Содержание

Введение

В настоящее время организация эффективной системы защиты информационной системы становится критически важным стратегическим фактором развития любой компании. По сути, информация является одним из ключевых элементов бизнеса. При этом под информацией понимаются не только статические информационные ресурсы (базы данных, текущие настройки оборудования и другие), но и динамические информационные процессы обработки данных.

Главной целью любой системы защиты является обеспечение устойчивого функционирования объекта, предотвращение угроз его безопасности, защита законных интересов организации от противоправных посягательств, недопущение хищения финансовых средств, разглашения, утраты, утечки, искажения и уничтожения служебной информации, обеспечение нормальной производственной деятельности всех подразделений.

Информационная среда организации, вне зависимости от своего состава, должна предусматривать систему защиты. Однако затраты на обеспечение высокого уровня безопасности могут быть неоправданны. Нахождение разумного компромисса и выбор приемлемого уровня защиты при допустимых затратах является важным условием постановки задачи обеспечения ИБ. Для решения этого вопроса необходимо проводить анализ рисков ИБ, позволяющий оценить существующий уровень защищенности ресурсов организации. Значение риска, являющееся произведением вероятности реализации угрозы по отношению к защищаемому ресурсу на ущерб от реализации данной угрозы, служит показателем полноты, комплексности и эффективности системы ИБ организации, а также позволяет

выявить ее слабые места. При этом возникает ряд трудностей с интерпретацией экономических показателей для области ИБ. В связи с этим, изучение данной темы представляется актуальным.

Объектом исследования являются информационные риски, а предметом - расчет рисков информационной безопасности.

Цель работы - изучение методики расчета рисков информационной безопасности.

Реализация намеченной цели потребовала постановки и решения следующих задач, определивших логику и концепцию исследования:

- рассмотреть теоретические основы рисков информационной безопасности;
- изучить показатели и алгоритм расчета рисков по угрозе информационной безопасности;
- провести расчет информационных рисков на примере Web-сервера торговой компании.

1. Теоретические основы рисков информационной безопасности

.1 Сущность и способы оценки информационной безопасности

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, функционирующих под управлением СМИБ и процессов осознания ИБ, инициирующих и поддерживающих деятельность по менеджменту ИБ.

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.

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.

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.

В общем виде процесс проведения оценки ИБ представлен основными компонентами процесса: контекст, свидетельства, критерии и модель оценки.

Общий вид процесса оценки ИБ организации представлен на Рис. 1.

