КИБЕРНЕТИКА. ИНФОРМАТИКА

МРНТИ 28.27.27, 81.93.29

В.Г. Дрозд[1], Б.Ж. Спанова[1]

[1]Карагандинский экономический университет Казпотребсоюза, г. Караганда, Казахстан

ИНФОРМАЦИОННАЯ СИСТЕМА ПРЕДПРИЯТИЙ: МОДЕЛЬ ВЗАИМОСВЯЗИ ПАРАМЕТРОВ И ПОКАЗАТЕЛЕЙ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ ПРЕДПРИЯТИЯ

Аннотация. Проводится рассмотрение использования системного подхода на этапе анализа рисков информационной безопасности предприятия, описывается состав и определяются приоритеты выбранных средств защиты. Выполнено описание процедурных вопросов построения модели взаимосвязи параметров информационной системы и показателей обеспечивающих комплексную защиту информации на предприятии. Подтверждено, что создавая систему защиты информации, обеспечивается снижение затрат при угрозах информационного вмешательства. Также, решение стратегических задач IT-безопасности связаны с обеспечением конкурентоспособности и повышением адаптивности к рынку. Создание систем защиты на базе модельных экспериментов учитывающих взаимосвязи параметров и показателей комплексной защиты информации бизнес-процессов на предприятии экономически эффективно и целесообразно.

Ключевые слова: защита информации, информационные технологии, информационная безопасность, защита данных, IT системы.

• • •

Түйіндеме. Кәсіпорынның ақпараттық қауіпсіздігінің тәуекелдерін талдау кезеңінде жүйелік тәсілді қолдану қарастырылады, құрамы сипатталады және таңдалған қорғаныс құралдарының басымдықтары анықталады. Ақпараттық жүйенің параметрлері мен кәсіпорындағы ақпаратты жан-жақты қорғауды қамтамасыз ететін көрсеткіштердің өзара байланысы моделін құрудың процедуралық мәселелерінің сипаттамасы жасалды. Ақпаратты қорғау жүйесін құра отырып, ақпараттық араласу қатерлері кезінде шығындарды азайту қамтамасыз етілетіні расталды. Сондай-ақ, IT-қауіпсіздіктің стратегиялық міндеттерін шешу бәсекеге қабілеттілікті қамтамасыз етумен және нарыққа бейімділікті арттырумен байланысты. Кәсіпорындағы бизнес-процестердің ақпаратын кешенді қорғаудың параметрлері мен көрсеткіштерінің өзара байланысын ескере отырып, модельдік эксперименттер негізінде қорғаныс жүйелерін құру қажеттілігі экономикалық тиімді және орынды.

Түйінді сөздер: ақпаратты қорғау, ақпараттық технологиялар, Ақпараттық қауіпсіздік, деректерді қорғау, IT жүйелер.

Abstract. This article reviews application of systematic approach on the stage information security risks analysis in industrial settings, and describes procedural issues of building a model on interrelation of information system parameters and indicators that provide comprehensive information protection. It is confirmed that by creating an information security system, help to reduce costs in case of threats to information interference. In addition, the solution of strategic tasks of IT security is associated with ensuring competitiveness and increasing adaptability to the market. The need to create security systems based on model experiments that take into account the relationship between parameters and indicators of integrated information protection of business processes at the enterprise is cost-effective and expedient.
Keywords: information protection, information technology, information security, data protection, IT systems.

Введение. Защита информации действующих субъектов рыночной экономики, которыми выступают предприятия страны, в настоящее время представляет собой одно из трендовых направлений по обеспечению безопасности не только отдельного субъекта экономики, а также государства и общества в целом. Существующие проблемы различных аспектов безопасности, с дальнейшим развитием информационно-коммуникационных технологий, приобретают все более актуальное значение. Возникающие в этой связи нарушения информационной безопасности на предприятиях могут выражаться большими финансовыми потерями. Зарубежный опыт в области защиты интеллектуальной собственности, а так же и отечественный опыт в защите государственных секретов, показывают, что только комплексная защита может быть весьма эффективной. И именно это обстоятельство, наряду с правовыми и инженерно-техническими методами, определяет особое внимание к вопросам, рассматривающим изучение методов организации защиты информации, первостепенной составляющей в триаде комплексного обеспечения информационной безопасности.

