УДК 338

ХАРАКТЕРИСТИКА И БАЗОВЫЕ ПОКАЗАТЕЛИ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Васильевых В. А.,
студент,
ФГБОУ ВО «Вятский Государственный Университет»
Россия, г. Киров

Смирнов Ф. Е.,
студент,
ФГБОУ ВО «Вятский Государственный Университет»
Россия, г. Киров

Сышева А. Р.,
студент,
ФГБОУ ВО «Вятский Государственный Университет»
Россия, г. Киров

Котанджян А. В.
Старший преподаватель кафедры финансов и экономической безопасности,
ФГБОУ ВО «Вятский Государственный Университет»
Россия, г. Киров

Аннотация

Обеспечение безопасности предприятия — это одна из актуальных проблем в современном обществе. В первую очередь, в статье рассматривается вопрос формирования системы обеспечения экономической безопасности, определяются и анализируются базовые показатели комплексной безопасности, выявляются тенденции её развития. Формулируется вывод о том, что обеспечивать экономическую безопасность предприятия становится сложнее.

Также в статье рассматриваются тренды, которые помогают обеспечивать стабильную безопасность для предприятий и работают на повышение эффективности их деятельности.

Ключевые слова: экономическая безопасность, комплексная безопасность, тенденции развития комплексной безопасности, базовые показатели комплексной безопасности, хозяйствующий субъект.

CHARACTERISTICS AND BASIC INDICATORS OF COMPREHENSIVE SECURITY OF THE ENTERPRISE

Vasilevykh V. A.,
student,
Vyatka State University
Kirov, Russia

Smirnov F. E.,
student,
Vyatka State University
Russia, Kirov

Sysheva A. R.,
student,
Vyatka State University
Russia, Kirov

Kotanjyan A. V.,
Senior Lecturer at the Department of Finance and Economic Security,
Vyatka State University
Russia, Kirov

Annotation

Ensuring enterprise security is one of the pressing problems in modern society. First of all, the article examines the issue of forming a system for ensuring economic security, defines and analyzes the basic indicators of comprehensive security, and identifies trends in its development. The conclusion is formulated that ensuring the economic security of an enterprise is becoming more difficult. The article also discusses trends that help ensure stable security for enterprises and work to improve the efficiency of their activities.

Key words: economic security, integrated security, trends in the development of integrated security, basic indicators of integrated security, economic entity.

Введение:

Обеспечение безопасности предприятия в современном обществе — это одна из актуальных проблем. В первую очередь исследователи рассматривают вопрос формирования системы обеспечения экономической безопасности. Такое внимание хозяйствующие субъекты получили из-за того, что на их экономическую активность оказывают влияние макроэкономические и микроэкономические факторы. В результате чего обеспечивать экономическую безопасность предприятия становится сложнее. Тогда на помощь приходит комплексная безопасность, охватывающая не только аспекты экономической безопасности, но и физическую безопасность, защиту от внутренних угроз.

Цели и задачи исследования:

Цель — определение понятия комплексной безопасности предприятия и рассмотрение её базовых показателей.

Задачи:

1. Дать характеристику основным терминам в области комплексной безопасности предприятия.

2. Обозначить тенденции развития и охарактеризовать базовые показатели комплексной безопасности.

3. Рассмотреть высокотехнологичные тренды, которые помогают обеспечивать стабильную безопасность для предприятий.

Основная часть:

Чтобы разобраться в данной теме, необходимо проанализировать понятие экономической безопасности. Под ним понимается состояние безопасности экономического субъекта, обеспечивающее наиболее оптимальное использование ресурсов.

Система безопасности представляет собой полноценный комплекс различных мер. Его основные цели заключаются в следующем:

— мониторинг и прогнозирование угроз экономической безопасности компании;

— оценка рисков и угроз с использованием количественных и качественных методов;

— разработка инструментов и механизмов для смягчения угроз и поддержания стабильного развития предприятия;

— постоянное совершенствование механизма обеспечения экономической безопасности. [4]

Рассмотрим базовые показатели и характеристики комплексной безопасности. Система безопасности предприятия — это система выявления, предотвращения, пресечения, минимизации посягательств на жизнь и здоровье сотрудников, а также на законные права организации, бизнес, интеллектуальную собственность, внутреннюю дисциплину, научные достижения и защищенную информацию.

