Published in the Russian Federation
Sochi Journal of Economy
Has been issued since 2007.
ISSN: 2541-8114
2017, 11(1): 17-28

www.vestnik.sutr.ru

UDC 338.14 + 004.056

Information Protection System as a Tool to Maintain the Competitiveness of Enterprises

Arina V. Nikishova [a, *], Vladlena S. Oladko [b]

[a] Volgograd state university, Russian Federation
[b] Financial University under the Government of the Russian Federation, Russian Federation

Abstract

The subject of the research is the study of the impact of information security of an enterprise and its economic stability. The aim of the study is to analyze methods of information security in the enterprise and reduce costs through the implementation of the proposed automated tools of intelligent analysis and decision support. The comparison study, the ratio of total and private, and decision theory are applied as the research methods. To obtain the study result, the main causes and sources of violations of security at the enterprise are analyzed, evaluated risks. The conclusion about the need to minimize the negative economic impact, due to the application of the protection system is made. Methods of synthesis of protection systems offered.

Keywords: economic security, information security, risk, small business, information security incident, intelligent information system, expert system, neural network, decision support system.

1. Введение

Как показано в [1], в настоящее время, субъекты малого и среднего предпринимательства играют важную экономическую и социальную роль в развитии экономики, как отдельного региона, так и всей страны в целом. Это связано с тем, что от уровня развития малого и среднего бизнеса зависят такие показатели экономического развития, как уровень конкуренции, внедрение новых технологий, развитие инноваций, эффективность производства и т.д. Поэтому при планировании и оценке экономического развития каждого региона необходимо уделить внимание состоянию малого и среднего бизнеса, в данном регионе, и факторам препятствующем его развитию. Анализ основных показателей деятельности индивидуальных предпринимателей, предприятий малого и среднего бизнеса по Волгоградской области за январь – сентябрь 2015 года показывает следующее распределение предприятий по сферам экономики региона: образование и здравоохранение (0,84 %), сельское хозяйство и промысел (6,36 %), промышленность, производство и добыча (3,73 %), строительство (2,64 %), оптовая и розничная торговля (57,63 %), гостиничный и ресторанный бизнес (1,36 %), транспорт и связь (12,66 %), сфера услуг (15,70 %). Вне зависимости от сферы деятельности, большая часть данных предприятий для автоматизации своих бизнес–процессов, обработки, передачи и хранения информации использует информационную инфраструктуру, городские и глобальные сети передачи данных, что подтверждается данными статистики [3]: персональные компьютеры

* Corresponding author
E-mail addresses: arinanv@mail.ru (A.V. Nikishova), oladko.vs@yandex.ru (V.S. Oladko)

используют 89,4 % предприятий, интернет используют 82,4 % предприятий. При этом от качества, устойчивости и безопасности функционирования образующих информационную инфраструктуру предприятия персональных компьютеров, автоматизированных рабочих мест сотрудников, информационных систем, локальных и глобальных вычислительных сетей будет напрямую зависеть эффективность деятельности, конкурентоспособность и экономическая безопасность каждого предприятия.

По данным Positive Technologies [3, с.12] в 58 % случаях инциденты, связанные с нарушением информационной безопасности (ИБ) на предприятии, привели к существенным экономическим проблемам и нарушениям деятельности:

- нарушение IT-инфраструктуры (31 %);
- финансовые потери (15 %);
- репутационные издержки (12 %).

Следовательно, можно сделать вывод, об актуальности проведения мероприятий и исследований в области обеспечения ИБ на предприятии. Поскольку именно создание адекватной и эффективной системы защиты, позволит не только снизить риски для предприятия от возможных последствий инцидентов ИБ, но полностью предотвратить их возникновение.

2. Материалы и методы

Для написания данной статьи были использованы материалы научной, учебной литературы, законодательство Российской Федерации, статистические данные, собранные из печатных и электронных источников информации.

В качестве основных методов исследования при выполнении работы были использованы: метод описания, системного анализа, аналогии и обобщения, а также элементы теории принятия решений и экспертных систем.

3. Обсуждение

Угрозы безопасности информационной инфраструктуры предприятий

Организация защиты информации на предприятии тесно связана с понятием безопасности информационных технологий, которое определяется как: «состояние защищенности информационной технологии, при котором обеспечиваются безопасность информации, для обработки которой она применяется, и информационная безопасность информационной системы, в которой она реализована» [4]. Таким образом, для того чтобы обеспечить безопасность информации и систем, которые ее хранят, передают и обрабатывают, необходимо в первую очередь идентифицировать возможные проблемы безопасности, их источники, природу возникновения, оценить потенциальный ущерб и тяжесть последствий.

Анализ литературных источников [3, 5-7] показывает, что в общем случае проблемы безопасности предприятия можно разделить на три основные составляющие (см. рис. 1):

1) угрозы физической безопасности;
2) угрозы информационной безопасности;
3) угрозы экономической безопасности.

При этом следует отметить, что подобное деление на составляющие весьма условно и угрозы одной группы могут оказывать влияние и провоцировать возникновение угроз из другой группы. Например, кража носителя информации или оборудования, входящего в состав информационной инфраструктуры предприятия может привести к нарушению доступности и конфиденциальности данных или прерыванию бизнес-процесса, что в свою очередь может нанести материальный ущерб предприятию и/или снижению репутации в бизнес среде. А поскольку подобных угроз огромное количество, то в данной работе, авторами для сужения области исследования будут рассматриваться преимущественно угрозы, связанные с нарушением ИБ на предприятии и их влияние на экономическую безопасность и конкурентоспособность предприятия.

