Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

На правах рукописи

УДК 004.056:658.5

ЛАВРОВА
Наталия Васильевна

АНАЛИТИЧЕСКАЯ ОЦЕНКА И УПРАВЛЕНИЕ РИСКАМИ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОМЫШЛЕННОГО ОБЪЕКТА

АВТОРЕФЕРАТ
диссертации на соискание степени
магистра техники и технологий

по специальности 1-39 81 01 – Компьютерные технологии
проектирования электронных систем

Минск 2017

Работа выполнена на кафедре проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Научный руководитель: **ЦЫРЕЛЬЧУК Игорь Николаевич,**
декан факультета непрерывного и дистанционного образования, кандидат технических наук, доцент, заведующий кафедрой проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Рецензент: **ПОЛУБОК Владислав Анатольевич,**
кандидат технических наук, доцент, заведующий кафедрой микропроцессорных систем и сетей института информационных технологий учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Защита диссертации состоится «22» июня 2017 г. года в $10^{\underline{00}}$ часов на заседании Государственной комиссии по защите магистерских диссертаций в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, Минск, ул. П.Бровки, 6, копр. 1, ауд. 415, тел. 293-20-80, e-mail: kafpiks@bsuir.by

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

ВВЕДЕНИЕ

В настоящее время информационные технологии (ИТ) являются необходимой составляющей повышения эффективности бизнес-процессов, позволяют хозяйствующим субъектам снизить издержки производства и многое другое[1]. Одной из наиболее серьезных проблем, затрудняющих применение современных ИТ, является обеспечение их информационной безопасности.

Усложнение форм, средств, методов автоматизации процессов обработки информации повышает зависимость промышленных предприятий от степени безопасности используемых ими ИТ, при этом качество информационной поддержки управления зависит непосредственно от организации инфраструктуры защиты информации (ИЗИ).

Данные мировой статистики свидетельствуют о тенденции роста масштаба компьютерных злоупотреблений, приводящих к значительным финансовым потерям хозяйствующих субъектов различного уровня. Ущерб от компьютерных злоупотреблений в мире ежегодно возрастает на 35%.[2–4].

Увеличение количества киберпреступлений произошло за счет прироста преступлений против информационной безопасности (глава 31 УК Республики Беларусь) на 63,6 % (с 404 до 651) [5]. Возросшее количество фактов несанкционированного доступа к компьютерной информации объясняется высоким уровнем латентности преступлений данной категории.

Сохраняющаяся тенденция заставляет вносить изменения в стратегию развития компаний и требует более обоснованной организации ИЗИ.

Анализ результатов исследований, ведущихся в направлении обеспечения информационной безопасности (ИБ) ИТ, показывает, что в настоящее время не до конца решены вопросы научного обоснования структуры системы защиты информации (СЗИ), реализуемой на предприятиях. В первую очередь это касается инфраструктуры защиты бизнес-процессов, которые играют решающую роль в достижении успеха хозяйствующим субъектом.

Отмеченные обстоятельства обусловливают противоречие между необходимостью научного обоснования концепции построения ИЗИ бизнес-процессов и возможностями теоретико-методологических решений, обеспечивающих это обоснование.

Рассматриваемый процессно-ориентированный подход к созданию (совершенствованию) ИЗИ бизнес-процессов позволит рассматривать процесс формирования СЗИ как один из вспомогательных процессов, обеспечивающих основные виды деятельности предприятия. Это дает возможность разработки ИЗИ в тесной взаимосвязи с проектированием других бизнес-процессов, что, несомненно, увеличит их интегрированность, гибкость, сбалансированность и управляемость.

Таким образом, потребность разрешения существующих противоречий в теории и практике создания СЗИ требует дальнейшего развития этих систем и, в частности, ИЗИ бизнес-процессов на промышленном предприятии.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

ИТ в настоящее время являются неотъемлемой частью эффективности бизнес-процессов. Одной из наиболее серьезных проблем, затрудняющих применение современных ИТ, является обеспечение их информационной безопасности. В качестве основных, можно выделить следующие моменты, которые подтверждают актуальность данной темы:

— резкое увеличение объемов информации, накапливаемой, хранимой на электронных носителях и обрабатываемой с помощью компьютеров;

— концентрация информации и сосредоточение в единых базах данных информации различного назначения и различной принадлежности;

— активное расширение круга пользователей, имеющих непосредственный доступ к вычислительным ресурсам и массивам данных.