Организационную защиту информации можно характеризовать как процедурную регламентацию взаимоотношений исполнителей и производственной деятельности на нормативно-правовой основе таким образом, что вероятность несанкционированного доступа к информации, обладающей уровнем конфиденциальности существенно затрудняется или становится невозможной за счёт организации и проведения соответствующих организационных мероприятий. Таким

образом, правовое направление затрагивает формирование совокупности нормативно-правовых документов, законодательных актов, положений, инструкций, руководств, требования которых выступают обязательными в отведенных рамках сферы их деятельности в системе защиты информации. Организационные мероприятия, по мнению многих ведущих специалистов, имеют существенное значение при создании надежного механизма защиты информации, так как имеющиеся возможности для несанкционированного использования конфиденциальных данных в значительной мере определяются злоумышленными действиями, нерадивостью, небрежностью и халатностью персонала обеспечивающего защиту или пользователей, а не техническими аспектами. Поэтому, воздействие подобных аспектов практически невозможно исключить программно-математическими методами, техническими средствами и физическими мерами.

К подобным организационно-структурным мероприятиям можно отнести:

− комплекс мероприятий, проводимых на этапах проектирования, строительства и оборудования служебных и производственных зданий и помещений. Данные мероприятия дают возможность исключить потенциальные попытки для тайного проникновения как в помещения организации, так и на территорию предприятия; организация самостоятельных производственных зон по принципу конфиденциальности работ с самостоятельными системами доступа и т.п.; организация качественных удобств проходного контроля и проезда транспорта, перемещения людей и иных средств передвижения;

− комплекс мероприятий, проводимых в период набора персонала, включающие в себя процедурные этапы по ознакомлению с сотрудниками, обучение правилам работы с соответствующей конфиденциальной информацией, информирование о мерах ответственности за нарушение установленных правил защиты информации и пр.;

− обеспечение надёжного контроля и пропускного режима посетителей;

− организация сохранности различного рода документов и физической безопасности самих носителей конфиденциальной информации, придерживаясь порядка выработанных процедур учёта, выдачи, исполнения и возвращения носителей конфиденциальной информации;

− эффективная организация охраны территории и помещений предприятия;

− создание условий для постоянного обучения и переобучения сотрудников;

− организация процедур защиты конфиденциальной информации: проведение систематического контроля за работой персонала с информацией, назначение ответственного лица за защиту информации в конкретных производственных коллективах, контроль за порядком учёта, хранения и уничтожения конфиденциальных документов и т.д.

Методы исследования. В процессе проверки проводилось исследование информационной системы организации в соответствии с формальной моделью, которая приведена на рисунке 1.

1. Уровень риска от реализации угроз информационной безопасности предприятия, в целом, может определяться при рассмотрении всех составляющих, т.е. описания системы защиты ресурсов и показателей вероятности реализации каждой угрозы;

2. Угрозы по обеспечению доступности: саботирование трудовых процессов; физическая порча серверов (оборудования); кража или потеря информации на резервных носителях; нарушение своевременности и адресности информационного обмена; нарушение и вывод из строя линий связи; нарушение процедур системы контроля и управления доступом; нарушение процессов передачи информации между подразделениями предприятия;

3. Угрозы по обеспечению целостности: выявление сбоя целостности данных в БД; ввод сотрудниками предприятия неверных данных или преднамеренное искажение информации; в случае отсутствия резервных копий предоставляется возможность восстановления критически важной информации; замена информации на носителях данных; искажение целостности программной среды, в том числе изменение настроек программного обеспечения; в результате пожара и других чрезвычайных ситуаций потеря информации.