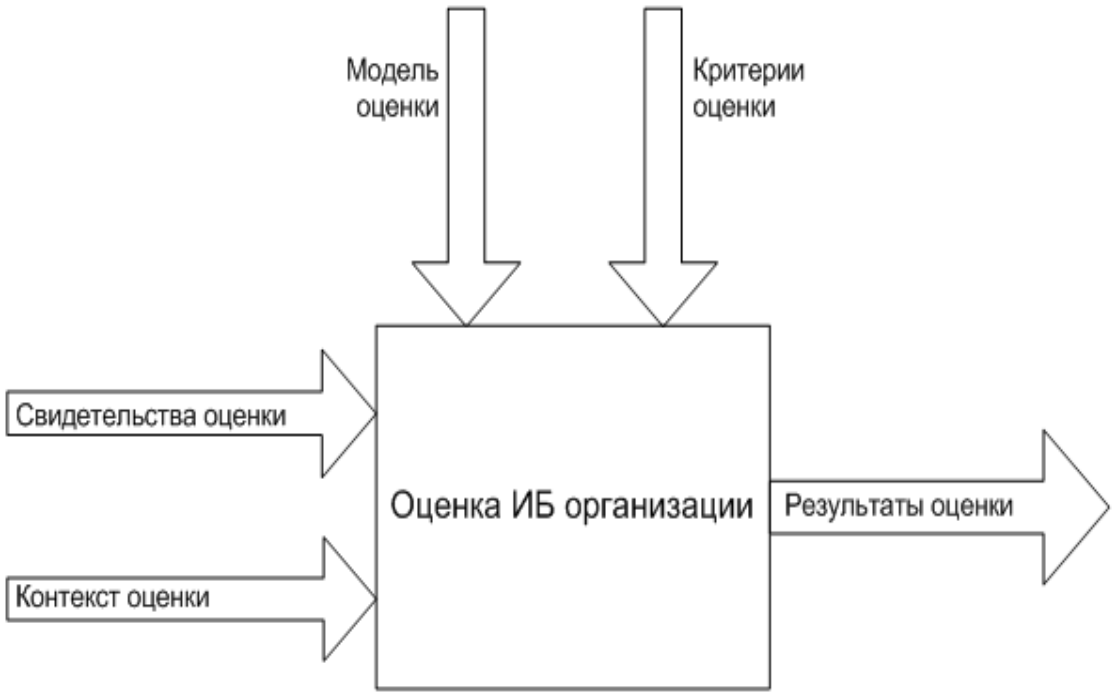

Рис. 1. - Общий вид процесса оценки ИБ организации

Возможны и другие цели проведения оценки ИБ:

– 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. [1]

В зависимости от выбранного для оценки ИБ критерия можно разделить способы оценки ИБ организации на оценку по эталону, риск-ориентированную оценку и оценку по экономическим показателям.

Классификация способов оценок информационной безопасности организации представлена на Рис. 2.

Рис. 2 - Способы оценки ИБ организации

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. [2]

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, показатели совокупной стоимости владения.

Под показателем совокупной стоимости владения 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 совокупной стоимости владения аналогичных организаций отрасли.

Оценка на основе показателя совокупной стоимости владения 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 совокупной стоимости владения, анализ областей обеспечения ИБ, выбор сравнимой модели совокупной стоимости владения в качестве критерия оценки, сравнение показателей с критерием оценки, формирование оценки ИБ. [3]

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 совокупной стоимости владения практически не применяется.

.2 Методы оценки информационных рисков

Информационные риски - это опасность возникновения убытков или ущерба в результате применения компанией информационных технологий.

Иными словами, IT-риски связаны с созданием, передачей, хранением и использованием информации с помощью электронных носителей и иных средств связи. риски делятся на две категории:

– риски, вызванные утечкой информации и использованием ее

конкурентами или сотрудниками в целях, которые могут повредить бизнесу;

– риски технических сбоев работы каналов передачи информации, которые могут привести к убыткам.

Работа по минимизации IT-рисков заключается в предупреждении несанкционированного доступа к данным, а также аварий и сбоев оборудования.

Процесс минимизации IT-рисков рассматривается комплексно: сначала выявляются возможные проблемы, а затем определяется, какими способами их можно решить.

Сейчас используются различные методы оценки информационных рисков отечественных компаний и управления ими.

Оценка информационных рисков компании может быть выполнена в соответствии со следующим планом:

– идентификация и количественная оценка информационных ресурсов компании, значимых для бизнеса;
– оценивание возможных угроз;
– оценивание существующих уязвимостей;
– оценивание эффективности средств обеспечения информационной безопасности.

Риски характеризуют опасность, которая может угрожать компонентам корпоративной информационной системы.

Информационные риски компании зависят от:

– показателей ценности информационных ресурсов;

– вероятности реализации угроз для ресурсов;

– эффективности существующих или планируемых средств обеспечения информационной безопасности.

Цель оценивания рисков состоит в определении характеристик рисков корпоративной информационной системы и ее ресурсов.

После оценки рисков можно выбрать средства, обеспечивающие

желаемый уровень информационной безопасности компании. При оценивании рисков учитываются такие факторы, как ценность ресурсов, значимость угроз и уязвимостей, эффективность имеющихся и планируемых средств защиты.

Возможность реализации угрозы для некоторого ресурса компании оценивается вероятностью ее реализации в течение заданного отрезка времени. При этом вероятность того, что угроза реализуется, определяется следующими основными факторами:

– привлекательностью ресурса (учитывается при рассмотрении угрозы от умышленного воздействия со стороны человека);

– возможностью использования ресурса для получения дохода (также в случае угрозы от умышленного воздействия со стороны человека);

– техническими возможностями реализации угрозы при умышленном воздействии со стороны человека;

– степенью легкости, с которой уязвимость может быть использована. [2]

В России в настоящее время чаще всего используются разнообразные «бумажные» методики, достоинствами которых являются гибкость и адаптивность. Как правило, разработкой данных методик занимаются компании - системные и специализированные интеграторы в области защиты информации.

Специализированное ПО, реализующее методики анализа рисков, может относиться к категории программных продуктов (имеется на рынке) либо являться собственностью ведомства или организации и не продаваться.