Степень разработанности проблемы

Анализ современных методов решения рассматриваемых задач показал, что используются ряд различных подходов. Можно выделить работы С. Као, Л.Ф. Кранор, П. Мела, К. Скарфоне и А. Романовского по проблеме оценки уровня защищённости, С.А. Петренко, С.В. Симонова по построению экономически обоснованных систем обеспечения информационной безопасности, А.В. Мельникова по проблемам анализа защищенности информационных систем, И.В. Котенко по разработке интеллектуальных методов анализа уязвимостей корпоративной вычислительной сети, П.П. Парамонова, В.И. Городецкого, О.Б. Макаревича, И.Д. Медведовского, Ю.С. Соломонова, А.А. Шелупанова, И.Н. Цырельчук, В.М. Алефиренко, И.Б. Троников и др. Вместе с тем вопросы объективного анализа уровня защищённости ИС и его прогнозирования в этих работах рассмотрены недостаточно глубоко [1-4].

Одним из недостатков исследований, представленных в современной технической литературе, является неполное рассмотрение особенностей и положений, используемых при разработке политики безопасности, также некоторые разработанные модели не учитывают влияния экономических факторов. Предложенное исследование направлено на устранение этого недостатка на основе построения имитационной модели функционирования ИЗИ.

Цель и задачи исследования

Целью диссертации является разработка методов организации экономически обоснованной инфраструктуры защиты информации (ИЗИ) на промышленном предприятии на основе процессного подхода организации управления и использования перспективных концепций обеспечения информационной безопасности.

Поставленная цель работы определяет следующие основные задачи:

1. Провести обзор и анализ основных тенденций и закономерностей развития инфраструктуры системы защиты информации на промышленном объекте, а также выделить основные проблемы безопасности и классифицировать их.

2. Разработать методику обоснования принципов организации ИЗИ и проанализировать состав затрат на создание ИЗИ промышленного предприятия.

3. Разработать имитационную модель функционирования ИЗИ, выделить ее структуру и принцип функционирования.

Область исследования

Содержание диссертации соответствует образовательному стандарту высшего образования второй ступени (магистратуры) специальности 1- 38 81 01 «Компьютерные технологии проектирования электронных систем».

Теоретическая и методологическая основа исследования

В основу диссертации легли работы белорусских и зарубежных ученых в области определения и рассмотрения методологий обеспечения информационной безопасности, а также анализ технических нормативных правовых актов по рассматриваемой тематике.

Информационная база исследования сформирована на основе литературы, открытой информации, технических нормативно-правовых актов, сведений из электронных ресурсов, а также материалов научных конференций и семинаров.

Научная новизна

Научная новизна и значимость полученных результатов работы заключается в разработке имитационной модели функционирования инфраструктуры, которая позволить обеспечить защиту информации в корпоративных сетях промышленного предприятия.

Теоретическая значимость работы заключается в детальном анализе и учете финансовой составляющей данного вопроса.

Практическая значимость диссертации состоит в разработанной имитационной модели, которая позволит оптимизировать расходы на разработку и поддержание в актуальном состоянии ИЗИ.

Основные положения, выносимые на защиту

1. На основе определения закономерностей влияния инфраструктуры на реализацию бизнес-процессов и выявления тенденций развития информационных активов промышленного предприятия сформированы основные принципы функционирования ИЗИ, определены структурные особенности информационных активов.

2. Сформулирована и предложена концептуальная модель ИЗИ на промышленном предприятии, учитывающая требования и принципы ее организации, проанализированы и классифицированы основные виды угроз корпоративным сетям предприятия.

3. Разработана имитационная модель функционирования ИЗИ как инструментальный метод оценки и прогнозирования уровня защищенности информации на промышленном предприятии. Предложена система мониторинга безопасности информационных активов промышленного предприятия, направленная на оценку и анализ текущих значений разработанной системы показателей ИБ, а также выработку необходимых корректирующих воздействий на ИЗИ.

Апробация диссертации и информация об использовании ее результатов

Результаты исследований, вошедшие в диссертацию, докладывались и обсуждались на 53-ой научно-техническая конференции аспирантов, магистрантов и студентов БГУИР (Минск, Беларусь, 2017 г.).