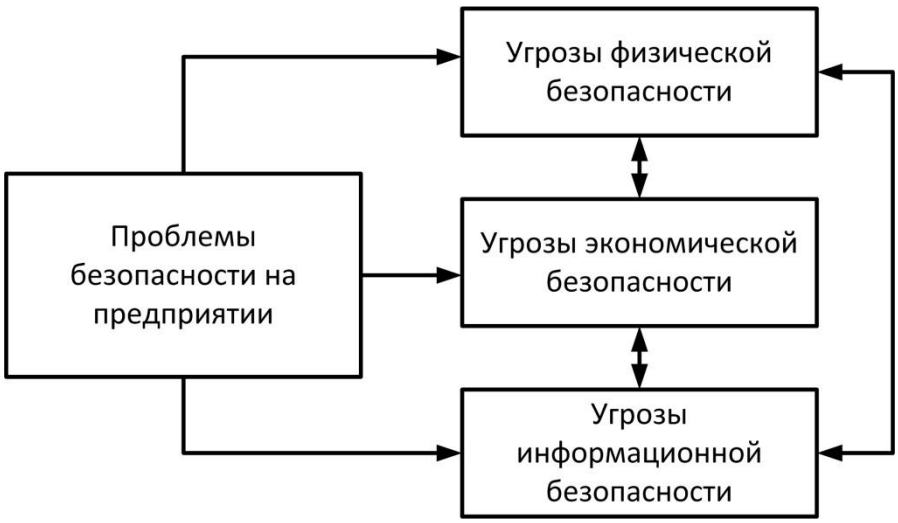

Рис. 1. Взаимовлияние угроз безопасности на предприятии

По природе возникновения угрозы ИБ можно разделить на случайные и умышленные. К случайным или неумышленным угрозам относят:

–катастрофы природного и техногенного характера;

–ошибки пользователей и обслуживающего персонала информационной инфраструктуры предприятия;

–сбои и отказы аппаратного обеспечения информационной инфраструктуры;

–ошибки и сбои в работе программного обеспечения информационной инфраструктуры предприятия.

Вероятность таких угроз определяется спецификой региона, где расположено предприятие, многолетними метеорологическими наблюдениями, геотектоническими данными, надежностью и временем наработки на отказ программно-аппаратного обеспечения, а также квалификацией пользователей и персонала предприятия.

Умышленные угрозы, как правило, связаны с действиями злоумышленника, который может быть как внутренним, так и внешним. По данным исследованиям компании InfoWatch [8] наибольшую опасность представляют именно внутренние злоумышленники (сотрудники, администраторы, руководители), на долю которых приходиться 61 % нарушений ИБ на предприятии. По своей цели атаки злоумышленников, как правило, направлены на: хищение персональных данных, хищение платежных данных и информации о банковских картах, хищение логинов и паролей пользователей, адресов электронной почты, хищение медицинских данных и карт, получение доступа к коммерческой тайне и know-how предприятия и т.п.

На рис. 2. представлена статистика угроз ИБ на предприятии за первую половину 2015 [3, 9], анализ которой показывает, что наиболее распространенными угрозами являются DDoS/DoS-атаки, которым были подвержены 23 % предприятий, атаки на внешние веб-приложения предприятий – 21 %, нарушения правил эксплуатации информационных систем – 16 % и вредоносное программное обеспечение – 14 %.

Рис. 3. Статистика угроз ИБ на предприятии за 2015 год

В результате успешной реализации угроз ИБ на предприятии может произойти:

– нарушение конфиденциальности информации и утечка данных;

– нарушение целостности информации и компрометация данных;

– нарушение доступности информации и компонентов информационной инфраструктуры предприятия;

– прерывание бизнес-процессов предприятия.

Таким образом, реализации той или иной угрозы ИБ может повлечь для предприятия ряд экономических рисков, выражающихся через материальный и не материальный ущерб, нарушение экономической безопасности, потерю эффективности деятельности, а самом худшем случае полному прекращению деятельности (см. рис. 4.). А это в соответствие с [9. с. 210], главные базовые условия конкурентоспособности:

Конкурентоспособность=эффективность + безопасность.

