия и координации между подразделениями для решения повседневных конкретных задач. Затраты на проведение аудита безопасности по каждой автоматизированной информационной системе, выделенной в информационной среде предприятия. Материально-техническое обеспечение системы контроля доступа к объектам и ресурсам предприятия. Затраты на внешний аудит Затраты на контрольно-проверочные мероприятия, связанные с лицензионно-разрешительной деятельностью в сфере защиты информации. Пересмотр информационной безопасности предприятия (проводится периодически) Затраты на идентификацию угроз безопасности. Затраты на поиск уязвимостей системы защиты информации. Оплата работы специалистов, выполняющих работы по определению возможного ущерба и переоценке степени риска. Затраты на ликвидацию последствий нарушения режима безопасности. Восстановление системы безопасности до соответствия требованиям политики безопасности. Установка патчей или приобретение последних версий программных средств защиты информации. Приобретение технических средств взамен пришедших в негодность. Проведение дополнительных испытаний и проверок технологических информационных систем.

	Затраты на утилизацию скомпрометированных ресурсов

2.Определение экономической эффективности защиты информации.

Основой определения эффективности защиты информации – это сопоставление отношения доходов и расходов. Эффективность определяется с помощью различных показателей, при этом сопоставляются данные, выражающие эффект (прибыль, объем производства, экономия от снижения издержек) с затратами обеспечивающими этот эффект (капитальные вложения, текущие издержки). При решении экономических задач определяется результативность каждого предприятия и производится сопоставление различных результатов. Большое значение в расчете эффективности, в том числе и эффективности защиты информации, имеет приведение расчетных величин к сопоставимым значениям, которое производится до расчетов. Приведение обеспечивает точность экономических расчетов и их обоснованность. Расчеты производятся в одинаковых единицах измерения, за одинаковые отрезки времени, на одинаковое количество объектов расчета.

Расчет экономического эффекта и эффективности защиты информации основывается на выявлении ущерба, нанесенного владельцу информации противоправным ее использованием, и позволяет оценить результативность защиты информации. Проведя анализ результатов расчетов, можно внести изменения в систему защиты информации для более эффективной ее защиты, недопущения разглашения охраняемой информации в дальнейшем, т.к. разглашение данной информации влечет за собой огромные убытки (ущерб) от контрафактного ее использования злоумышленником. В ущерб входит также потерянная владельцем информации выгода вследствие противоправного использования данной информации.

При расчетах данного ущерба применяются:

1) действительные цены на товары и услуги;

2) установленные законодательством нормативы платы за ресурсы;

3) установленные законодательством нормативы налогов; 52

4) правила и нормы расчетов физических и юридических лиц с банками;

5) ставки выплат установленных аналитическим путем для лицензионных платежей;

6) официальный курс котировки валют.

Поскольку осуществляемые затраты и получаемые результаты в течение всего срока противоправного использования информации неравноценны, то при расчетах осуществляется приведение к единому расчетному году. При расчёте экономической эффективности защиты информации можно использовать следующие формулы:

Пt Rt Ct Ht a t = (− −) (3.1)

где Пt – прибыль, оставшаяся в распоряжении нарушителя прав в течение года t;

Rt – выручка от реализации продукции, созданной на базе противоправного использования информации в году t;

Ct – себестоимость продукции, выпущенной в году t;

Ht – общая сумма налогов и других выплат, которые были произведены в году t.

tpta E−= 1(+) (3.2)

где a – коэффициент приведения разновременных результатов;

tp – год расчета;

E – коэффициент доходности капитала;

t – текущий год.

( )1tNtT tП = a × П ×= (3.3)

где ПТ – прибыль, оставшаяся в распоряжении злоумышленника за период использования на внутреннем рынке;

Пt – прибыль, оставшаяся в распоряжении злоумышленника в течение года t;

а – коэффициент приведения разновременных результатов.