Публикации

Изложенные в диссертации основные положения и выводы опубликованы в 4 печатных работах в сборниках материалов научных конференций.

Общий объем публикаций по теме диссертационной работы составляет 0,7 авторских листа.

Структура и объем работы

Диссертация состоит из введения, общей характеристики работы, трех глав с краткими выводами по каждой главе, заключения, библиографического списка и приложений.

В первой главе приведен обзор современных тенденций и закономерностей развития инфраструктуры защиты информации, рассмотрены основные понятия и структурные составляющие. **Во второй главе** исследованы основные принципы обеспечения информационной безопасности, представлена концептуальная модель, приведены основные проблемы обеспечения информационной безопасности корпоративных сетей и их классификация. **В третьей главе** представлена разработка имитационной модели для комплексной оценки используемых средств защиты, рассмотрены ее основные свойства и показан ее возможный синтез. **В приложении** представлены публикации автора и акт внедрения результатов исследования в учебный процесс.

Общий объем диссертационной работы составляет 90 страницы. Из них 54 страницы основного текста, 75 иллюстраций на 10 страницах, 2 таблицы на 1 странице, библиографический список из 79 наименований на 7 страницах, список собственных публикаций соискателя из 6 наименований на 1 странице, 3 приложений на 20 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** рассмотрены проблемы обеспечения информационной безопасности на современном этапе, указаны основные направления развития, для улучшения и усовершенствования методов по защите, а также описано обоснование актуальности темы.

В **общей характеристике работы** показана актуальность проводимых исследований, степень разработанности проблемы, сформулированы цель и задачи диссертации, обозначена область исследований, научная (теоретическая и практическая) значимость исследований, а также апробация работы.

В первой главе проанализированы тенденции и закономерности развития ИЗИ в промышленном предприятии, а также идентифицирована проблема ее совершенствования ИЗИ. По результатам проведенного анализа установлено, что наряду с производственной и социальной инфраструктурами следует выделять информационную инфраструктуру, обеспечивающую информационными ресурсами все уровни управления предприятием.

Поддержка и защита системы управления предприятием подразумевает, прежде всего, поддержку и защиту самих бизнес-процессов и развитие инфраструктурной составляющей бизнес-системы, в частности, информационной, за счет преодоления инфраструктурной и информационной разобщенности подразделений предприятия. Инвестиции в управления бизнес-процессами могут приносить значительные доходы за счет повышения рыночной стоимости компании в части ее нематериальных активов.

Проведенный анализ возможных угроз показал, что информационная инфраструктура должна обладать свойством защищенности информации, используемой в бизнес-процессах. С учетом компонентов бизнес-процесса, а также их взаимосвязей, к потенциально опасным ситуациям, которые могут возникнуть при низком уровне защищенности, относятся:

— несанкционированное влияние на бизнес-процесс нарушителей из числа владельцев и (или) участников процесса;

— уничтожение (изменение, искажение) информации за счет случайных помех, сбоев технических (программных) средств при передаче, хранении и обработке информации;

— несанкционированный доступ (НСД) нарушителей (не владельцев и участников) к информации, хранящейся и обрабатываемой в средствах автоматизации, с целью ознакомления, искажения и уничтожения;

— перехват информации при ее приеме (передаче) по каналам связи функциями процесса, а также за счет хищения носителей информации.

На основе оценки влияния возрастающих возможностей новых ИТ на поддержку и защиту бизнес-процессов, состояния существующей организации ИБ, реализации требований к ИЗИ и требований стандартов ИБ в современных бизнес-системах сформулирована научная проблема, решаемая в диссертации (рисунок 1). Она заключается в разработке методов организации ИЗИ на промышленном предприятии как целостной системы концептуальных положений, методов, моделей, алгоритмов и практических рекомендаций, обеспечивающих процесса создания и сопровождения ИЗИ. Решение сформулированной проблемы позволит

обоснованно подходить к организации ИЗИ бизнес-процессов на промышленном предприятии, а также осуществлять синтез СЗИ.