Если ПО разрабатывается как программный продукт, оно должно быть в достаточной степени универсальным. Ведомственные варианты ПО адаптированы под особенности постановок задач анализа и управления

рисками и позволяют учесть специфику информационных технологий организации.

Предлагаемое на рынке ПО ориентировано в основном на уровень информационной безопасности, несколько превышающий базовый уровень защищенности. Таким образом, инструментарий рассчитан в основном на потребности организаций 3-4 степени зрелости, описанных в первой главе.

Для решения данной задачи были разработаны программные комплексы анализа и контроля информационных рисков: CRAMM, FRAP, RiskWatch, Microsoft, ГРИФ. Ниже приведены краткие описания ряда распространенных методик анализа рисков.

Распространенные методики анализа рисков:

– методики, использующие оценку риска на качественном уровне (например, по шкале «высокий», «средний», «низкий»). К таким методикам, в частности, относится FRAP;

– количественные методики (риск оценивается через числовое значение, например размер ожидаемых годовых потерь). К этому классу относится методика RiskWatch;

– методики, использующие смешанные оценки (такой подход используется в CRAMM, методике Microsoft и т.д.). [4]

Методика CRAMM одна из первых зарубежных работ по анализу рисков в сфере информационной безопасности, разработанная в 80-х гг.

Ее основу составляет комплексный подход к оценке рисков, сочетающий количественные и качественные методы анализа. Метод является универсальным и подходит как для крупных, так и для малых организаций, как правительственного, так и коммерческого сектора. Версии программного обеспечения CRAMM, ориентированные на разные типы организаций, отличаются друг от друга своими базами знаний (профили):

– коммерческий профиль;

– правительственный профиль.

При работе методики на первых этапах учитывается ценность ресурсов исследуемой системы, собираются первичные сведения о конфигурации системы. Проводится идентификация ресурсов: физических, программных и информационных, содержащихся внутри границ системы.

Результатом этого этапа является построение модели системы, с деревом связи ресурсов. Эта схема позволяет выделить критичные элементы. Ценность физических ресурсов в CRAMM определяется стоимостью их восстановления в случае разрушения.

Ценность данных и программного обеспечения определяется в следующих ситуациях:

– недоступность ресурса в течение определенного периода времени;

– разрушение ресурса - потеря информации, полученной со времени последнего резервного копирования, или ее полное разрушение;

– нарушение конфиденциальности в случаях несанкционированного доступа штатных сотрудников или посторонних лиц;

– модификация - рассматривается для случаев мелких ошибок персонала (ошибки ввода), программных ошибок, преднамеренных ошибок;

– ошибки, связанные с передачей информации: отказ от доставки, недоставка информации, доставка по неверному адресу.

Методика CRAMM рекомендует использовать следующие параметры:

– ущерб репутации организации;

– нарушение действующего законодательства;

– ущерб для здоровья персонала;

– ущерб, при разглашении персональных данных отдельных лиц;

- финансовые потери от разглашения информации;
- финансовые потери, связанные с восстановлением ресурсов;
- потери, связанные с невозможностью выполнения обязательств;
- дезорганизация деятельности.

На второй стадии рассматривается все, что относится к идентификации и оценке уровней угроз для групп ресурсов и их уязвимостей. В конце стадии заказчик получает идентифицированные и оцененные уровни рисков для своей системы. На этой стадии оцениваются зависимость пользовательских сервисов от определенных групп ресурсов и существующий уровень угроз и уязвимостей, вычисляются уровни рисков и анализируются результаты.

Ресурсы группируются по типам угроз и уязвимостей. Программное обеспечение CRAMM для каждой группы ресурсов и каждого из 36 типов угроз генерирует список вопросов, допускающих однозначный ответ.

Уровень угроз оценивается, в зависимости от ответов, как очень высокий, высокий, средний, низкий и очень низкий. Уровень уязвимости оценивается, в зависимости от ответов, как высокий, средний и низкий.

На основе этой информации рассчитываются уровни рисков в дискретной шкале с градациями от 1 до 7. Полученные уровни угроз, уязвимостей и рисков анализируются и согласовываются с заказчиком.

Основной подход, для решения этой проблемы состоит в рассмотрении:

- уровня угрозы;
- уровня уязвимости;
- размера ожидаемых финансовых потерь.

Исходя из оценок стоимости ресурсов защищаемой ИС, оценок угроз и уязвимостей, определяются «ожидаемые годовые потери».