э э в э D = Z × К − З (3.4)

где D э – доход от экспорта контрафактной продукции. Ущерб владельца информации;

Z э – валютная стоимость от экспорта продукции;

К в – курс валюты на дату расчета;

З э – затраты на изготовление экспортной продукции.

Робщ = Dэ + Пt (3.5)

где Робщ – общий ущерб владельца информации;

DЭ – ущерб владельца информации, понесенный при экспорте контрафактной продукции;

ПТ – прибыль, оставшаяся в распоряжении похитителя информации за период использования на внутреннем рынке.

Упр = Ср × Х × Робщ (3.6)

Где Упр – ущерб, понесенный владельцем информации из-за утраты возможности получения дохода на основе лицензионного соглашения;

Ср – среднестатистическая ставка роялти, дается в процентах от годовой прибыли;

Робщ – общий ущерб владельца информации.

Рсум =Упр + Робщ (3.7)

где Рсум – стоимостная оценка предотвращенного ущерба;

Упр – ущерб, понесенный владельцем информации из-за утраты возможности получения дохода на основе лицензионного соглашения;

Робщ – общий ущерб владельца информации.

а ЗИИРЭосумзи = (3.8)

где ЭЗИ – эффективность ЗИ;

Рсум – стоимостная оценка предотвращенного ущерба;

åЗЗИ – суммарные затраты на ЗИ.

Ответить на вопросы:

1. Аудит системы безопасности

2.Затраты на контроль;

3.Затраты на обеспечение соответствия принятым стандартам и требованиям, достоверности информации, действенности средств защиты

4. Затраты на идентификацию угроз безопасности

Лабораторная работа 5.

Методы и способы страхования информации, оценка эффективности защиты и страхования информации

Тема: Оценка экономического риска системы защиты информации.

Рассмотрена задача оценки экономического риска системы защиты информации для совокупности компьютеров, установленных в отдельном помещении, с учётом угроз, средств и мероприятий по защите информации. В перспективе новый импульс к развитию теории допустимого риска должен дать статистический метод оценки среднего риска информационной безопасности с учётом всего спектра угроз, средств и мероприятий по защите информации и их экономических последствий .

Рассмотрим задачу расчёта экономического риска системы защиты информации, когда объектом защиты является совокупность компьютеров, установленных в отдельном помещении, а предметом защиты – информация на их электронных носителях. Будем считать, что регистрируется пуассоновский поток компьютерных нарушений на интервале времени T, тогда вероятность совершения компьютерного нарушения на одном компьютере будет определяться формулой

$Pc = 1 - \exp\{-\lambda T\}$, (1)

где λ - интенсивность потока компьютерных нарушений;

$\lambda = m / N \cdot T$,

m и N – количество нарушений и количество компьютеров соответственно.

Примем, что Pc зависит от вероятности угрозы Py и вероятности защиты Pз в следующем виде

$Pc = Py \cdot (1 - Pз)$, (2)

$Py = Pпу \cdot (1 - Pпз)$, (3)

где Pпу – вероятность потенциальных факторов угрозы;

Pпз – вероятность предупреждения появления потенциальных факторов угрозы.

Тогда можно записать выражение для остаточного экономического риска угрозы

$Ry = Pc \cdot Уy$, (4)

где Уy – математическое ожидание экономического ущерба от всех компьютерных нарушений при реализации одной угрозы.

С учётом полного спектра угроз получим выражение для остаточного среднего экономического риска угроз информационной безопасности

$$Rcy = \sum_{i=1}^{n} Pci \cdot Уyi \quad (5)$$

и правило оценки допустимости уровня экономического риска$Rcy < Rcудоп = \nu \cdot D$, (6)

где Rcудоп – уровень допустимого экономического риска;

ν – норматив риска;

D – размер ежегодной экономической выгоды (дохода от информационных услуг) от применения информационной системы, оборудованной системой защиты информации.