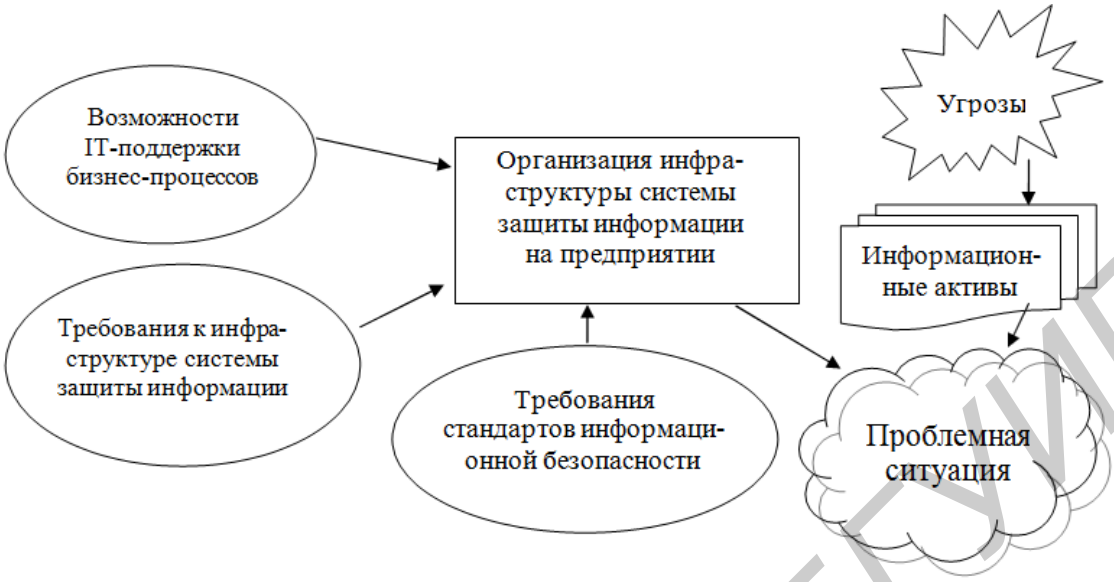

Рисунок 1 — Схема идентификации проблемы создания инфраструктуры системы защиты информации на предприятии

Во второй главе обоснованы принципы обеспечение ИБ, разработана концептуальная модель ИЗИ бизнес-процессов, сформирована система показателей ИБ.

Установлено, что организация ИЗИ бизнес-процессов производится в соответствии с принципами: системности; комплексности; непрерывности защиты; разумной достаточности; гибкости управления и применения; простоты применения защитных ме и средств. На основе этих принцпипов и с учетом типовых требований к ИЗИ разработана концептуальная модель ИЗИ бизнес-процессов.

Данная модель раскрывает основные функциональные возможности ИЗИ с учетом внешнихнегативных воздействий на информационные ресурсы.

С другой стороны, для реализации основной функции модели, учитывая характер возможных угроз, СЗИ должна обладать определенными свойствами. Математическаи это формулируется в следующем виде:

$$R = \sum_{i \epsilon N} K_i r_i \ , \sum_{i \epsilon N} K_i = 1, \qquad (1)$$

где R - обобщенный показатель оценки качества ИЗИ (обобщенный коэффициент защищенности, показывающий уровень отражения атак по всей совокупности возможных угроз); r_i — i-й частный показатель оценки качества ИЗИ (частный коэффициент защищенности, показывающий, какая часть атак угрозы i-го вида отражается); N — множество частных показателей оценки качества, сводимых в обобщенный показатель; K_i — весовой коэффициент i-го частного показателя качества в аддитивной свертке.

Коэффициент защищенности бизнес-процесса $R_{б\text{-}п}$ может быть представлен выражением:

$$R_{б-п} = 1 - \frac{\sum_{b \epsilon B} p_b \sum_{i \epsilon N_b} \lambda_{ib} t_b (1 - r_i)}{\sum_{b \epsilon B} p_b \sum_{i \epsilon N_b} \lambda_{ib} t_b}, \quad (2)$$

где N_b — количество наиболее вероятных информационных угроз для b-ой бизнес-операции; r_i — коэффициент защищенности от i-ой угрозы; λ_{ib} — интенсивность потока атак i- го вида угроз на b-ую бизнес-операцию ($i \in N_b$), для $i \notin N_b$, $\lambda_{ib} = 0$; t_b — время выполнения b-ой бизнес– операции; B — количество бизнес– операций в бизнес-процессе; p_b — вероятность выполнения бизнес-операции b в бизнес-процессе.