При оценке компании выбираются те сферы её деятельности, которые наиболее подвержены уязвимости. Как правило, к этим направлениям относятся: защита материальных и финансовых ресурсов, физическая защита рабочего

персонала и эффективное управление им, защита интеллектуальной собственности, защита информационных ресурсов. [5]

Каждый из этих параметров оценивается в ходе оценки безопасности предприятия — в дальнейшем выбранный для них рейтинг будет использоваться при поиске способов их нейтрализации. Для выявленных опасностей применяются следующие меры:

— физические: создание препятствий в доступе к охраняемому имуществу, финансам, информации;

— административные: внедрение соответствующего режима работы бизнеса, создание службы безопасности;

— экономические: меры материального стимулирования, финансирование защитных мероприятий;

— технические: использование технических средств и систем безопасности;

— программное обеспечение: использование современных информационных технологий, баз данных, систем защиты от несанкционированного доступа к ним и т.п.;

— морально-этические: меры морального воздействия;

— воспитательная работа;

разработка кодексов поведения, создание атмосферы корпоративного духа, партнерства единомышленников и т.д. [2]

Однако контроль и оценка экономической безопасности предприятия проходят не так гладко, как хотелось бы. На эффективность мер экономической безопасности на предприятии влияют многие факторы, в том числе: соблюдение действующих нормативных актов, выявление и пресечение посягательств на законные права организации, ее имущество, положительные финансово-хозяйственные условия, стабильность экономических связей, моральные психологический климат в коллективе, производственная дисциплина.

Сначала проводится оценка, а затем исследование экономической эффективности предприятия.

При этом наиболее уязвимые каналы в экономической безопасности определяются устройством предприятия и уровнем, на котором оно работает. Одно из самых уязвимых мест — это традиционно плохая организация учета, хранения и прохождения документов, содержащих данные сведения. Причём такую проблему можно наблюдать вне зависимости от уровня предприятия.

При обнаружении такой проблемы руководству организации следует обратить внимание на делопроизводство и преобразовать существующую систему с целью сохранения коммерческой тайны таким образом, чтобы возможность утечки данных была сведена к минимуму, а в случае ее возникновения она могла бы быть устранена.

Вторым важнейшим аспектом обеспечения экономической безопасности является устранение или минимизация человеческого фактора. Основная проблема обеспечения экономической безопасности предприятия при устранении этого фактора состоит в том, что полностью исключить влияние действий сотрудников на информацию, используемую в работе, сложно и практически невозможно. Чтобы избежать потери данных в работе из-за ошибок персонала или перебоев в подаче электроэнергии, достаточно обеспечить системы предприятия облаком для резервного копирования данных. Однако при использовании такой технологии возникает другая проблема – данные, автоматически передаваемые в облако, нуждаются в защите, т.е. необходимо обеспечить как минимум надежное шифрование.

Но вернемся к человеческому фактору, который можно назвать проблемой экономической безопасности. Чтобы свести её к минимуму, работникам необходимо обеспечить достойную заработную плату, страхование и профсоюзную организацию по месту работы – для защиты нарушенных прав работников.

При этом даже соблюдение вышеперечисленных параметров не гарантирует, что человек не передаст конкурентам коммерчески важную для конкретной компании информацию. Поэтому важно ограничить доступ к информации, составляющей коммерческую тайну, и предоставить ее узкому кругу лиц. [1]

Тенденции развития комплексной безопасности. Государственные правоохранительные органы в настоящее время не могут в полной мере обеспечить необходимый уровень безопасности всех объектов различных форм собственности. Поэтому руководство многих компаний ищет пути решения этой проблемы собственными средствами, в первую очередь путем создания собственных служб безопасности с широким использованием технических средств и систем.

