Висновок. Для проекту системи повинен бути проведений вибір однієї або декіль відповідних моделей життєвого циклу. Необхідно встановити, є модель життєвого цик програмного механізму захисту складовою частиною моделі життєвого циклу КСЗІ. Кожн модель життєвого циклу має процеси, які можуть бути виконані послідовно, повторно аб комбіновано. Процеси повинні бути відображені в моделі, яка обрана, з точки зору створен модифікованого, структурованого і запланованого продукту. Результати одного процесу моделі життєвого циклу повинні бути передані наступному. В цьому випадку відповід документи створюються до закінчення визначеного процесу та початку наступної роботи.

Список літератури:

1. Павлов І.М. Неформальний опис життєвого циклу комплексної системи захисту інформації [Текст] І.М. Павлов, В.О. Бірюков // Сучасний захист інформації. – Киев.: 2011. – № 2. – С. 58 – 69.
2. Жук К.Д. Системные методы в программировании жизненных циклов новой техники [Текст] / К.Д Жук // Автоматизация проектирования сложных систем. – Москва.: 1999. – С. 15-26.
3.Хорошко В.А. Модель системы защиты информации [Текст] / В.А. Хорошко // Захист інформації. Київ.: 1999. – №. 1. – С. 5 – 11.
4. Третьякова О.О. Модель комплексной системы защиты информации [Текст] / О.О. Третьякова Сборник научных трудов НАУ "Защита информации". – Киев.: 2002. – Вып. 1. – С. 3 – 10.
5. Павлов И.Н. Проектирование систем защиты информации. Фор-мальный подход [Текст] / И.Н Павлов // "Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні". – Київ 2005. – Вип. 11. – С. 54 – 59.
6. Михайлов С.Ф. Информационная безопасность. Защита информации в автоматизированны системах. Основные концепции. / С.Ф. Михайлов, В.А. Петров, Ю.А. Тимофеев // – М.: Связь, 1995. – 56 с.
7. Герасименко В.А. Комплексная защита информации в современных средствах обработк информации / В.А. Герасименко // Зарубежная радиоэлектроника. – Москва.: 1993. – № 2. – С. 35 – 38.
8. Малюк А.А. Информационная безопасность: Концептуальные и методологические основы защит информации. / А.А. Малюк // – М.: Высшая школа, 2004. – 280 с.
9. Павлов І.М., Радзівілов Г.Д. Формальное описание процесса проектирования комплексных систе защиты информации в информационно − телекоммуникационных системах [Текст] // Вісник ДУІКТ. Київ 2010. – Т. 8. – №1. – С.84 – 93.

В статті розглянуті моделі життєвого циклу програмних механізмів захисту, які є основою у складі КСЗІ
Ключові слова: комплексна система захисту інформації, моделі життєвого циклу, проектування програмні механізми захисту інформації.

В статье рассмотрены модели жизненного цикла программных механизмов защиты, которые являютс основою в составе КСЗИ.
Ключевые слова: комплексная система защиты информации, модели жизненного цикла, проектирование программные механизмы защиты информации.

The models of life cycle of protection program mechanisms as a part of complex system of informatio protection are highlighted in the article.
Keywords: complex system of information protection, life cycle model, designing, program mechanisms o information protection.

Рецензент: д.т.н., проф. Лєнков С.В
Надійшла 28.01.201

УДК 004.347.7
Скачек Л.Н. (ДУІКТ)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

Анализ состояния проблемы и постановка задачи исследования. В последнее врем наблюдается активизация процесса приватизации промышленных предприятий Украины, чт приводит к образованию на них нового негосударственного сектора информационного ресурса Указанный сектор охватывает коммерческую (промышленную) тайну предприятия и по своем правовому статусу и области применимости принципиально отличается от традиционного дл

интервал или момент времени не ниже значения требуемой вероятности $P_т$ ее защиты при имеющихся ассигнованиях на создание системы защиты. Этот процесс может быть более приближаемым и реальным условием, если применить для этого модели СЗИ [3].

Основой экономического анализа СЗИ на стадии ее формирования является избранный предприятием вариант оптимизационной модели, позволяющий исследовать взаимосвязь между ассигнованиями на организацию ЗИ и эффективностью ее защиты. Известны два подхода к использованию упомянутой модели [6]:

- прямая постановка оптимизационной задачи - обеспечить требуемый уровень $P_т$ ЗИ при минимальных затратах C_{min} т. е.

$$\begin{cases} C_{min} \to \min \\ P_З \geq P_т \end{cases}$$

- обратная постановка оптимизационной задачи – обеспечить максимальный уровень $P_П$ ЗИ при ограниченных ассигнованиях $C_{ОТ}$, т.е.

$$\begin{cases} P_З \to \max \\ \tilde{N}_{ЮЗ} \leq \tilde{N}_{min} \end{cases}$$

Первый из рассмотренных подходов характерен для организации защиты государственной и (или) служебной тайны; второй - предпочтителен при организации защиты коммерческой тайны.