Модель минимизации затрат на построение инфраструктуры ЗИ. Данная модель может быть представлена в виде задачи целочисленного программирования с булевыми (двоичными) переменными.

Пусть$x_{ij} = 1$, если i-е средство ЗИ разработчик выбирает для защиты j-го информационного актива, и $x_{ij} = 0$ — в противном случае (при этом допускается, что i-е средство используется для защиты от i-ой угрозы). Требуется минимизировать затраты:

$$S = \sum_{i \epsilon I} \sum_{j \epsilon J} S_{ij} x_{ij} + \sum_{i \epsilon I} S_i y_i \to min, \quad (3)$$

при соблюдении системы ограничений:

$$\sum_{i \epsilon I} \sum_{j \epsilon J} a_j r_{ij} x_{ij} \geq R_{доп}, \sum_{i \epsilon I} x_{ij} = 1, \forall j \in J, \quad (4)$$

где $x_{ij} \in \{0; 1\}, y_i \in \{0; 1\}$.

В моделях (3-4) приняты следующие обозначения: S_{ij} — затраты на защиту j-го информационного актива i-м средством; S_i — затраты, общие для всех информационных активов, на защиту i-м средством; I — множество средств защиты информации; J — множество защищаемых информационных активов; r_{ij} — оценка качества защиты i-м средством j-го информационного актива (частный коэффициент защищенности, показывающий, какая часть атак угрозы i-го вида отражается); a_j — весовой коэффициент j-го информационного актива в общей оценке ИЗИ, $\sum_{j \epsilon J} a_j = 1$; $R_{доп}$ — допустимый уровень качества ИЗИ в целом; y_i — двоичная булева переменная, принимающая значение «1», если i-е средство ЗИ может быть использовано в ИЗИ, и «0» — в противном случае, причем i-е средство защиты в системе может быть использовано только один раз.

Модель максимизации уровня защищенности информационных активов предприятия. Данная модель описывает двойственную задачу по отношению к исходной задаче. В этом случае ограничение на уровень качества ЗИ становится критерием, а критерий исходной задачи — ограничением:

$$R = \sum_{i \epsilon I} \sum_{j \epsilon J} a_j r_{ij} x_{ij} \rightarrow max. \quad (5)$$

Таким образом, в данной модели требуется максимизировать уровень качества СЗИ при соблюдении следующих ограничений:

$$S = \sum_{i \epsilon I} \sum_{j \epsilon J} S_{ij} x_{ij} + \sum_{i \epsilon I} S_i y_i \leq S_{\text{доп}}, \quad (6)$$

$$\sum_{i \epsilon I} x_{ij} = 1, \ \forall j \in J, y_i \in \{0; 1\}, \quad (7)$$

где $S_{\text{доп}}$ — допустимая стоимость системы защиты информации для конкретного предприятия, $x_{ij} \in \{0;1\}$.

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. В ряде случаев не включаются единовременные затраты на формирование политики ИБ предприятия, если такая политика уже выработана.

Основным показателем экономической эффективности затрат на ИЗИ промышленного предприятия, как любого инвестиционного проекта является чистая приведенная стоимость (*NVP*) в заданный период времени *T:*

$$NVP = \sum_{t=1}^{T} \frac{\Delta if_t(R) - \Delta of_t(R)}{(1+E)^t} - K_R, \quad (8)$$

где $\Delta if_t(R)$ — изменение входного денежного потока в *t*-ый подпериод с учетом проведения мероприятий по защите информации; $\Delta of_t(R)$ — изменение выходного денежного потока с учетом проведения мероприятий по защите информации; K_R — внеоборотные и оборотные информационные активы ИЗИ; E — годовая норма прибыли на капитал.

Организация ИЗИ на предприятии влияет на результаты его хозяйственной деятельности и должна отвечать граничным условиям, приведенным в таблице 1.