Часть угроз имеет отношение к нарушению двух из трех или всех трех вышеуказанных качеств информации и информационных систем: возникновение техногенных аварий; обнаружение несанкционированного доступа путем использования чужих атрибутов разграничения доступа; попадание посторонних в защищенное помещение; нецелевое использование программно-аппаратных средств сотрудниками организации; злоупотребление полномочиями; несанкционированный доступ к информации сотрудниками организации; технические сбои в работе систем сигнализации и охраны; заражение компьютерными вирусами и внедрение в информационную систему вредоносных программ; не-

санкционированный доступ к ресурсам операционной системы; порча оборудования технических средств охраны.

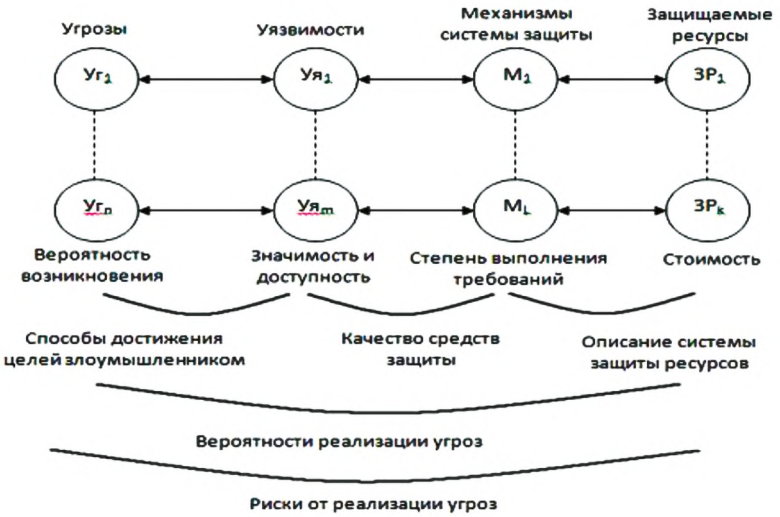

Рисунок 1 - Модель взаимосвязи параметров информационных систем и показателей экономической эффективности системы защиты информации

Инженерно-техническое направление скомбинировано на базе программно-аппаратных средств защиты конфиденциальной информации. Аппаратные средства включают механические, электромеханические, оптические, радио- и радиотехнические, лазерные, электронные, радиолокационные и ряд других устройств, сооружения и системы, которые предназначены для обеспечения безопасности и защиты информации.

Данные средства защиты используются непосредственно для решения следующего ряда задач:

− препятствия дистанционному подслушиванию и визуальному наблюдению;

− нейтрализации вредных«наводок» и электромагнитных излучений;

− защиты информации, передаваемой в системах автоматизированной обработки информации и средствах связи;

− выявления технических средств магнитной записи и подслушивания.

На текущий период, зависимость казахстанской экономики от поставок программного обеспечения, оборудования и сервисов из-за рубежа повышает риски роста издержек на формирование и обслуживание казахстанской IT-инфраструктуры, которая призвана поддерживать информационную безопасность предприятий Казахстана. Как отражают статистические данные, общий объем затрат на информационные технологии в Казахстане в 2016 г. составил 375600,4 млн. тенге. В сравнении с 2015 г. общий объем финансирования сферы IT увеличился на 37%, в сравнении с 2012 г. – на 43%. В проводимом исследовании, на базе данных официальной статистики, выполним прогнозирование этих данных на перспективный период, которое наглядно продемонстрирует динамику развития показателя «Настройка программного обеспечения, включая изменение в операционную систему или программы по обеспечению безопасности реализуемые субъектами экономики РК». Статистические значения показателя приведены в таблице 1.