В случаях страхования информационных средств, ресурсов или услуг определяется максимальное значение Rcум среднего экономического риска с заданной доверительной вероятностью. В частности, при использовании "правила трёх сигма" с учётом "затянутости хвостов" распределения значений ущерба, величина Rcум с вероятностью 0,95 определяется по формуле

$Rcум = Rcy + 3 \cdot \sigma$, (7)

где σ – среднее квадратическое значение экономического ущерба от всех реализованных угроз застрахованному имуществу или услугам.

С целью экспериментальной апробации изложенного подхода была разработана анкета компьютерных нарушений в составе 20 реквизитов, с использованием которой обследованы компьютерные классы 8 коммерческих вузов в течение 1 года, категория важности информации – КТ4. Объём выборки: 840 персональных компьютеров и 330 зарегистрированных компьютерных нарушений.

Все выявленные компьютерные нарушения сгруппированы по следующим видам источников угроз:

1. Отказы технических средств.
2. Сбои и отказы программных средств.
3. Поражения вирусами.
4. Случайные или преднамеренные нарушения студентов и сотрудников вуза.
5. Случайные или преднамеренные поступки внешних нарушителей.
6. Выбросы или отключения сети электропитания.
7. Другие источники, например, проверки представителями органов власти.
8. Природные источники (гроза, пожар, ураган, наводнение).

На рис. 1 представлены три группы вероятностей этих источников угроз:

Ант – вузы с высоким уровнем защиты информации; коммерческие вузы, где компьютерные классы практически не защищены;

КомвузПУ – расчётные вероятности потенциальных факторов угроз классам Комвуз. Вероятности источников угроз

0, 0,05, 0,1 ,0,15, 0,2, 0,25, 0,3, 0,35, 0,4, 0,45, 0,5

Значения вероятностей потенциальных факторов угроз определялись по формуле (3), где значения Рпз оценены экспертным путём в диапазоне 0,1-0,6.

Из сопоставления представленных зависимостей следует, что принятие мер по защите информации может позволить уменьшить в несколько раз вероятности реализации компьютерных нарушений.

На рис. 2. представлены экономические риски угроз, из рассмотрения которых следует, что повышение уровня защиты информации позволяет существенно снизить ущерб, в основном благодаря уменьшению количества отказов техники и количества инцидентов из-за внутренних и внешних нарушителей.

Составляющие риска, $0., 10, 20, 30, 40, 50, 60, 70, 80.

Результаты обработки анкет показали, что доля среднего риска составляет 15 % стоимости образовательных услуг, но может быть реально достигнут уровень остаточного среднего риска не более 3 %.

Оценка и управление рисками информационных систем

Обобщается опыт анализа рисков для информационных систем, излагаются существующие методики и приводятся новые методы анализа рисков для организаций.

Ключевые слова: анализ рисков, система защиты информации, преднамеренные и непреднамеренные угрозы, качественная оценка рисков, количественная оценка рисков, стоимость информационного ресурса, стратегия управления рисками.

Методология анализа рисков.

На практике сложились два подхода к организации систем защиты информации (СЗИ) на предприятиях. Первый подход характерен для организаций, ведущих обработку государственной тайны, и заключается в выполнении нормативных требований с привлечением специального оборудования и специальных организаций. Другой подход

относится к коммерческим организациям, обрабатывающим коммерческую и профессиональную (например, банковскую) тайны, и заключается в анализе рисков, в частности, в анализе существующей системы защиты информации. При построении системы защиты информации и при совершенствовании существующей СЗИ сегодня рекомендуется применение методологии анализа рисков, что предполагает количественный или качественный анализ рисков. Основой методологии анализа рисков на сегодняшний день является американский стандарт NIST [1], где приводится общая методология анализа рисков для организаций. В настоящее время существуют коммерческие программные продукты, которые оценивают риски для организаций и выдают некоторые рекомендации по усовершенствованию существующих систем.