Таблица 1 — Граничные условия эффективности затрат

№ п.	Основные показатели хозяйственной деятельности предприятия	Граничные условия
1.	Прибыль годовая	$\Delta П(R) \geq C_R + EK_R$
2.	Стоимость предприятия (доходный подход)	$\sum_{t=1}^{T} \frac{if_t + \Delta if_t(R) - of_t - \Delta of_t(R)}{(1+E)^t} + \frac{PV_T + \Delta PV_T(R)}{(1+E)^T} \geq \sum_{t=1}^{T} \frac{if_t - of_t}{(1+E)^t} + \frac{PV_T}{(1+E)^T}$

3.	Рентабельность	$\frac{\text{П} + \Delta\text{П}(R) - C_R}{\Phi_{\text{пр}} + K_R} \geq \frac{\text{П}}{\Phi_{\text{пр}}}$

В таблице 2.1 приняты следующие обозначения: $\Delta\text{П}(R)$ — годовой прирост прибыли в результате мероприятий по ЗИ; П(R) — прибыль при условии проведения мероприятий по ЗИ за год; П — прибыль в условиях отсутствия ЗИ (базовый вариант) за год; C_R — годовые эксплуатационные затраты на ЗИ; $\Phi_{\text{пр}}$ — стоимость производственных фондов; PV_T — прогнозная стоимость в T-ый год (базовый вариант) в условиях отсутствия мероприятий по ЗИ; $\Delta PV_T(R)$ — прогнозная стоимость с учетом проведения мероприятий по ЗИ; if_t —входной денежный поток; of_t — выходной денежный поток; $\Delta if_t(R)$ — изменение входного денежного потока в t-ый год с учетом проведения мероприятий по ЗИ; $\Delta of_t(R)$ — изменение выходного денежного потока в t-ый год с учетом проведения мероприятий по ЗИ.

В третьей главе для комплексной оценки предлагаемых мер и средств ЗИ бизнес-процессов разработана имитационная модель, реализующая имитацию атак на ИЗИ в соответствии с общей концептуальной моделью. Эта модель является структурным элементом схемы взаимосвязей показателей защищенности.

Совокупность поступающих транзактов создает входные потоки попыток атак на объекты защиты. При этом существенными свойствами потоков являются: тип источника атаки и время поступления транзактов-атак, подчиняющееся заданному закону распределения; максимально возможное число атак; время поступления первого транзакта-атаки; число одновременно поступающих транзактов-атак.

Основные ограничения и допущения при создании модели СЗИ:

— предполагается, что возможны все описанные в концептуальной модели типы угроз (несанкционированный доступ к информации, перехват информации при ее передаче (получении), уничтожение (повреждение) информации в результате различных видов сбоев в информационной инфраструктуре, несанкционированное вмешательство в бизнес-процесс);

— каждая атака может иметь целью получение (модификацию) любого информационного ресурса или их комбинации;

— потоки транзактов-атак являются пуассоновскими;

— время захвата информационного ресурса является случайной величиной;

— величина возможного ущерба в случае доступа злоумышленника на определенное время к конкретному информационному ресурсу фиксируется заданной константой.

Имитационная модель структурно состоит из блока имитации субъектов защиты, имитирующего нагрузку атак, блока имитации мер и средств защиты, имитирующего функционирование этих средств и блока имитации объектов защиты, имитирующего доступ к информационным ресурсам в случае преодоления мер и средств защиты.

Механизм основан на методах управления рисками промышленного предприятия. Ущерб определяется в зависимости от количества удавшихся попыток, типа и времении “захвата” информационного ресурса, его ценности в информационной инфраструктуре бизнес-процесса.

Основными выходными параметрами имитационной модели являются: число удавшихся попыток атак на информационную инфраструктуру бизнес-процессов; коэффициент доступа к каждому типу информационного ресурса; суммарный риск, характеризующий велечину ущерба от удавшихся атак.

Предложена система мониторинга защиты информационных активов предприятия, представляющая собой комплекс мер и мероприятий (организационных, технических, правовых), направленных на проведение наблюдений, оценки и прогноза изменений в информационной инфраструктуре и ее компонентах.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Определены основные тенденции развития и структурные особенности информационных активов промышленного предприятия во взаимосвязи с его бизнес-процессами.

2. Обоснованы принципы организации инфраструктуры защиты информации, ориентированной на поддержке бизнес-процессов промышленного предприятия.

3. Предложена концептуальная модель инфраструктуры защиты информации на промышленном предприятии, позволяющая разработать систему математических моделей оценки и оптимизации этой инфраструктуры.

4. Выполнен анализ состава затрат на создание инфраструктуры защиты информации промышленного предприятия.

5. Разработана система показателей информационной безопасности бизнес-процессов, обеспечивающая оценку инфраструктуры защиты информации, как по отдельным ее свойствам, так и в целом.