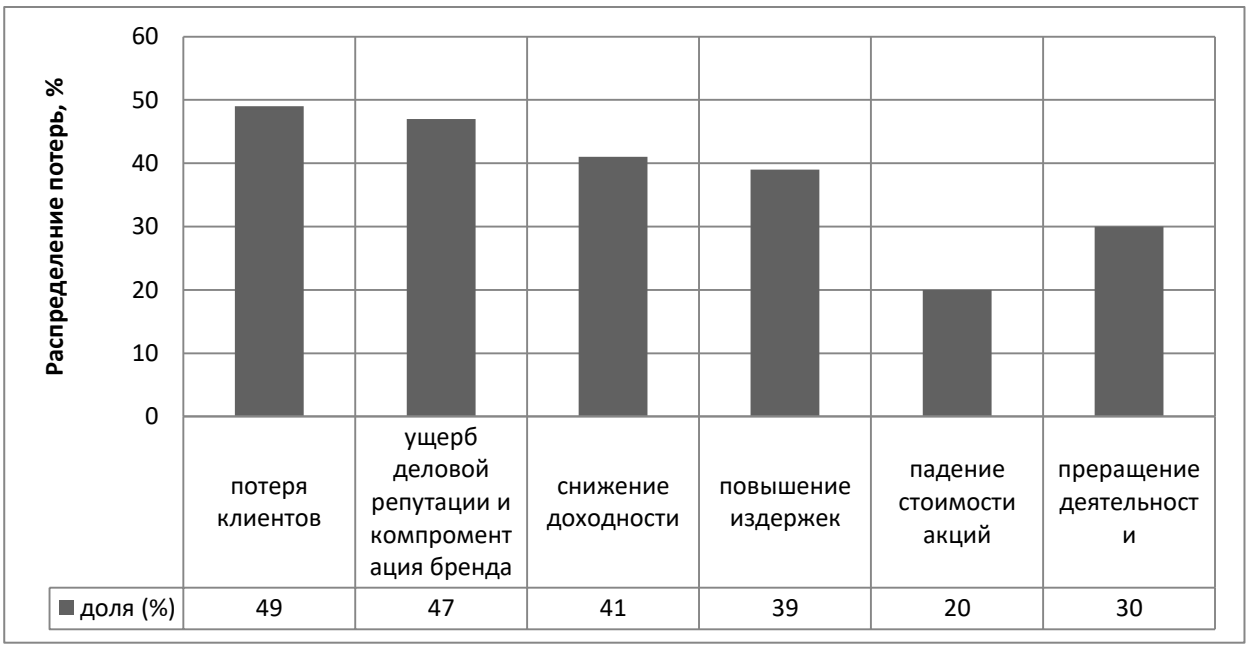

Рис. 4. Экономические последствия угроз ИБ, данные исследований компаний Symantic, Strategic Reasearch Institute и Информзащита

Таким образом, для предотвращения возможных рисков и снижения их тяжести для предприятия, а, следовательно, поддержания его конкурентоспособности, необходимо использовать специализированные средства и механизмы, объединенные в единую систему защиты. Цель синтеза и использования такой системы защиты на предприятии – идентификация источников и объектов риска и приведение потенциальных рисков к уровню допустимых и приемлемых для предприятия.

На рис. 5. представлена методика построения системы защиты информации на предприятии. В соответствие с данной методикой для того чтобы спроектировать и внедрить систему защиты необходимо предварительно составить модель актуальных для данного предприятия угроз ИБ и оценить риски.

Рис. 5. Методика построения системы защиты информации на предприятии

В соответствии с [10] процесс определения актуальных угроз ИБ представляет собой непрерывный жизненный цикл и делится на четыре этапа:

1) Определение области применения процесса определения угроз ИБ. Этап направлен на выявление физических и логических границ информационной инфраструктуры предприятия, в которых принимаются и контролируются меры защиты информации.

2) Идентификация источников угроз и угроз ИБ.

3) Оценка вероятности реализации угроз ИБ и степени возможного ущерба. Размер ущерба от реализации угрозы в отношении информации или информационной инфраструктуры предприятия зависит от [10, 11]:

— стоимости информации или ресурса, который подвергается риску.

— степени разрушительности воздействия на информацию или ресурс, выражаемой в виде коэффициента разрушительности.

Соотношение между ущербом, частотой и вероятностью возникновения определяет уровень риска от реализации угрозы и степень допустимости каждой угрозы.

Значения риска указывает насколько необходимо использовать средства и механизмы, противодействующие каждой конкретной угрозы. Для этого ожидаемый риск сравнивается с

затратами на покупку, конфигурацию и сопровождение средства защиты, после чего принимается решение в отношении данного риска (см. таблицу 1).

Таблица 1. Действия по отношению к риску от потенциальной угрозы безопасности предприятия

Степень допустимости	Действие в отношении риска	Пояснение
Недопустимый	Снижен	за счет внедрения средств защиты, уменьшающих вероятность реализации угрозы или коэффициент разрушительности
	Устранен	за счет отказа от использования подверженного угрозе ресурса или информации
	Перенесен	застрахован, в результате чего в случае реализации угрозы безопасности, потери будет нести страховая компания, а не владелец
Допустимый	Принят	потери незначительны и/или вероятность реализации минимальна и могут не применяться средства защиты

4) Мониторинг и переоценка угроз ИБ. Направлен на пересмотр логических и физических границ информационной инфраструктуры предприятия, ее составляющих, которые могли быть изменены в результате переопределения целей и бизнес задач, перестроения ее структуры, изменения базовых конфигураций и структурно-функциональных характеристик. А также переоценку актуальных угроз ИБ с последующим анализом их изменений.

На этапе оценки вероятности реализации угроз ИБ и степени возможного ущерба используется два подхода. В рамках первого подхода собирается статистика об инцидентах нарушения ИБ. На ее основании дается оценка вероятности реализации угроз ИБ предприятия. [11] Однако такой подход обладает рядом недостатков. Во-первых, общедоступная статистика не всегда содержит полные сведения обо всех инцидентах нарушения ИБ. Во-вторых, она не всегда является репрезентативной для конкретного предприятия.