Третья стадия исследования поиск варианта системы безопасности, наилучшим образом удовлетворяющей требованиям заказчика.

На этой стадии CRAMM генерирует несколько вариантов мер противодействия, адекватных выявленным рискам и их уровням.

Таким образом, CRAMM - пример методики расчета, при которой первоначальные оценки даются на качественном уровне, и потом производится переход к количественной оценке (в баллах).

Работа по методике CRAMM осуществляется в три этапа, каждый из которых преследует свою цель в построении модели рисков информационной системы в целом. Рассматриваются угрозы системы для конкретных ее ресурсов. Проводится анализ как программного, так и технического состояния системы на каждом шаге, построив дерево зависимостей в системе, можно увидеть ее слабые места и предупредить потерю информации в результате краха системы, как из за вирусной атаки, так и при хакерских угрозах.

Недостатки метода CRAMM:

- использование метода CRAMM требует специальной подготовки и высокой квалификации аудитора;
- CRAMM в гораздо большей степени подходит для аудита уже существующих ИС, находящихся на стадии эксплуатации, нежели чем для ИС, находящихся на стадии разработки;
- аудит по методу CRAMM - процесс достаточно трудоемкий и может потребовать месяцев непрерывной работы аудитора;
- программный инструментарий CRAMM генерирует большое количество бумажной документации, которая не всегда оказывается полезной на практике;
- CRAMM не позволяет создавать собственные шаблоны отчетов или модифицировать имеющиеся;
- возможность внесения дополнений в базу знаний CRAMM не

доступна пользователям, что вызывает определенные трудности при адаптации этого метода к потребностям конкретной организации;

– программное обеспечение CRAMM существует только на английском языке;

– высокая стоимость лицензии. [5]

.3 Показатели и алгоритм расчета рисков по угрозе информационной безопасности

На первом этапе рассчитываем уровень угрозы по уязвимости $T_h T_h$ на основе критичности и вероятности реализации угрозы через данную уязвимость. Уровень угрозы показывает, насколько критичным является воздействие данной угрозы на ресурс с учетом вероятности ее реализации.

Для режима с одной базовой угрозой:

$$T_h = \frac{ER}{100} \times \frac{P(V)}{100} T_h = \frac{ER}{100} \times \frac{P(V)}{100}, \quad (1)$$

где $T_h T_h$ - уровень угрозы по уязвимости;- критичность реализации угрозы, %;(V) - вероятность реализации угрозы через данную уязвимость, %.

Для режима с тремя базовыми угрозами используются следующие формулы:

$$T_{h_c} = \frac{ER_c}{100} \times \frac{P(V)_c}{100} T_{h_c} = \frac{ER_c}{100} \times \frac{P(V)_c}{100}, \quad (2)$$

где $T_{h_c} T_{h_c}$ - уровень угрозы по уязвимости конфиденциальности;

$ER_c ER_c$ - критичность реализации угрозы конфиденциальности, %;

$P(V)_c \ P(V)_c$ - вероятность реализации угрозы конфиденциальности, %.

$$T_{h_i} = \frac{ER_i}{100} \times \frac{P(V)_i}{100} T_{h_i} = \frac{ER_i}{100} \times \frac{P(V)_i}{100}, \quad (3)$$

где $T_{h_i} T_{h_i}$ - уровень угрозы по уязвимости целостности;

$ER_i ER_i$ - критичность реализации угрозы целостности, %;

$P(V)_i P(V)_i$ - вероятность реализации угрозы целостности, %.

$$T_{h_a} = \frac{ER_a}{100} \times \frac{P(V)_a}{100} T_{h_a} = \frac{ER_a}{100} \times \frac{P(V)_a}{100}, \quad (4)$$

где $T_{h_a} T_{h_a}$ - уровень угрозы по уязвимости доступности;

$ER_a ER_a$ - критичность реализации угрозы доступности, %;

$P(V)_a P(V)_a$ - вероятность реализации угрозы доступности, %.

Значения уровня угрозы по уязвимости находятся в интервале от 0 до 1.

Чтобы рассчитать уровень угрозы по нескольким уязвимостям, через которые возможна реализация данной угрозы на ресурсе, нужно просуммировать полученные уровни угроз через конкретные уязвимости.