Основными тенденциями развития современных систем безопасности являются процессы автоматизации, интеграции и компьютеризации на основе искусственного интеллекта.

Обеспечение безопасности и жизнедеятельности включает в себя широкий комплекс мероприятий, направленных на защиту от различных видов угроз, источником которых (и объектом защиты) могут быть три основные части: человек, природа и техногенная среда (все, что создано так называемый человек). [4]

В 2024 году индустрия безопасности продолжает развиваться, несмотря на социальные и экономические факторы, оказавшие глубокое влияние на бизнес и рынок в целом. Помимо традиционной физической безопасности, крупные и малые предприятия внедряют высокотехнологичные решения на основе искусственного интеллекта (ИИ), облачных вычислений и Интернета вещей, уделяя особое внимание обеспечению киберзащиты систем и данных. Индустрия безопасности постепенно движется к более широкому спектру продуктов и услуг, которые не только обеспечивают защиту, но и работают на повышение эффективности бизнеса и создают добавленную стоимость для отдельных

пользователей и компаний, для общества и государства. Рассмотрим некоторые их таких высокотехнологичных решений.

Тренд № 1. Искусственный интеллект везде и во всем.

Искусственный интеллект уже давно используется в системах безопасности, и с каждым годом количество пользователей и поставщиков умных решений будет стремительно расти. Все большее число участников рынка безопасности осознают ценность приложений и функций искусственного интеллекта и находят новые области и варианты использования. Разрабатываются интеллектуальные решения ANPR для парковки и растет количество систем на основе интеллектуальной видеоаналитики, позволяющих снизить количество ложных срабатываний и повысить эффективность охранных устройств.

Тренд №. 2. Конвергентные системы как замена традиционным хранилищам данных. Когда данные хранятся в хранилищах, сложно обмениваться информацией и совместно работать над ней, а у участников нет общего понимания ситуации и текущих операций, выполняемых различными группами пользователей. Решение проблемы — создание конвергентной инфраструктуры, устраняющей недостатки независимых, отдельных систем обработки и хранения данных. В сфере безопасности сохраняется тенденция объединения отдельных систем – видеонаблюдения, контроля доступа, сигнализации и других. К той же инфраструктуре подключены и другие решения, не связанные напрямую с безопасностью, такие как управление персоналом, финансы, логистика и корпоративные платформы. Конвергенция улучшает сотрудничество и помогает более эффективно и быстро принимать стратегические решения на основе большего количества данных и аналитики.

Тренд №. 3. Облачные решения и сервисы. Как и искусственный интеллект, облачные технологии не являются чем-то новым в сфере безопасности. Однако в последние годы многие компании стали все чаще обращаться к платформам и сервисам, обеспечивающим возможность удаленной

работы и удаленного доступа к различным системам, в том числе к системам безопасности. Облачные решения устраняют необходимость использования локального сервиса или дополнительного программного обеспечения. Пользователь может выполнять необходимые операции – например, проверять рабочее состояние систем, получать тревожные уведомления, реагировать на события – из любой точки мира с помощью мобильных устройств. Отдельно стоит выделить развитие облачных сервисов и создание дополнительной ценности для поставщиков услуг безопасности – монтажных организаций и сервисных компаний, для которых облачные приложения создают дополнительный бизнес-инструмент для удаленной настройки пользовательских систем, решения технических проблем и обновления. программное обеспечение.

Тренд №. 4. Высокая детализация изображения в любых условиях – новый отраслевой стандарт. Для систем безопасности важно поддерживать высокий уровень производительности 24 часа в сутки. Для камер видеонаблюдения важно сохранять высокое качество изображения при любых условиях, включая низкую освещенность или неблагоприятные погодные условия. Количество запросов на камеры с технологиями создания полноцветного и детального изображения в требовательных условиях безопасности стремительно растёт. Такие системы используются на крупных инфраструктурных объектах: аэропортах, вокзалах и городских площадях, стадионах, автостоянках, парках и т.д.