Для преодоления выделенных недостатков применяется второй подход – использование экспертных оценок. Однако собирать для каждой оценки группу экспертов – это затратно как с точки зрения финансовой составляющей, так и временных затрат. Для ускорения и удешевления процесса оценки вероятности реализации угроз ИБ и степени возможного ущерба применяются системы искусственного интеллекта, называемые экспертными системами.

Экспертная система (ЭС) — это компьютерная программа, оперирующая со знаниями в определенной предметной области для выработки рекомендаций или решения проблем. [12] Однако применение подобных систем имеет свои недостатки. Функционирование ЭС включает этап приобретения знаний. В режиме приобретения знаний общение с ЭС осуществляется через посредничество инженера по знаниям. Также в данном этапе участвует эксперт. Эксперт описывает проблемную область в виде совокупности данных и правил. Данный этап выполняется перед началом эксплуатации экспертной системы в конкретной предметной области, а также может повторяться периодически. Его наличие увеличивает стоимость эксплуатации ЭС. Но его проведение очень важно, оно определяет эффективность функционирования ЭС, т.е. точность выдаваемых ей оценок [13].

К основным преимуществам, которые даёт использование ЭС, относятся постоянство знаний, воспроизводимость, способность к объяснению предлагаемого решения и возможность объединения знаний многих экспертов. Однако ЭС обладают и рядом недостатков: сложность обеспечения полноты знаний ЭС о предметной области, сложность устранения избыточных и конфликтующих правил в базе правил, а также неспособность ЭС к самообучению.

Для уменьшения влияния недостатков ЭС на эффективность их функционирования предлагается применить гибридный подход, который предполагает создание гибридной ЭС, сочетающей в себе ЭС и нейронную сеть. Концепция нейронных сетей, в отличие от ЭС, использует другой подход в области моделирования мыслительной деятельности – нейрокибернетический. Объединение ЭС и искусственной нейронной сети в одну систему позволит избавиться от недостатков обоих подходов и шире реализовать преимущества каждого из них.

Для подтверждения данного предположения была разработана гибридная ЭС [14], и были проведены ее экспериментальные исследования. Были сделаны выводы, что при использовании гибридного подхода повысилась доля обнаруживаемых атак: два вида атак были дополнительно обнаружены гибридной ЭС в сравнении с ЭС. Также было выявлено, что при использовании нейронной сети, как дополнения к ЭС, повышается и общая эффективность работы ЭС, под которой понимается доля обнаруживаемых атак, деленная на время работы, на 5 %.

Увеличение эффективности функционирования ЭС имеет и экономический эффект. Увеличение количества обнаруживаемых атак снижают риски от злоумышленных воздействий на предприятия – возможные финансовые издержки от реализации одной из атак. Снижение времени функционирования ЭС снижает издержки на обеспечение ее функционирования. В итоге экономический эффект может составить больше, чем 5 %.

После составления модели актуальных угроз и оценки рисков, определяется стратегия организации защиты информации на предприятии. Цель стратегии заключается в поиске оптимального компромисса между потребностями предприятия в защите и необходимыми для этих целей ресурсами. Тип и размер затрачиваемых на защиту ресурсов может быть ограничен определенным пределом, поскольку затраты на проектирование, внедрение и сопровождение системы защиты не должны быть больше стоимости самой защищаемой информации или капитала предприятия, либо определяется условием обязательного достижения требуемого уровня защиты, который зависит от категории обрабатываемой информации и требований регуляторов. Таким образом, в первой ситуации защита должна быть организована так, чтобы при выделенных ресурсах обеспечивался максимально возможный уровень защиты, а во второй — чтобы требуемый уровень защиты обеспечивался при минимальном расходовании предприятием ресурсов. Как правило, стратегии защиты информации на предприятии могут быть оборонительными, наступательными и упреждающими и включают в себя комплекс методов и средств защиты, способствующих снижению рисков и обеспечению непрерывности бизнес-процессов, доступности, целостности и конфиденциальности информации.

Исходя из [15, 16] структуру системы защиты информации на предприятии можно разделить на 2 основных группы компонентов:

1) программно-техническая подсистема, в состав которой входят инженерно-технические и программно-аппаратные средства защиты информации:

— системы видеонаблюдения;

— системы пожарной сигнализации;

— устройства для ввода идентифицирующей пользователя информации (например, магнитные и пластиковые карты, биометрические считыватели и т.п.);

— устройства и программное обеспечение для шифрования информации;

— устройства для воспрепятствования несанкционированному включению рабочих станций и серверов (например, электронные замки и блокираторы);

— программы разграничения доступа пользователей к ресурсам информационной инфраструктуры предприятия;

— системы обнаружения и предотвращения вторжений;

— средства резервного копирования и восстановления информации;

— антивирусное программное обеспечение;

— межсетевые экраны и средства распределенной фильтрации и глубокого анализа трафика;

— средства регистрации событий;

— средства мониторинга и аудита состояния безопасности.

2) нормативно-экономическая подсистема, включающая в себя политику безопасности предприятия, регламентирующую работу программно-технических подсистем и персонала с учетом выделенных финансовых средств.

Выделенные подсистемы и средства обеспечивают защиту периметра предприятия, сетевой инфраструктуры, серверов и конечных точек пользователей (см. рис. 6), что обеспечивает безопасную обработку данных и выполнение бизнес-процессов предприятия.