Далее рассмотрим две основные задачи экономического анализа СЗИ: определение условий экономической целесообразности ЗИ и технико-экономическая оценка СЗИ.

Формулировка условий экономической целесообразности ЗИ в сферах ее обращения на предприятии зависит от характера и размеров потенциального ущерба, причиняемого интересам предприятия несанкционированной утечки или разглашение информации. Рассматривая в качестве упомянутого ущерба упущенную выгоду предприятия, примем в качестве условия неравенство вида:

$$C_{ЮЗ} \leq \beta У$$

где $У$ - величина характеризующая упущенную выгоду предприятия ($C_{ОТ}$ выражается в ее единицах измерения); β - статистический коэффициент, учитывающий затраты ресурсов организацию ЗИ.

При затруднении с оценкой величины $У$ может быть избран другой путь, основанный определении размера прибыли П, получаемой предприятием за счет обладания конкретным информации. Условие (1) экономической целесообразности ЗИ трансформируется в этом слу виду:

$$C_{ОТ} < \beta П$$

Допустимые пределы коэффициента $0,05 < \beta < 0,20$ (как в неравенствах (2) и (3)) соответствуют мировой практике.

Согласно [7] соотношение между величинами C_{0T} и $У$ (C_{0T} и $П$), когда затраты ресурсов C_{0T} на ЗИ составляют от 5 до 20 % величины упущенной выгоды $У$ или прибыли П, обусловленной указанными выше факторами, считается оптимальным. Если указанные ассигнования менее 5 %, то предприятие рискует своей экономической безопасностью; если же затраты превышают 20 %, целесообразно пересмотреть технологию ЗИ.

Технико-экономическая оценка СЗИ является, по существу, процедурой комплексной оценки СЗИ, позволяющей, во-первых, ранжировать альтернативные варианты СЗИ, удовлетворяющие моделям [3], по величине показателя их технико-экономической эффективности, во-вторых, произвести выбор предпочтительного варианта СЗИ, руководствуясь избранным решающим правилом.

Показатель технико-экономической j-го варианта СЗИ представляет собой зависимость

$$Ýj = \Delta j / C_{îò}, \quad Ñ_{îò} \succ 0 \qquad (3)$$

где Δj - приращение контролируемой характеристике эффективности СЗИ, обусловленное ЗИ; C_{0Ti} - количество i-тих ассигнований, затраченных на ЗИ.

Стратегия выбора предпочтительного варианта СЗИ специфицируется множеством правил вида $â: \{Ý_j\} \to \max \qquad (4)$

где левая часть в скобках составляет условие, а правая - определяет действие.

Следуя логике рассуждений [7], конкретизируем свойства ассигнований на реализацию СЗИ. Допустим, что ассигнования потребности предприятия на СЗИ выражаются матрицей $C_{\min} = \|C_{ij}\|$ размерности N x M, имеющей, по крайней мере, один нулевой элемент в строке и столбце.

Здесь C_{ij} - минимальное количество i-го ассигнования для реализации j-го варианта СЗИ; M - число альтернативных вариантов СЗИ; N - число ассигнований, который распределяются по указанным вариантам СЗИ.

Аналогично вышеизложенному запишем матрицу фактических возможностей предприятия на ассигнования:

$$C_{\min} = \|C_{ij}\| \; ðàçìåðíîñòè \quad è \quad N \times M$$

где C_{ij} - фактическое количество i-го ресурса для реализации j-го варианта СЗИ.

Очевидно, что идеальной является ситуация, когда потребности ассигнований $C_{\min}$ на СЗИ совпадают с фактическими ресурсными возможностями C_{OT} предприятия.

Практический интерес для предприятия представляет также ситуация, при которой возможно некоторое замещение i-го ассигнования с относительной эффективностью $Э_{ij}$ эквивалентная ей ассигнованием A с эффективностью $Э_{iα}$.

В случае, когда рассмотренное замещение ассигнований не возможно, их распределение осуществляется согласно тривиальному правилу $C_{ij} = n_{ij}$. Индексом n_{ij} здесь обозначено число единиц i-го ассигнования, распределенного по j-му варианту СЗИ при условии

$$\sum_{j=1}^{M} n_{ij} \le n_i, \quad i = \overline{\alpha N},$$

где n_i - число условно неделимых (с позиции удобства измерения в рамках рассматриваемой проблемы) единиц каждого /-го ассигнования.