Таблица 1 - Компьютерные действия членов экономических субъектов РК в процентах

	2015	2016	2017
Настройка ПО, включая изменение в операционную систему или программы по обеспечению безопасности	7,9	10,9	12,2

*Примечание: составлено на основе статистических данных (Статистический сборник «Развитие связи и информационно-коммуникационных технологий в РК»)

Выполним количественный анализ прогнозирования используя формализованный метод, который основывается на статистическом информационном материале методом экстраполяции по аналитическому выравниванию тренда. Подобный расчет прогнозных значений, базируется на экстраполяции рядов динамики, который можно представить в виде функции:

$$Y^*_{t+l} = f(y_i, l, a_j) \quad (1)$$

где Y^*_{t+l} - расчетное прогнозируемое значение ряда динамики; y_i – текущий уровень ряда, который принят за основу экстраполяции; l – значение упреждающего периода; a_j – параметр из уравнения тренда.

Линейную трендовую зависимость можно получить, произведя сглаживание временного ряда используя метод наименьших квадратов:

$$\hat{Y}_t = f(t) \quad (2)$$

Экстраполяция дает возможность расчетным путем получить точечное значение прогноза, т. е. количественную оценку прогнозируемого показателя в точке по уравнению, которое описывает тенденцию прогнозируемого показателя. Экстраполяция реализована путем подстановки в уравнение тренда значения независимой переменной *t*, соответствующей величине прогноза (периода упреждения). Величина тесноты связи расчетного показателя с фактором определялась посредством коэффициента корреляции. Корреляционная зависимость между последовательными уровнями временного ряда называется автокорреляцией уровней ряда. Количественно её можно измерить с помощью линейного коэффициента корреляции между уровнями исходного временного ряда и уровнями этого ряда, сдвинутыми на несколько шагов во времени.

Одна из рабочих формул для расчёта коэффициента автокорреляции имеет вид:

$$r_{xy} = \frac{\sum(x_j - \bar{x})(y_j - \bar{y})}{\sqrt{\sum(x_j - \bar{x})^2 \sum(y_j - \bar{y})^2}} \quad (3)$$

где , в качестве переменной x рассматривается ряд y_2, y_3, … , y_n; в качестве переменной y – ряд y_1, y_2, . . . ,$y_n - 1$.

Проиллюстрируем использование этого метода на примере прогнозирования исследуемого показателя за период 2015-2017гг. Расчетные значения, характеризующие полученную трендовую модель приведены в таблице 2.

Таблица 2 - Уравнение трендовой модели прогнозируемого показателя, характеризующего компьютерные действия членов экономических субъектов РК, в период 2015-2017 гг.

	Уравнение трендовой модели	Средне квад. ошибка оценки	Коэф.-т детерм., R^2
Настройка программного обеспечения, включая изменение в операционную систему или программы по обеспечению безопасности	Yt= 6,033+2,15t	0,4	0,950

* Таблица составлена на основе расчета

Полученная модель, на базе которой осуществлялся прогноз, с полученными характеристиками уравнения, позволяет утверждать,

что при сохранении сформировавшихся закономерностях развития прогнозируемой величины они попадают в расчетное значение выявленной тенденции изменения показателя. Результаты прогнозных значений приведены в таблице 3.

Таблица 3 - Прогнозные значения прогнозируемого показателя, на период 2018-2019гг., %

	2019г	2020г
Настройка программного обеспечения, включая изменение в операционную систему или программы по обеспечению безопасности	14,3	16,2

* Таблица составлена на основе расчета

Можно отметить, что прогнозные значения, полученные на основе однофакторного уравнения регрессии от временного тренда, совпадают в пределах допустимой погрешности. Для обеспечения защиты коммерческих секретов предприятия формируют собственные службы безопасности, важной предпосылкой для создания которых является разработка их структуры, состава, положений о подразделениях и должностных инструкций для руководящего состава и сотрудников. Служба безопасности предприятия выступает как самостоятельная организационная единица, подчиняющаяся непосредственно руководителю предприятия. Подобная структура управления системой безопасности, обладающая строгой вертикалью, характерна для области обеспечения безопасности, где требуется определённость, строгие границы, регламентация отношений на всех уровнях – от рядового сотрудника до менеджеров высшего звена. Как показывает практический опыт, только на предприятиях, где вопросы безопасности находятся под постоянным контролем руководителя предприятия, достигаются наиболее высокие результаты. Возглавляет службу безопасности начальник службы в должности заместителя руководителя предприятия по безопасности. При этом руководитель СБ должен обладать максимально возможным кругом полномочий, позволяющим ему влиять на другие подразделения и различные области деятельности предприятия, если этого требуют интересы безопасности.