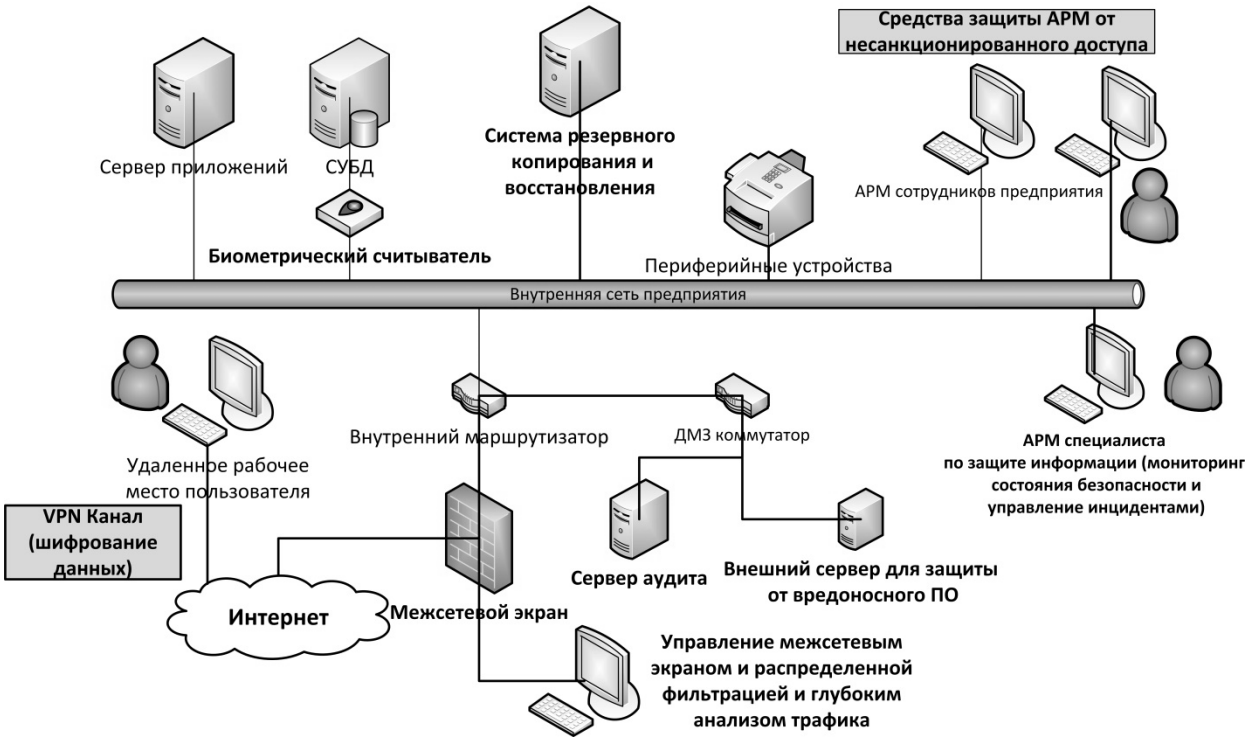

Рис. 6. Структура системы защиты информационной инфраструктуры предприятия

Информационной инфраструктуры предприятия является сложной системой, содержащей множество разнородных элементов, что усложняет ее построение и управление ею, а также разработку и администрирование системы защиты информации для нее. Одним из основных видов гетерогенности, присущих информационной инфраструктуре предприятия является программная гетерогенность, которая влияет на программную составляющую системы защиты информации. Основным программным обеспечением компонентов информационной инфраструктуры предприятия является операционная система. Была проанализирована статистика использования различных операционных систем [17] (см. рис. 7-8).