Для режима с одной базовой угрозой используется формула:

$$cT_h = 1 - \prod_{i=1}^{n} \left(1 - T_{h_i}\right) cT_h = 1 - \prod_{i=1}^{n} \left(1 - T_{h_i}\right), \quad (5)$$

где - уровень угрозы по нескольким уязвимостям;

$T_h T_h$ - уровень угрозы по уязвимости.

Значения уровня угрозы по нескольким уязвимостям находятся в интервале от 0 до 1.

Для режима с тремя базовыми угрозами:

$$cT_{h_c} = 1 - \prod_{j=1}^{n}\left(1 - T_{h_{c,j}}\right) cT_{h_c} = 1 - \prod_{j=1}^{n}\left(1 - T_{h_{c,j}}\right), \quad (6)$$

где - уровень угрозы по нескольким уязвимостям по критерию угрозы конфиденциальности;

$T_{h_{c,j}} T_{h_{c,j}}$ - уровень угрозы по уязвимости конфиденциальности.

$$cT_{h_i} = 1 - \prod_{j=1}^{n}\left(1 - T_{h_{i,j}}\right) cT_{h_i} = 1 - \prod_{j=1}^{n}\left(1 - T_{h_{i,j}}\right), \quad (7)$$

где - уровень угрозы по нескольким уязвимостям по критерию угрозы целостности;

$T_{h_{i,j}} T_{h_{i,j}}$ - уровень угрозы по уязвимости целостности.

$$cT_{h_a} = 1 - \prod_{j=1}^{n}\left(1 - T_{h_{a,j}}\right) cT_{h_a} = 1 - \prod_{j=1}^{n}\left(1 - T_{h_{a,j}}\right), \quad (8)$$

где - уровень угрозы по нескольким уязвимостям по критерию угрозы доступности;

$T_{h_{a,j}} T_{h_{a,j}}$ - уровень угрозы по уязвимости доступности;

Значения уровня угрозы по всем уязвимостям находятся в интервале от 0 до 1.

Аналогично рассчитывается общий уровень угроз по ресурсу (учитывая все угрозы, действующие на ресурс):

Для режима с одной базовой угрозой:

$$cT_h R = 1 - \prod_{i=1}^{n}\left(1 - T_{h_i}\right) cT_h R = 1 - \prod_{i=1}^{n}\left(1 - T_{h_i}\right), (9)$$

где - уровень угрозы по ресурсу;

$T_h T_h$ - уровень угрозы по уязвимости.

Значение общего уровня угрозы находятся в интервале от 0 до 1.

Для режима с тремя базовыми угрозами используются следующие формулы:

$$cT_h R_c = 1 - \prod_{j=1}^{n}\left(1 - CT_{h_{c,j}}\right) cT_h R_c = 1 - \prod_{j=1}^{n}\left(1 - CT_{h_{c,j}}\right), (10)$$

где $T_{h_{c,j}} T_{h_{c,j}}$ - уровень угрозы по уязвимости конфиденциальности; уровень угрозы конфиденциальности по всем угрозам ресурса.

$$cT_h R_i = 1 - \prod_{j=1}^{n}\left(1 - CT_{h_{i,j}}\right) cT_h R_i = 1 - \prod_{j=1}^{n}\left(1 - CT_{h_{i,j}}\right), (11)$$

где $T_{h_{i,j}} T_{h_{i,j}}$ - уровень угрозы по уязвимости целостности; уровень угрозы целостности по всем угрозам ресурса.

$$cT_h R_a = 1 - \prod_{j=1}^{n}\left(1 - T_{h_{a,j}}\right) cT_h R_a = 1 - \prod_{j=1}^{n}\left(1 - T_{h_{a,j}}\right), (12)$$

где $T_{h_{a.j}}$ $T_{h_{a.j}}$ - уровень угрозы по уязвимости доступности;
уровень угрозы доступности по всем угрозам ресурса.
Значение общего уровня угрозы находится в интервале от 0 до 1.
Риск по ресурсу R рассчитывается следующим образом:
Для режима с одной базовой угрозой:

$$R = CT_hR \times D \; R = CT_hR \times D \quad (13)$$

где D - критичность ресурса (задается в деньгах или уровнях);

CT_hR CT_hR - общий уровень угроз по ресурсу.

Если риск задается в уровнях, то в качестве значения критичности берется оценка уровня.