При организации и реализации политики безопасности всех уровней нужно придерживаться того, что разработанная политика безопасности на нижнем уровне должна быть тождественно соответствующей политике безопасности, приведенной на верхнем уровне. При этом в положении политики безопасности должны быть приведены правила, не имеющие двойного смысла и они должны быть понятными для сотрудников предприятия. Важ-

нейшее значение для защиты информации на предприятии имеет политика безопасности, представленная в виде логически и семантически связанных, формируемых и анализируемых структур данных, применяемых для защиты информации на всех уровнях функционирования предприятия. Проведём рассмотрение основных составляющих политики информационной безопасности предприятия. Под защитой, в данном случае, подразумевается использование организационных мероприятий. С помощью внедрения политики информационной безопасности на предприятиях выполняют внешний и внутренний аудит защиты информации, результаты которого применяются для расчета уровня эффективности, используемых методов и средств защиты. В свою очередь, положительная динамика выступает в виде подстройки мероприятий с использованием полученных результатов от проведенного тестирования и мониторинга [1]. Реализуемая политика безопасности в процессе функционирования предприятия постоянно обновляется. При этом все внесенные изменения следует постоянно сравнивать с теми методами и средствами, которые уже используются. Основные составляющие политики информационной безопасности предприятия можно отразить в виде схемы, которая приведена на рисунке 2. Как видно из рисунка 2, в политике информационной безопасности отражены взаимосвязанные последовательные этапы организации информационной безопасности предприятия, которые описаны процедурами, позволяющими систематизировать и эффективно решать поставленные задачи для того, чтобы достичь требуемого уровня защиты данных.

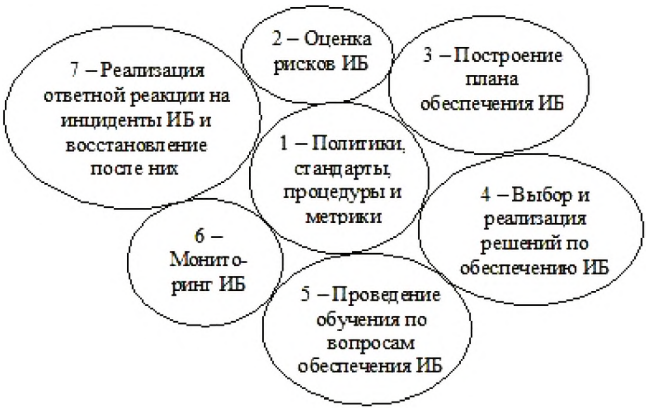

Рисунок 2 - Основные составляющие политики информационной безопасности предприятия

На самом первом этапе необходимо очертить границы, в рамках которых будет действовать политика информационной безопасности предприятия, определить критерии для оценки результатов. На следующем этапе проводится анализ рисков, описывается состав и определяются приоритеты выбранных средств защиты с распределением их по степени важности. Проводится идентификация уязвимости активов предприятия и определяться возможный ущерб. Полученные результаты анализа рисков информационной безопасности предприятия, как правило, применяются как исходный материал для планирования работы системы информационной безопасности, выбора наиболее эффективной стратегии и тактики. Для повышения эффективности политики безопасности применяются такие приёмы как групповое определение объектов безопасности, косвенное определение с использованием верительных атрибутов и мандатное управление доступом. Многими предприятиями применяется глобальная и локальная политики безопасности, которые базируются на принципах управления безопасностью информации.