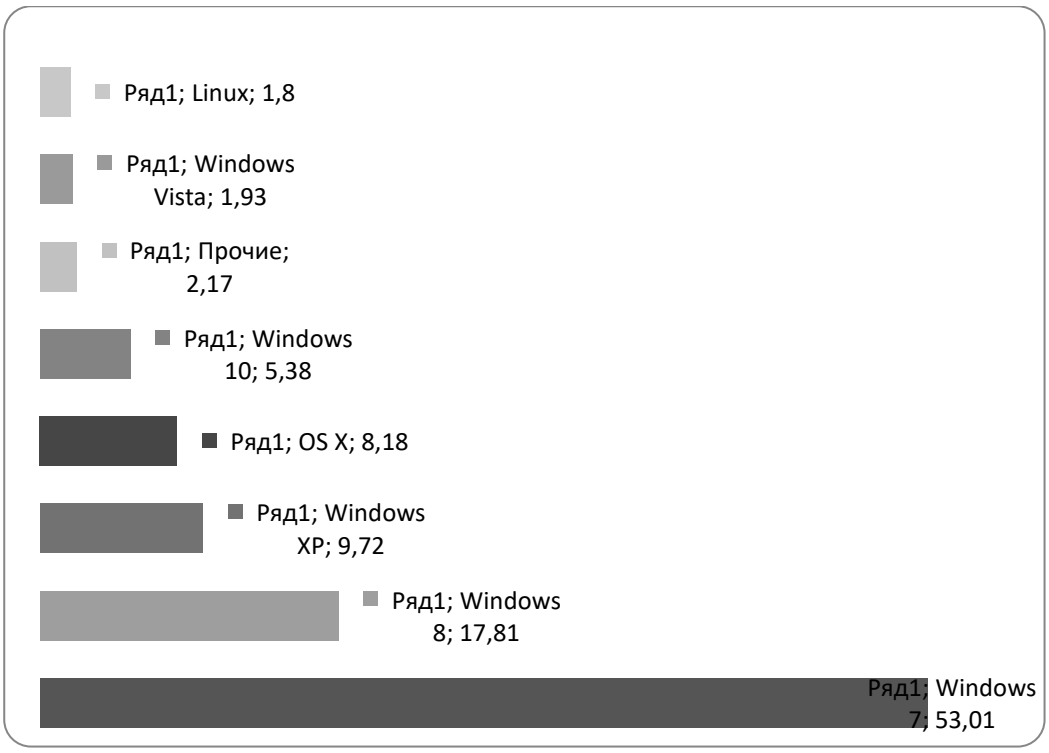

Рис. 7. Статистика использования ОС в стационарных и портативных компьютерах (август 2015)

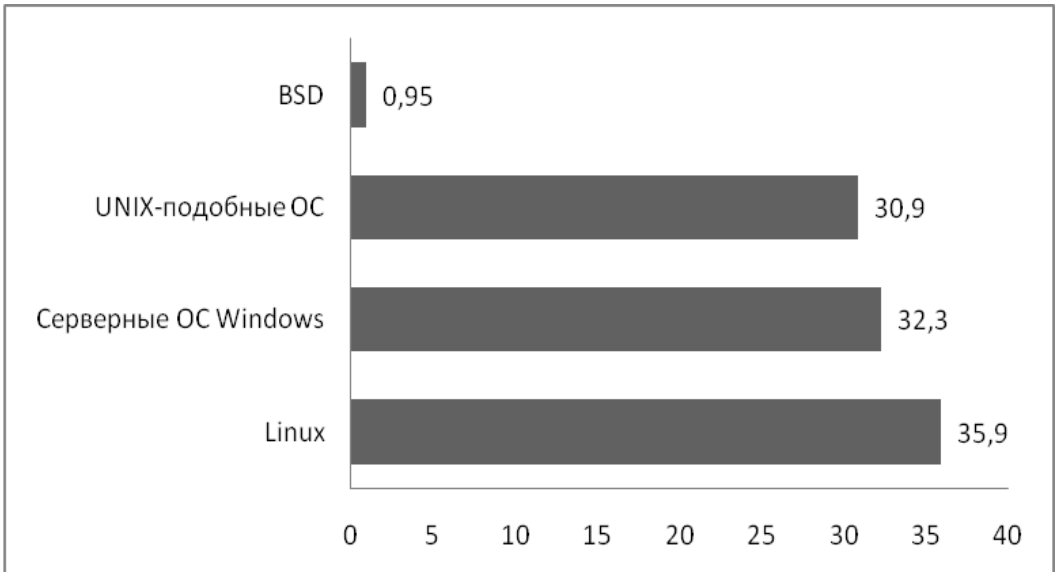

Рис. 8. Статистика использования ОС в публичных серверах Интернет (февраль 2015)

По статистике наиболее «популярными» ОС для рабочих станций являются ОС семейства Windows (самая распространённая — Windows 7). Для серверов же самыми часто используемыми считаются Unix-подобные ОС (наибольший процент принадлежит Linux). Таким образом, можно сделать вывод о том, что наиболее распространенной информационной инфраструктурой является гетерогенная информационная инфраструктура предприятия. Это приводит к тому, что администратору безопасности непросто сформировать систему защиты информации из богатого списка предлагаемых средств, при этом учесть тот факт, что стоимость системы защиты не должна превышать стоимости конфиденциальной информации, вероятность потери которой необходимо снизить до минимума. Системы поддержки принятия решений (СППР) могут эффективно решать задачу поиска оптимального решения при создании, модернизации, настройке

системы защиты информации, генерируя на основе полученных данных наиболее подходящее решение. Использование СППР позволяет увеличить скорость реагирования на возникающие попытки нарушения защищенности ИС организации, свести к минимуму ошибки администратора, допускаемые при ручной настройке СЗИ, и увеличить скорость принятия решений по обеспечению информационной безопасности.

Однако, современные СППР предназначены в основном для сферы менеджмента. Поэтому была разработана СППР [18], учитывающая особенности защиты информации информационной инфраструктуры предприятия. В ней реализованы метод принятия решений с группой экспертов, характеризуемые весовыми коэффициентами, и метод принятия решений с группой экспертов, характеризуемые нечетким отношением нестрогого предпочтения. Второй метод использует нечеткую логику в процессе своей работы, что позволяет улучшить его взаимодействие с пользователями-людьми. Экспериментальные исследования для каждого из реализованных методов показали, что эффективность второго метода, оцениваемая как отношение процента безошибочных генераций решений из набора испытаний к временным затратам, на 15 % выше, чем первого.