Принимая во внимание изложенное, представляется возможным преобразовать зависимость (3) к виду, учитывающему рассмотренные выше свойства ассигнований и позволяющие использовать приоритетные изменения приращения контролируемой характеристики эффективности СЗИ, обусловленной ЗИ, и количество i-го ассигнования, затрагиваемое на ЗИ. Простейшая модификация такого показателя, обеспечивающая возможность анализа альтернативных вариантов СЗИ в терминах "стоимость - эффективность", выглядит согласно [7] так:

$$\acute{Y}_j = \sum_{j=1}^{M} \alpha_i f_i / \sum_{i=1}^{N} C_i n_{ij},$$

при следующих ограничениях: (5)

$$\sum_{j=1}^{M} \alpha_i = 1; \quad \sum_{i=1}^{N} n_{ij} \le n_i,$$

где α_i- обобщенный приоритет j-го варианта СЗИ в иерархии ожидаемых приращений контролируемой характеристике эффективности СЗИ, обусловленной ЗИ; f_i - некоторая функция неадекватности распределения i-го ассигнования на j-й вариант СЗИ (учитывает разность между тем, что требуется, и тем, что выделяется для реализации j-го варианта СЗИ); C_i - приоритет издержанной единицы ассигнования i.

Стратегия выбора предпочтительного варианта СЗИ на основе показателя (5) сохраняется согласно правилу (4).

Общие выводы, которые можно сделать по результатам анализа указанных подходов, состоят в следующем.

До настоящего времени не разработаны методики, в полной мере учитывающие влияние угроз безопасности информации. Кроме того, не существует методик, которые позволили бы оценить конечный результат воздействия угроз безопасности информации, т. е. получить оценку ущерба предприятию в результате нарушения безопасности информации. Это связано с недостаточной крученностью самого механизма возникновения ущерба, отсутствием достаточно подробных математических описаний объектов информации, процессов обработки информации, позволяющих оценить влияние угроз не только на эффективность информационных отношений на предприятии, но и на эффективность решения предприятием частных функциональных задач, а также на качество и эффективность функционирования предприятия и СЗИ как в отдельности, так и в целом.Решение этой проблемы - одна из основных задач, стоящих перед разработчиками СЗИ для конкретных предприятий, действующих в конкретных условиях.

Методы оценки эффективности систем защиты информации. Одним из целесообразных вариантов построения методики оценки эффективности мер ЗИ является предлагаемая методика, в основу которой положена процедура оценки ущерба от угроз безопасности информации, которая имеет четыре этапа.

На первом этапе оценивается влияние угроз безопасности информации предприятию. Результатом этого этапа является оценка относительного или абсолютного показателей эффективности функционирования СЗИ под воздействием угроз безопасности информации с учетом вероятности осуществления этих угроз. Исходными данными для этих этапов являются: перечень угроз безопасности информации с указанием вероятностей их осуществления; перечень тактико-технических характеристик СЗИ и предельные значения их изменения.

Кроме того, необходимо иметь аналитические соотношения, позволяющие оценить влияние угроз на тактико-технические характеристики СЗИ, или методику натурных испытаний для получения экспериментальных данных, позволяющих получить эти зависимости.

На этом же этапе производится учет влияния угроз, который может осуществляться, помимо перечисленных выше методов, экспертным путем, что особенно актуально при оценки влияния угроз на качество информации, так как.получить аналитические зависимости на основе математического и натурного моделирования в этом случае достаточно сложно.

На втором этапе производится оценка относительного снижения эффективности ЗИ, вызванного ухудшения тактико-технических характеристик СЗИ. Исходными данными для этого этапа являются выходные данные первого этапа и допустимые значения показателя, выбранного для оценки эффективности процесса информационного обмена, связывающие показатель эффективности обеспечения безопасности информации с показателями качества функционирования СЗИ.

Третий этап заключается в оценке относительного снижения эффективности СЗИ при решении частных задач обеспечения безопасности информации вследствие ухудшения эффективности противодействия. Для проведения оценки необходимо иметь перечень частных задач, решаемых СЗИ, показатели их эффективности и аналитические соотношения, позволяющие учесть влияние эффективности процесса обеспечения безопасности информации на эффективность функционирования системы.

На четвертом этапе проводится оценка относительного снижения эффективности функционирования СЗИ в целом в зависимости от снижения эффективности решения частных задач обеспечения безопасности информации. Для получения аналитических соотношений, устанавливающих зависимость эффективности функционирования СЗИ от эффективности решения частных задач по обеспечению безопасности информации, может быть использован метод анализа иерархий [7].

Метод дает возможность на основе попарных сравнений с использованием специальной шкалы относительной важности оценивать выпад камерой из частных задач в общую эффективность функционирования СЗИ.

Для получения более наглядных оценок камерой из этапов производится расчет потерь, связанных с несанкционированными действиями получения информации на эффективность функционирования СЗИ.

Для расчета потерь из-за снижения эффективности функционирования СЗИ в целом необходимо учитывать внешнее окружение системы и предприятия, т. е. его назначение, область использования. При этом должны использоваться выведенные зависимости (4) и (5).