В случае угрозы доступности (отказ в обслуживании) критичность ресурса в год вычисляется по следующей формуле:

$$D_{\frac{a}{год}} = D_{\frac{a}{час}} \times T_{\max} \square \; D_{\frac{a}{год}} = D_{\frac{a}{час}} \times T_{\max} \square \quad (14)$$

где $D_{\frac{a}{год}}$ $D_{\frac{a}{год}}$ - критичность ресурса по угрозе доступности в год;
$D_{\frac{a}{час}}$ $D_{\frac{a}{час}}$ - критичность ресурса по угрозе доступности в час;
$T_{\max} \square$ $T_{\max} \square$ - максимальное критическое время простоя ресурса в год.

Для остальных угроз критичность ресурса задается в год.

В результате работы алгоритма просчета угроз пользователь системы получает следующие данные:

- риск реализации по трем базовым угрозам (или по одной суммарной угрозе) для ресурса;
- риск реализации суммарно по всем угрозам для ресурса;
- риск реализации по трем базовым угрозам (или по одной суммарной угрозе) для информационной системы;
- риск реализации по всем угрозам для информационной системы;
- риск реализации по всем угрозам для информационной системы после задания контрмер;

- эффективность контрмер;
- эффективность комплекса контрмер. [6]

2. Расчет информационных рисков на примере сервера Web торговой компании

Расчет качественных значений информационных рисков проводится на примере сервера Web торговой компании, занимающейся продажей компьютерной техники через собственный Internet-магазин. Можно предположить, что годовой торговый оборот составляет 100 тыс. долл. США в год. В качестве сервера Web используется ПО Microsoft IIS и СУБД Microsoft SQL Server.

Для упрощения расчета принимается две модели нарушителей: внешний легальный пользователь и внешний хакер.

Первый обознается как A1, второй - A2.

Для категории A1 свойственны следующие черты нарушителя:

- достаточная квалификация для эксплуатации возможностей Internet- магазина;
- отсутствие цели нанести ущерб компании;

Для категории A2 свойственны следующие черты нарушителя:

- необходимые технические познания для эксплуатации возможностей Internet-магазина;
- навыки и опыт использования уязвимостей и недекларированных возможностей ОС, распространенного прикладного ПО;
- опыт взлома подобных систем;
- намерение нанести ущерб компании. [4]

В отношении сервера Web могут быть идентифицированы следующие угрозы:

- нарушение целостности информации, хранящейся в СУБД Internet-магазина;

– нарушение доступности сервера Web;

– нарушение конфиденциальности информации, хранящейся в СУБД Internet-магазина.

Каждая из названных угроз может возникнуть в результате проведения атак SQL Injection и Cross-Site Scripting и эскалации привилегий злоумышленника в системе в результате переполнения буфера ОС или СУБД.

Атака наподобие SQL Injection может быть намеренно осуществлена злоумышленником категории A2, но не может быть проведена ни при каких обстоятельствах злоумышленником категории A1.

Атака Cross-Site Scripting может быть предпринята злоумышленником категории A2, но ни в коем случае не злоумышленником категории A1.

Эскалация привилегий прав злоумышленника в системе может произойти в результате намеренных действий злоумышленника категории A2 и ненамеренных действий злоумышленника категории A1.

Создание шторма сетевых пакетов, направленных на сервер Web, может стать следствием намеренных действий злоумышленника категории A2 и ненамеренных действий злоумышленника категории A1 (например, вследствие частого нажатия кнопки «Обновить» обозревателя Internet).

Формирование некорректных пакетов, направленных на сервер Web, влекущих за собой крах службы, может произойти в результате намеренных действий злоумышленника категории A2, но ни при каких обстоятельствах не случится в результате действий злоумышленника категории A1.

Ресурс сервера Web является критичным для функционирования компании, поэтому ему присвоено значение AV = 3. Мере уязвимости ресурса к угрозе нарушения целостности) тоже назначено максимальное значение (3), так как нарушение целостности хранимых в СУБД данных влечет за собой срыв поставок, если, например, удалены данные об оформленных, но еще не

проведенных заказах. Вероятность реализации угрозы нарушения целостности оценена как средняя ввиду того, что не исключается эксплуатация широко известных уязвимостей и недостатков программирования (SQL). Параметры в отношении угроз нарушения конфиденциальности и доступности рассчитывались аналогично. Большинство параметров принимались исходя из экспертного мнения аудитора. Все идентифицированные риски являются высокими, поскольку реализация порождающих эти риски угроз неизбежно нанесет существенный ущерб компании. Таким образом, дальнейшие меры подразумевают снижение идентифицированных рисков. [3]

Для снижения меры уязвимости в части реализации угрозы нарушения доступности рекомендуется пересмотреть исходный код сценариев Internet-магазина и добавить в него функции фильтрации запросов SQL с целью предотвращения внедрения запросов SQL в запросы http GET. Сходные меры могут быть предприняты в отношении атаки Cross-Site Scripting.