Обычно такие программные продукты строятся на основе вопросных листов, после ответа на вопросы программа решает, какие меры следует предпринять. Можно выделить три программных продукта: CRAMM, RiskWatch, ГРИФ. Но не следует думать, что данные программные продукты рассчитаны для неподготовленных людей, они ориентированы на пользователей, обладающих специальной подготовкой и высокой квалификацией. Так, входными данными программного продукта CRAMM должна стать следующая информация: ресурсы системы (оценка их стоимости), угрозы (идентифицируются и оцениваются) и уязвимости[2]. Оценка производится согласно выбранной шкале. Далее программа предлагает варианты мер противодействия выявленным рискам.

Методики анализа рисков. Можно выделить три сформировавшихся направления анализа рисков:

• качественная оценка рисков;

• количественная оценка рисков;

Программные продукты, в которых может быть реализована как количественная и качественная оценка рисков, так и оба подхода сразу. Модель качественной оценки. Качественная оценка обычно сводится к введению некоторых качественных шкал оценки показателей для оценки важности информации (например, важная, критичная, жизненная) и оценки риска атаки (низкий, средний, высокий). Далее выбираются ресурсы с наибольшими показателями риска, они и подвергаются дополнительной защите.

Например, защищаются ресурсы с показателями важности информации (жизненная) и риском атаки (высоким).

Достоинства качественной оценки рисков:

• ускоряется и упрощается анализ рисков;

• нет необходимости оценивать в денежных единицах стоимость ресурса;

• нет необходимости вычислять вероятности проявления угрозы;

• нет необходимости вычислять соответствие применяемых мер угрозам.

Модель количественной оценки рисков. Количественная модель рисков оперирует такими понятиями, как:

• годоваячастотапроисшествия (англ. Annualized Rate of Occurrence – ARO);

• ожидаемыйединичныйущерб (англ. Single Loss Expectancy – SLE);

• ожидаемыйгодовойущерб (англ. Annualized Loss Expectancy – ALE),

величина, равная произведению ARO на SLE.

ALE=ARO′ SLE (1), где

ARO – частота появления события, приносящего ущерб в год. Данный показатель также можно назвать интенсивностью события.

SLE – показатель, который рассчитывается как произведение стоимости информации (AssetValue – AV) на фактор воздействия (англ.ExposureFactor – EF). Фактор воздействия – это размер ущерба или влияния на значение актива (от 0 до 1), то есть часть значения, которую актив потеряет в результате события.

SLE=AV′ EF. (2)

Управление рисками считается эффективным, если расходы на безопасность в год не превышают ожидаемый годовой ущерб.

Пример. Имеется предприятие с внутренней инфраструктурой общей стоимостью 200 000 дол. Пожар может нанести ущерб с фактором воздействия 0,3. Пожар может случиться раз в 10 лет. Тогда: SLE= 200000′ 0,3=60000, ALE= 60000′ 0,1=6000.

Таким образом, если предприятие тратит до 6000 дол.в год, то управление рисками осуществляется верно.

Модель обобщенного стоимостного результата Миоры. Модель Миоры разработана как альтернатива количественной модели рисков для улучшения и облегчения расчетов и вычислений. Одним из основных недостатков которой является ее вероятностная составляющая. Модель Миоры не учитывает вероятностей происшествия, она оперирует понятием ущерба от простоя как функцией времени после наступления события.

Для каждого информационного актива или группы сходных по ряду признаков активов, называемых категорией, определяется размер возможного ущерба, срок начала его влияния на организацию и распределённость по времени. Развитие картины ущерба можно представить в виде графика, где категории – это функции по двум осям: «время в днях»; «ущерб в деньгах». В результирующем графике представляются две кривые: суммарный ущерб организации при отсутствии защитных мероприятий; суммарный ущерб при наличии защитных мероприятий.

На таком графике наглядно видны необходимость и эффективность применяемых мер для обеспечения защиты информации.