В качестве критериев оценки работы СЗИ могут выступать такие категории, как пригодность и оптимальность. Категорию «пригодность» можно оценить выполнением требований, относящихся к данной системе, категорию «оптимальность» можно оценить при принятии одной из характеристик экстремального значения [2]. Гораздо сложнее обстоит ситуация, когда появляется несколько характеристик, и по каждой необходимо достижение экстремального значения. Тогда приходится обращаться к сложным методам, которые получают интегрированные сводные показатели. Выборку критерия проводят после изучения целей системы защиты. Имеется ряд определений, согласно которых под эффективностью функционирования системы защиты информации понимается уровень соответствия результатов поставленной цели [3]. Но для сравнительных характеристик работы СЗИ важна и количественная оценка эффективности.

В своей работе, С.В. Домарев дает рекомендацию, как использовать при расчёте эффективности СЗИ системный подход [4]. При изучении системы защиты информации кажется вполне логичным применение системного подхода, который предполагает, что объект воспринимается как система. Примененный подход демонстрирует целостность объекта, связи с внешними факторами, внутреннюю структуру объекта. При этом предполагается также проведение анализа общих элементов, а затем, переходящий к частным элементам. Оценочные составляющие системы защиты информации организу-

ются по трём векторным направлениям: «основы», «направления», «этапы». Каждый из этих векторов сочетает в себе набор из четырех, пяти и семи элементов соответственно. Перемножение данных векторов образует матрицу, включающую в себя 140 вопросов, на которые требуется готовить ответы. В качестве ответов выступает набор требований к системе защиты информации.

Для формирования объективной оценки характеризующей состояния защищенности информационной системы предприятия, проверка должна проводиться независимыми от объекта специалистами. Результаты проверки могут служить исходными данными для количественной оценки качества систем защиты информации, в том числе и ее экономической эффективности [4,5]. Исходя из этого, многие предприятия страны относятся к финансовым вложениям в информационную безопасность как к виду инвестиций. На этом основании, можно ожидать конкретные результаты от построения системы защиты информации, окупаемость этих инвестиций и возможность оценки их эффективности. Основным экономическим эффектом, на который делает ставку предприятие, создавая систему защиты информации, выступает снижение затрат при реализации угроз информационной безопасности. Получить освобождение средств и снизить затраты можно в случае, если относится к этим выделениям средств на информационную безопасность только как к затратам. Однако, в перспективе это может отдалить предприятие от решения стратегических задач, которые связаны с обеспечением конкурентоспособности, повышением адаптивности к рынку, так как информационная безопасность оказывает влияние на эти процессы.

Выводы. Таким образом, потребность разрешения существующих противоречий в теории и практике создания систем защиты информации на базе модельных экспериментов учитывающих взаимосвязи параметров и показателей комплексной защиты информации бизнес-процессов на предприятии экономически эффективна и целесообразна.

Список литературы

1 *Аверченков, В. И.* Организационная защита информации : учебное пособие для вузов / В. И. Аверченков, М. Ю. Рытов. – Москва : Изд-во «ФЛИНТА», 2011. – 184 с.

2 Основы организованного обеспечения информационной безопасности объектов информатизации / С. Н. Сёмкин, Э. В. Беляков, С. В. Гребенев, В. И. Козачок. – Москва : Изд-во «Гелиос АРВ», 2005.

3 Основы информационной безопасности : учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. – Москва : Горячая линия – Телеком, 2006. – 544 с.

4 Организационно-правовое обеспечение информационной безопасности : учебное пособие / А. А. Стрельцов, В. С. Горбатов, Т. А. Полякова [и др.]; под ред. А. А. Стрельцова. – Москва : Издательский центр «Академия», 2008. – 256 с.

5 *Мельников, П. В.* Информационная безопасность и защита информации / П. В. Мельников, С. А. Клейменов, А. М. Петраков. – 6-е изд. – Издательский центр «Академия», 2012.

Дрозд В.Г. – кандидат экономических наук, доцент, e-mail: vgdrozd@mail.ru
Спанова Б.Ж. – кандидат экономических наук, доцент, e-mail: sbg789@mail.ru