Что касается эскалации привилегий злоумышленника, то на этот случай могут быть приняты такие меры, как установка недавно вышедших обновлений безопасности службы сервера Web, а также постоянный аудит и периодический пересмотр учетных записей пользователей и прав доступа на системном уровне. В результате этих действий автоматически снижается параметр доступности, установка обновлений безопасности уменьшает вероятность реализации описанных угроз. Снижение степени уязвимости и вероятности реализации угрозы в части нарушения конфиденциальности достигается аналогично.

Риск нарушения доступности понижается путем установки обновлений безопасности, размещения межсетевого экрана перед сервером Web с учетом топологии сети и ограничения количества одновременных соединений со

службой сервера Web с одного IP-адреса.

После идентификации перечисленных мер произведем расчет остаточных рисков. Их величина снизится от 66 до 83 %, что является приемлемым уровнем. Затраты на внедрение описываемых мер составят: доработка сценариев сервера Web 56 человеко-часов и финансовых вложений 5000 долл. США, установка межсетевого экрана: трудозатраты в 112 человеко-часов и 10 тыс. долл. Таким образом, общие затраты на внедрение предложенных мер - 168 человеко-часов и 15 тыс. долл.

Затраты на снижение информационных рисков будут экономически оправданы, если уровень экономической безопасности предприятия позволит сохранить стабильность рентабельности анализируемого предприятия.

В примере, где годовой оборот Internet-магазина составляет 100 тыс. долл. и среднегодовой уровень рентабельности 38 %, затраты на информационную безопасность (информационный риск) в размере 15 тыс. долл. хотя и высоки, но вполне оправданы.

Заключение

В данной курсовой работе были рассмотрены теоретические основы рисков информационной безопасности, выявлены основные способы ее оценки, также были освещены наиболее распространенные методики расчета оценки рисков информационной безопасности.

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

В курсовой работе детально рассмотрена одна из самых распространенных и широко используемых методик - методика CRAMM, а также выполнен расчет информационных рисков по этой методике на примере сервера Web торговой компании.

Работа по методике CRAMM осуществляется в три этапа, каждый из которых преследует свою цель в построении модели рисков информационной системы в целом.

Результатом работы алгоритма просчета угроз для пользователя системы являются следующие данные:

- риск реализации по трем базовым угрозам (или по одной суммарной угрозе) для ресурса;
- риск реализации суммарно по всем угрозам для ресурса;
- риск реализации по трем базовым угрозам (или по одной суммарной угрозе) для информационной системы;
- риск реализации по всем угрозам для информационной системы;
- риск реализации по всем угрозам для информационной системы

после задания контрмер;

- эффективность контрмер;
- эффективность комплекса контрмер.

Список сокращенных обозначений

ИБ - информационная безопасность

ИС - информационная система

ПО - программное обеспечение

ПО - программное обеспечение

СМИБ - системы менеджмента информационной безопасности

СОИБ - система обеспечения информационной безопасности

СУБД - система управления базами данных

США - Соединенные Штаты Америке

http - hyper text transport protocol, протокол передачи гипертекстовых сообщений

IP - internet protocol, интернет-протокол

IT- information technologies, информационные технологии

SQL - Structured Query Language, язык структурированных запросов

Web - сеть

Список использованных источников

1 Абрамова М.А. Информационные технологии [Текст]: - М.: ЛОГОС, 2011.

2 Белоглазова Г.Н. Информационные технологии [Текст]: - М.: Высшее образование, 2011.

3 Жукова Е.Ф. Информационные технологии [Текст]: - М.: ЮНИТИ, 2012.

4 Лаврова О.И. Информационные технологии [Текст]: - М.: Юрайт, 2008.

Макеев С.Р. Информационные технологии: теория и практика [Текст]: - М.: Парус, 2009.

Свиридов О.Ю. Информационные технологии [Текст]: - М: Ростов н/Д: Март, 2009.