6. Разработана имитационная модель как инструментальный метод оценки и прогнозирования уровня защищенности информации на промышленном предприятии.

7. Предложена система мониторинга безопасности информационных активов, направленная на оценку и анализ текущего состояния показателей информационной безопасности, а также выработку необходимых корректирующих воздействий на инфраструктуру защиты информации.

8. Предложенные положения организации инфраструктуры системы защиты информации обеспечивают необходимые условия для предотвращения информационных угроз, сокращение затрат на информационную безопасность и повышение экономической эффективности производственно-хозяйственной деятельности промышленного предприятия.

Рекомендации по практическому использованию результатов

Полученные результаты внедрены в учебный процесс на кафедре проектирвоания информационно−компьютерных систем учреждения образования “Белорусский государственный университет информатики и радиоэлектроники в учебный курс “Методы и технические средства обеспечения безопасности”.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

Статьи в сборниках научных трудов

1. Лаврова, Н.В. Анализ и обеспечение безопасности корпоративных беспроводных сетей / Н.В. Лаврова, И.Н. Цырельчук, // Современные проблемы радиоэлектроники и телекоммуникаций, РТ-2017: сб. науч. трудов по материалам междунар. науч.−практич. конф., Севастополь, Российская Федерация / ФГАО УВО “СГУ”. – Севастополь. 2017. – поступило в печать.

2. Лаврова, Н.В. Основные способы тестирования системы на проникновение / Н.В. Лаврова, И.Н. Цырельчук, // Современные проблемы радиоэлектроники и телекоммуникаций, РТ-2017: сб. науч. трудов по материалам междунар. науч.−практич. конф., Севастополь, Российская Федерация / ФГАО УВО “СГУ”. – Севастополь. 2017. –поступило в печать.

Тезисы конференций

3. Лаврова, Н.В. Анализ и обеспечение безопасности корпоративных беспроводных сетей / Н.В. Лаврова, И.Н. Цырельчук, // материалы 53-ей науч. конф. аспирантов, магистрантов и студентов «Проектирование информационно−компьютерных систем», Минск, Респ. Беларусь, 02–06 мая 2017 г. / УО «БГУИР». – Минск, 2017. – поступило в печать

4. Лаврова, Н.В. Основные способы тестирования системы на проникновение / Н.В. Лаврова, И.Н. Цырельчук, // материалы 53-ей науч. конф. аспирантов, магистрантов и студентов «Проектирование информационно−компьютерных систем», Минск, Респ. Беларусь, 02–06 мая 2016 г. / УО «БГУИР». – Минск, 2017. – поступило в печать.

РЭЗЮМЭ

Лаўрова Наталля Васільеўна

Аналітычная ацэнка і кіраванне рызыкамі парушэння інфармацыйнай бяспекі прамысловага аб'екта

Ключавыя словы: інфармацыйная бяспека, мадэль.

Мэта працы: распрацоўка метадаў арганізацыі эканамічна абгрунтаванай інфраструктуры абароны інфармацыі (Ізі) на прамысловым прадпрыемстве на аснове працэсныя падыходу арганізацыі кіравання і выкарыстання перспектыўных канцэпцый забеспячэння інфармацыйнай бяспекі.

Атрыманыя вынікі і іх навізна: вызначаны асноўныя тэндэнцыі развіцця і структурныя асаблівасці інфармацыйных актываў прамысловага прадпрыемства ва ўзаемасувязі з яго бізнэс-працэсамі, абгрунтаваныя прынцыпы арганізацыі інфраструктуры абароны інфармацыі, арыентаванай на падтрымцы бізнес-працэсаў прамысловага прадпрыемства. Прапанаваная канцэптуальная мадэль інфраструктуры абароны інфармацыі на прамысловым прадпрыемстве, якая дазваляе распрацаваць сістэму матэматычных мадэляў ацэнкі і аптымізацыі гэтай інфраструктуры. Выкананы аналіз складу затрат на стварэнне інфраструктуры абароны інфармацыі прамысловага прадпрыемства і распрацавана сістэма паказчыкаў інфармацыйнай бяспекі бізнес-працэсаў, якая забяспечвае ацэнку інфраструктуры абароны інфармацыі, як па асобных яе уласцівасцях, так і ў цэлым. Распрацавана імітацыйная мадэль як інструментальны метад ацэнкі і прагназавання ўзроўню абароненасці інфармацыі на прамысловым прадпрыемстве, прапанавана сістэма маніторынгу бяспекі інфармацыйных актываў, накіраваная на ацэнку і аналіз бягучага стану паказчыкаў інфармацыйнай бяспекі, а таксама выпрацоўку неабходных карэкціруючых уздзеянняў на інфраструктуру абароны інфармацыі.