Вывод. В настоящее время нет методики, учитывающей влияние угроз безопасности информации, что не позволяет получить оценку ущерба предприятию в результате нарушения безопасности информации. Это связано с недостаточными знаниями механизма возникновения ущерба, отсутствием математических описаний объектов информации, процессов обработки информации, позволяющих оценить влияние угроз. Это все влияет на эффективность информационных отношений на предприятии. В работе предлагается методика оценки эффективности мер защиты информации, в основу которой положена процедура оценки ущерба от угроз безопасности.

Список литературы

1. ДСТУ 3396.1 - 96. Захист шформації. Технічний захист іформації. Порядок проведения робгт. - Введ.

2. *Герасименко В. А.* Защита информации в автоматизированных системах обработки данных. - Кн. 1,2. - М: Энергоатомиздат, 1994.-Кн. 1, С.

3. *Хорошко В. А.* Модель системы защиты информации. Захист іформації, 1999-№1. -С.5- 11.-Введ.

4. ДСТУ 3396.0 - 96. Захист інформації. Технічний захист інформації. Основні положення.

5. Постанова Кабінету Міністрів України № 1126 вщ 08.10.1997 року про концепщю техшчного захисту шформацй в УкраУш.

6. *А. Р. Марковский, Бесанар Карим, В.А. Баканов, В.А. Хорошко.* Критерии оценки эффективности сложных систем. Моделювання та іформаційні технології. Зб.наук, праць ІПМЕ НАНУ. - 1999.-№2. - С. 156- 159.

7. *Саати Т., Керис К.* Аналитическое планирование. Организация систем: Пер. с англ. -М.: Радио и связь, 1991.-458 с.

Работа посвящена выбору показателей эффективности мер защиты информации, которые определяются такими факторами, как назначение методик; технология оценки эффективности и выбора мер ЗИ; целевое назначение мер ЗИ, которое заключается в предотвращении ущерба субъектам информационных отношений на предприятии от угроз нарушения безопасности информации.

Робота присвячена вибору показників ефективності заходів захисту інформації, які визначаються такими чинниками, як призначення методик; технологія оцінки ефективності і вибору заходів ЗІ; цільове призначення заходів ЗІ, яке полягає в запобіганні збитку суб'єктам інформаційних відносин на підприємстві від загроз порушення безпеки інформації.

Work is devoted the choice of indexes of efficiency of measures of ZI, which are determined such factors, as setting of methods; technology of estimation of efficiency and choice of measures of ZI; having a special purpose setting of measures of ZI, which consists in prevention of harm the subjects of informative relations on an enterprise from the threats of security of information breach

Рецензент: д.т.н., проф. Корнійчук М.Т.

Надійшла 06.01.2011

УДК 004.056 **Єжова Л.Ф. (ДУІКТ)**

АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ : ТЕХНОЛОГІЇ І ПЕРСОНАЛ

ВСТУП

Діяльність будь-якої організації у наш час пов'язана з отриманням і передачею інформації. Більш того, кожному реальному об'єкту чи суб'єкту організації відповідає певний інформаційний актив, який потребує захисту. Інформація стала стратегічно важливим товаром. Втрата інформаційних ресурсів або заволодіння секретною інформацією конкурентами, може завдати підприємству значних збитків і навіть може привести до банкрутства.

Інформаційна безпека (ІБ) має здатність до деградації, коли не відбуваються її суттєві порушення і створюється ілюзія цілковитої безпеки, тоді не зберігаються у таємниці паролі, не відслідковуються відвідувачі організації тощо. Тому в сьогоднішній ситуації підприємства повинні мати стратегію ІБ, яка ґрунтується на комплексному підході, здійснювати контроль всіх параметрів ІБ, мати систему заходів з оцінки відповідності інформаційних систем підприємства певним стандартам та вимогам, мати процедури оцінки ризиків, пов'язаних з використанням інформаційних технологій та участю персоналу в них.

МЕТОЮ даної роботи є дослідження ролі персоналу в проведенні аудиту інформаційної безпеки технологічних процесів на об'єкті.

Серед процесів контроля та перевірки ІБ особливу роль відіграє аудит ІБ, основним призначенням якого є формування незалежної оцінки ІБ організації, незалежної від діяльності, яка перевіряється.

Зауважимо, що в такому випадку висновок про те, наскільки успішно функціонує об'єкт і наскільки він відповідає всім вимогам, робиться на основі вивчення якості виконання персоналом цього об'єкта відповідних функцій, зафіксованих у технологічних регламентах, створених по встановлених стандартах.

Через специфіку області інформаційної безпеки фундаментальну роль і місце має думка (суб'єктивне відчуття) людини. Небезпека і безпека, як її протилежність, є умогляд-