Отечественный опыт оценки рисков. После того как в коммерческой фирме выявлены все носители конфиденциальной информации (КИ), по каждому (группам однотипных) носителю должен быть произведен анализ рисков в целях выявления слабых мест существующей СЗИ и более правильного распределения выделенных на защиту материальных средств. В работе [2] приводятся двухфакторный и трехфакторный анализы рисков, которые производятся по следующим формулам:

R = Рпроисшествия Спотери , (3)

R = Ругрозы Руязвимости Спотери , (4)

где R -риск, Рпроисшествия – вероятность происшествия, Ругрозы – вероятность возникновения угрозы, Руязвимости – вероятность потери информации (потеря трактуется широко: уничтожение, разглашение, уничтожение, модификации), Спотери – стоимость информации (цена потери).

Данная методика является шагом назад по сравнению с приведенной выше методикой количественной оценки рисков, так как последняя позволяет рекомендовать, сколько средств нужно тратить на защиту информации. А методология, указанная в работе [2],

лишь позволяет ранжировать риски. При этом в обоих случаях количественная оценка рисков осложняется тем, что не приводится никаких методик по вычислениям вероятностей (или частоты появления события) и цены информации. Но не понятно, чем должны руководствоваться привлекаемые эксперты, поэтому методика нуждается в объяснении, желательно близком к математическому, каждого показателя вероятности и стоимости информации.

Отдельно рассмотрим формулу (4), в которой автор разложил Р -происшествия на Р-угрозы и Р-уязвимости

Однако вероятности возникновения преднамеренных угроз в формуле (4) будут зависеть от вероятности уязвимости, поэтому данную формулу не всегда следует применять. Ругрозы будет зависеть от Руязвимости , поэтому следует более подробно подойти к анализу рисков, исходя из характера возникающих угроз. Таким образом, можно будет избежать ошибок, которые будут происходить по причине того, что вероятность происшествия и вероятность уязвимости будут не независимыми событиями.

Ответить на вопросы

1.Затраты на обслуживание системы безопасности (затраты на предупредительные мероприятия);

2.Затраты на планирование системы защиты информации

3. В чем заключается страхование и самострахование?

Учебно-методическое и информационное обеспечение дисциплины

Рекомендуемая литература

Перечень основной литературы

1. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ Шаньгин В.Ф.— Электрон.текстовые данные.— М.: ДМК Пресс, 2014.— 702 с.— Режим доступа: http://www.iprbookshop.ru/29257.— ЭБС «IPRbooks», по паролю

2. Прохорова О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ Прохорова О.В.— Электрон.текстовые данные.— Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014.— 113 с.— Режим доступа: http://www.iprbookshop.ru/43183.— ЭБС «IPRbooks», по паролю

Перечень дополнительной литературы

1. Кубанков А.Н. Система обеспечения информационной безопасности Российской Федерации: организационно-правовой аспект [Электронный ресурс]: учебное пособие/ Кубанков А.Н., Куняев Н.Н.— Электрон.текстовые данные.— М.: Всероссийский государственный университет юстиции (РПА Минюста России), 2014.— 78 с.— Режим доступа: http://www.iprbookshop.ru/47262.— ЭБС «IPRbooks», по паролю

2. Методы и средства инженерно-технической защиты информации [Электронный ресурс]: учебное пособие/ В.И. Аверченков [и др.].— Электрон.текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 187 с.— Режим доступа: http://www.iprbookshop.ru/7000.— ЭБС «IPRbooks», по паролю

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по выполнению лабораторных работ по дисциплине «Экономика защиты информации»

2. Методические рекомендации для студентов по организации самостоятельной работы

по дисциплине «Экономика защиты информации»

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

1. Национальный Открытый Университет. Интуит. http://www.intuit.ru;
2. Федеральный портал «Российское образование. http://www.edu.ru;
3. Российская государственная библиотека. http://www.rsl.ru;
4. Институт Юнеско по информационным технологиям в образовании. http://ru.iite.unesco.org/publications.