Ступень выкарыстання: вынікі ўкаранёны ў навучальны працэс на кафедры праектавання інфармацыйна-камп'ютэрных сістэм ўстановы адукацыі "Беларускі дзяржаўны універсітэт інфарматыкі і радыёэлектронікі ў навучальны курс" Метады і тэхнічныя сродкі забеспячэння бяспекі".

Вобласць ужывання: інфармацыйная бяспека, метады і сродкі абароны інфармацыі.

РЕЗЮМЕ

Лаврова Наталия Васильевна

Аналитическая оценка и управление рисками нарушения информационной безопасности промышленного объекта

***Ключевые слова*:** информационная безопасность, модель.

***Цель работы*:** разработка методов организации экономически обоснованной инфраструктуры защиты информации (ИЗИ) на промышленном предприятии на основе процессного подхода организации управления и использования перспективных концепций обеспечения информационной безопасности.

***Полученные результаты и их новизна*:** определены основные тенденции развития и структурные особенности информационных активов промышленного предприятия во взаимосвязи с его бизнес-процессами, обоснованы принципы организации инфраструктуры защиты информации, ориентированной на поддержке бизнес-процессов промышленного предприятия. Представлена концептуальная модель инфраструктуры защиты информации на промышленном предприятии, позволяющая разработать систему математических моделей оценки и оптимизации этой инфраструктуры. Выполнен анализ состава затрат на создание инфраструктуры защиты информации промышленного предприятия и разработана система показателей информационной безопасности бизнес-процессов, обеспечивающая оценку инфраструктуры защиты информации, как по отдельным ее свойствам, так и в целом. Разработана имитационная модель как инструментальный метод оценки и прогнозирования уровня защищенности информации на промышленном предприятии, предложена система мониторинга безопасности информационных активов, направленная на оценку и анализ текущего состояния показателей информационной безопасности, а также выработку необходимых корректирующих воздействий на инфраструктуру защиты информации.

***Степень использования*:** результаты внедрены в учебный процесс на кафедре проектирования информационно-компьютерных систем учреждения образования “Белорусский государственный университет информатики и радиоэлектроники в учебный курс “Методы и технические средства обеспечения безопасности”.

***Область применения*:** информационная безопасность, методы и средства защиты информации.

SUMMARY

Lavrova Natallia Vasil'evna

Analytical estimation and management of risks of infringement information safety of an industrial object

***Keywords*:** information security, model.

***The object of study*:** To increase the stability of the CEA to the damaging factors of electrification due to detection the effect of characteristics of electronic compo–nents on the threshold of their failure when subjected to discharge by CBM–model.

***The results and novelty*:** to develop methods for organizing an economically sound information security infrastructure in an industrial enterprise based on the process approach of managing the organization and using perspective concepts of ensuring information security. The received results and their novelty: the basic tendencies of development and structural features of information assets of the industrial enterprise in interrelation with its business processes are determined, the principles of organization of an information protection infrastructure oriented on supporting business processes of an industrial enterprise are grounded. A conceptual model of the information security infrastructure in the industrial enterprise is proposed, which allows developing a system of mathematical models for the assessment and optimization of this infrastructure. The analysis of the cost structure for the creation of an information security infrastructure for an industrial enterprise has been carried out, and a system of business process information security indicators has been developed that provides an assessment of the information protection infrastructure both for its individual properties and for the whole. A simulation model was developed as an instrumental method for assessing and forecasting the level of information security in an industrial enterprise. A system for monitoring the security of information assets was proposed, aimed at assessing and analyzing the current state of information security indicators, as well as developing the necessary corrective influences on the information security infrastructure.

***Degree of use*:** the results implemented in the educational process at the department of design information and computer systems educational institution "Belarusian State University of Informatics and Radio Electronics in the training course" Belarusian State University of Informatics and Radioelectronics in the training course" Methods and technical means of ensuring security".

Sphere of application: information security, methods and means of information protection.