4. Выводы

Можно сделать вывод, что каждое предприятие, для минимизации экономического ущерба, должно обеспечивать защиту информации в своей информационной инфраструктуре. В настоящее время системы защиты информации – сложные системы, требующие квалифицированных специалистов для построения и управления ими. Применение интеллектуальных информационных систем позволит снизить требования к администраторам безопасности, что позволит также уменьшить издержки предприятий на обеспечение защиты информации, снизить экономические риски от возможных инцидентов ИБ на предприятии, а значит обеспечить эффективность и безопасность деятельности предприятия, т.е. повысить его конкурентоспособность. Кроме того данные средства могут применяться в рамках образовательного процесса при подготовке специалистов по защите информации и на специализированных предприятиях-интеграторах, предоставляющих свои услуги в области информационной безопасности.

Литература

1. Нурмухаметов А.В. Значение малого и среднего бизнеса в экономике страны // Актуальные вопросы экономических наук: материалы III междунар. науч. конф. (г. Уфа, июнь 2014 г.). Уфа: Лето, 2014. С. 16-19.

2. Официальная статистика. Предпринимательство // Территориальный орган Федеральной службы государственной статистики по Волгоградской области. URL: http://volgastat.gks.ru/wps/wcm/connect/rosstat_ts/volgastat/ru/statistics/enterprises/ (дата обращения 04.12.2016).

3. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения [Электронный ресурс]. Доступ из справ.-правовой системы «Электронный фонд правовой и нормативно-технической документации». URL: http://docs.cntd.ru/document/1200075565 (дата обращения 04.12.2016).

4. Карпин А. Внутренние угрозы, опаснее чем вирусы // Positive Research 2015. [Электронный ресурс]. URL: http://www.ptsecurity.ru/download/PT_Positive_ Research_2015_RU_web.pdf (дата обращения 04/12/2015).

5. Ланцман Е.Н. Концептуальные подходы к проблеме обеспечения экономической безопасности организации//Вестник АГТУ. Сер: Экономика. 2010. №1. С. 58-61.

6. Аткина В.С. Анализ катастрофических воздействий на информационную систему//Актуальные проблемы гуманитарных и естественных наук. 2010. №1. С.15-19.

7. Гарнаева М.А., Функ К. Kaspersky Security Bulletin 2013//Вопросы кибербезопасности. 2013. № 3(4). С. 65-68. Глобальное исследование утечек конфиденциальной информации в I полугодии 2015 года [Электронный ресурс] //Аналитический центр

8. InfoWatch. URL: http://www.infowatch.ru/sites/default/files/report/analytics/russ/ InfoWatch_Global_Report_2015_half_year.pdf (дата обращения 04.12.2015).

9. Козицин А.А., Дудинская М.В. Конкурентоспособность и экономическая безопасность – приоритетные задачи металлургического комплекса региона и его лидеров в условиях нестабильности // Экономика региона. 2015. №3. С. 204-215. DOI 10.17059/2015-3-17.

10. Выборнова О.Н. Онтологическая модель процесса оценки рисков// Вестник АГТУ. Сер.: Управление, вычислительная техника и информатика. 2015. №2. С. 97-102.

11. Зефиров С.Л., Щербакова А.Ю. Оценка инцидентов информационной безопасности // Доклады Томского государственного университета систем управления и радиоэлектроники. 2014. №2(32). С.77-81.

12. Джексон П. Введение в экспертные системы. М.: Вильямс, 2001. 397 с.

13. Kendal S.L, Creen, M. (2007). An introduction to knowledge engineering. London: Springer, 287.

14. Никишова А.В., Болдырев С.Д. Гибридная экспертная система для решения задач защиты информации // Актуальные вопросы информационной безопасности регионов в условиях глобализации информационного пространства: материалы IV Всероссийской науч. практ. конф., г. Волгоград, 23-24 апреля 2015 г. Волгоград: Изд-во ВолГУ, 2015. 308 с. С. 177-182.

15. Конев А.А., Давыдова Е.М. Подход к описанию структуры системы защиты информации // Доклады ТУСУРа. 2013. №2 (28). С. 107-111.

16. Никишова А.В. и др. Поддержка принятия решений в области защиты информации // Актуальные вопросы информационной безопасности регионов в условиях глобализации информационного пространства: материалы IV Всероссийской науч.-практ. конф., г. Волгоград, 23-24 апреля 2015г. Волгоград: Изд-во ВолГУ, 2015. 308 с. С. 200-204.

17. Usage share of operating systems (2015). Wikipedia. Retrieved from http://en.wikipedia.org/wiki/Usage_share_of_operating_systems

18. Витенбург Е.А., Никишова А.В., Чурилина А.Е. Программный комплекс поддержки принятия решений в области защиты информации // Свидетельство о государственной регистрации программ для ЭВМ. № 2015613761, 25 марта 2015.

References

1. Nurmukhametov A.V. Znachenie malogo i srednego biznesa v ekonomike strany // Aktual'nye voprosy ekonomicheskikh nauk: materialy III mezhdunar. nauch. konf. (g. Ufa, iyun' 2014 g.). Ufa: Leto, 2014. S. 16-19.

2. Ofitsial'naya statistika. Predprinimatel'stvo // Territorial'nyi organ Federal'noi sluzhby gosudarstvennoi statistiki po Volgogradskoi oblasti. URL: http://volgastat.gks.ru/wps/wcm/connect/rosstat_ts/volgastat/ru/statistics/enterprises/ (data obrashcheniya 04.12.2016).