Тренд №. 5. Биометрические технологии контроля доступа. Сегмент систем контроля доступа в настоящее время все еще переживает переходный период, но тенденция перехода на биометрические технологии становится все более заметной. В настоящее время рынок предлагает широкий спектр решений биометрической идентификации: распознавание лиц, отпечатков пальцев, ладони, рисунка вен и чтение сетчатки. Главным преимуществом биометрии является высокая степень достоверности и точности распознавания. Системы распознавания лиц из этого списка становятся все более популярными как самый удобный и быстрый способ бесконтактной идентификации пользователя.

Тренд №. 6. Системы безопасности начинают использовать модель нулевого доверия: минимальное доверие, максимальный контроль. Чем больше устройств подключаются к сети, тем актуальнее становится вопрос кибербезопасности. После нескольких крупных хакерских атак на инфраструктуру по всему миру в последние годы укрепление архитектуры сетевой безопасности, а также обучение и повышение знаний конечных пользователей в этой области становятся главным приоритетом. Концепция нулевого доверия или «нулевого доверия» была разработана еще в 2010 году, но лишь недавно получила широкое распространение и популярность. Стратегическая инициатива Zero Trust основана на постулате «никогда не доверяй и всегда проверяй» и направлена на предотвращение утечки данных и повышение уровня безопасности современных информационных систем.

Тренд №. 7. Растущий спрос на «зеленое» производство и «зеленые» технологии. В мире принят тренд на экологически чистые материалы и энергоэффективные технологии. Растет спрос на устройства, оснащенные солнечными батареями, в том числе на устройства безопасности. Спрос заставляет инженеров создавать все более сложные и в то же время более экологичные системы, которые работают на солнечной энергии и могут использоваться не только в городских районах, но и в отдаленных районах, где имеется сложная инфраструктура. Что касается производства, все большее число стран запускают инициативы по вознаграждению предприятий, которые используют экологически безопасные методы и энергоэффективные технологии и разработки.

Результаты и заключение:

Подводя итог, хотелось бы сказать, что вопросы безопасности важны для обеспечения экономической безопасности. Причиной этого является то, что недостаточный уровень физической, экономической, информационной и экологической безопасности предприятия может привести к различного рода

ущербам, характер и масштабы которых снизят уровень конкурентоспособности и эффективности хозяйственной деятельности предприятия, что может повлечь возникновение вопроса о его банкротстве и ликвидации. Рассмотрены основные термины в области безопасности, сформулировано определение корпоративной безопасности, наиболее подходящее для использования при организации и управлении деятельностью в сфере комплексной корпоративной безопасности. Обозначены тенденции развития обеспечения комплексной безопасности материальных объектов и средств предприятия, его экономической (финансовой) и экологической безопасности. Основные понятия интегрированной системы безопасности предприятия, представленные в данной статье, могут быть использованы менеджерами при разработке интегрированной системы управления предприятием. Для того, чтобы создать систему безопасности организации или бизнеса, необходимо сначала сформулировать, какие функции будут на нее возложены, выявить потенциально опасные объекты и проанализировать степень их защищенности.

Библиографический список:

1. Криворученко Ю.А., Шевченко М.В. Проблема оценки угроз экономической безопасности предприятия и способы их устранения // IX Международный молодежный форум «Образование. Наука. Производство» Белгород, 2017. С. 2691–2695.

2. Рябов Д.И., Хахалева Е.Н. Основные направления обеспечения экономической безопасности предприятия // Международная научно-техническая конференция молодых ученых БГТУ им. В.Г. Шухова, 2016. С. 4860–4863.

3. Сергеева. И.А. Комплексная система обеспечения экономической безопасности предприятия: учеб. Пособие. - Пенза: Изд-во ПГУ, 2017. С. 34–36.

4. Серебрякова Н.А., Волкова С.А., Волкова Т.А. Формирование системы обеспечения экономической безопасности предприятия // Вестник ВГУИТ. - 2016. - №4. - С. 460–465.

5. Уразгалиев, В.Ш. Экономическая безопасность. Учебник и практикум для вузов. - СПб.: Издательство «Юрайт», 2017. С. 66-70.

Оригинальность 76%