3. GOST R 53114-2008 Zashchita informatsii. Obespechenie informatsionnoi bezopasnosti v organizatsii. Osnovnye terminy i opredeleniya [Elektronnyi resurs]. Dostup iz sprav.-pravovoi sistemy «Elektronnyi fond pravovoi i normativno-tekhnicheskoi dokumentatsii». URL: http://docs.cntd.ru/document/1200075565 (data obrashcheniya 04.12.2016).

4. Karpin A. Vnutrennie ugrozy, opasnee chem virusy // Positive Research 2015. [Elektronnyi resurs]. URL: http://www.ptsecurity.ru/download/PT_Positive_Research_2015_RU_web.pdf (data obrashcheniya 04/12/2015).

5. Lantsman E.N. Kontseptual'nye podkhody k probleme obespecheniya ekonomicheskoi bezopasnosti organizatsii//Vestnik AGTU. Ser: Ekonomika. 2010. №1. S. 58-61.

6. Atkina V.S. Analiz katastroficheskikh vozdeistvii na informatsionnuyu sistemu//Aktual'nye problemy gumanitarnykh i estestvennykh nauk. 2010. №1. S.15-19.

7. Garnaeva M.A., Funk K. Kaspersky Security Bulletin 2013//Voprosy kiberbezopasnosti. 2013. № 3(4). S. 65-68. Global'noe issledovanie utechek konfidentsial'noi informatsii v I polugodii 2015 goda [Elektronnyi resurs] //Analiticheskii tsentr

8. InfoWatch. URL: http://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Global_Report_2015_half_year.pdf (data obrashcheniya 04.12.2015).

9. Kozitsin A.A., Dudinskaya M.V. Konkurentosposobnost' i ekonomicheskaya bezopasnost' – prioritetnye zadachi metallurgicheskogo kompleksa regiona i ego liderov v usloviyakh nestabil'nosti // Ekonomika regiona. 2015. №3. S. 204-215. DOI 10.17059/2015-3-17.

10. Vybornova O.N. Ontologicheskaya model' protsessa otsenki riskov // Vestnik AGTU. Ser.: Upravlenie, vychislitel'naya tekhnika i informatika. 2015. №2. S. 97-102.

11. Zefirov S.L., Shcherbakova A.Yu. Otsenka intsidentov informatsionnoi bezopasnosti // Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki. 2014. №2(32). S. 77-81.

12. Dzhekson P. Vvedenie v ekspertnye sistemy. M.: Vil'yams, 2001. 397 s.
13. Kendal S.L, Creen, M. (2007). An introduction to knowledge engineering. London: Springer, 287.
14. Nikishova A.V., Boldyrev S.D. Gibridnaya ekspertnaya sistema dlya resheniya zadach zashchity informatsii // Aktual'nye voprosy informatsionnoi bezopasnosti regionov v usloviyakh globalizatsii informatsionnogo prostranstva: materialy IV Vserossiiskoi nauch. prakt. konf., g. Volgograd, 23-24 aprelya 2015 g. Volgograd: Izd-vo VolGU, 2015. 308 s. S. 177-182.
15. Konev A.A., Davydova E.M. Podkhod k opisaniyu struktury sistemy zashchity informatsii // Doklady TUSURa. 2013. №2 (28). S. 107-111.
16. Nikishova A.V. i dr. Podderzhka prinyatiya reshenii v oblasti zashchity informatsii // Aktual'nye voprosy informatsionnoi bezopasnosti regionov v usloviyakh globalizatsii informatsionnogo prostranstva: materialy IV Vserossiiskoi nauch.-prakt. konf., g. Volgograd, 23-24 aprelya 2015g. Volgograd: Izd-vo VolGU, 2015. 308 s. S. 200-204.
17. Usage share of operating systems (2015). Wikipedia. Retrieved from http://en.wikipedia.org/wiki/Usage_share_of_operating_systems
18. Vitenburg E.A., Nikishova A.V., Churilina A.E. Programmnyi kompleks podderzhki prinyatiya reshenii v oblasti zashchity informatsii // Svidetel'stvo o gosudarstvennoi registratsii programm dlya EVM. № 2015613761, 25 marta 2015.

УДК 338.14 + 004.056

Интеллектуальная система защита как инструмент поддержания конкурентоспособности предприятия

Арина Валерьевна Никишова [a, *], Владлена Сергеевна Оладько [b]

[a] Волгоградский государственный университет, Российская Федерация
[b] Финансовый университет при Правительстве Российской Федерации, Российская Федерация

Аннотация. Рассмотрено влияние состояния информационной безопасности на экономическую стабильность и конкурентоспособность предприятия. Цель исследования – анализ методики обеспечения информационной безопасности на предприятие и сокращение объема издержек за счет внедрения автоматизированных средств интеллектуального анализа и поддержки принятия решений. Для получения результатов исследования проанализированы основные причины и источники нарушения информационной безопасности на предприятии, оценены риски и сделан вывод о необходимости минимизации негативного экономического эффекта от нарушений, за счет применения системы защиты. Предложена методика синтеза системы защиты.

Ключевые слова: экономическая безопасность, информационная безопасность, риск, малый бизнес, инцидент информационной безопасности, интеллектуальная информационная система, экспертная система, нейронная сеть, система поддержки принятия решений.

[*] Корреспондирующий автор
Адреса электронной почты: arinanv@mail.ru (А.В. Никишова), oladko.vs@yandex.ru (В.С. Оладько)