SECURITY DIMENSIONS
INTERNATIONAL & NATIONAL STUDIES
NO. 11; 2014 (241-251)

СИСТЕМА УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ ИНФОРМАЦИИ - ЭФФЕКТИВНОЕ ОРУДИЕ ПОЛИТИКИ ИНФОРМЦИОННОЙ БЕЗОПАСНОСТИ

INFORMATION SECURITY MANAGEMENT SYSTEM – EFFECTIVE TOOL INFORMATION SECURITY POLICY

Юлиуш Пивоварски [Juliusz Piwowarski] [1]
Мариуш Розвадовски [Mariusz Rozwadowski] [2]

[1,2] School of Higher Education in Public and Individual Security "Apeiron" in Kraków

ВВЕДЕНИЕ
ABSTRTACT

Система управления Безопасностью информации (СУБИ)- эффективноое орудие политики информационной безопасности. Ее использование позволяет оценить риск, позволяет правильно обслуживать риск,, эффективно управлять безопасностью информаци внутри организации и в контактах с посторонними. Очень важно при этом, чтобы обеспечить безопасность человевеческих ресурсов и информации, компьютерных систем и особенно важных данных, Универсальный характер СУБИ) позволил использовать ее в организацищях, как частного так и публичного секторов.

Information Security Management System is an effective information security policy. Its application allows estimating the risk, service risk in an appropriate manner, the effective management of information security within the organization and in dealing with others. It is very important to ensure the safety of human resources and information systems, networks and sensitive data. The universal character of the ISMS resulted in its use in organizations in the private and public sectors.

ARTICLE INFO

Article history
Received 05.05.2014 Accepted 16.07.2014

Keywords
политика безопасноти информации, система управления безопаностью информации, особо важные ресурсы

1. ВВЕДЕНИЕ

Уровень достижения намеченной цели свидетельствует об эффективности деятельности и развития организацции, как частного, так и публичного секторов. В принадлежащим к второму столпу культуры безопасности[1] процессе современных технологий, характерных для профиля работ организациии.Информация - важнейший актив организации, часто, решающий о ее успехе или поражении. Поэтому она должна быть соответстующим образом защищена. Защитой важной дла организации информациии должно заниматься ее руководство и все ее сотрудники. Важно, чтобы для обеспечения высокого уровня защиты информации, анализа и оценки возникающего риска,

[1] J. Piwowarski, *Kultura bezpieczeństwa,* [в:] „Kultura bezpieczeństwa. Praktyka – Nauka – Refleksje", Apeiron WSBPiA, No. 12, Kraków 2012.

создать политику безопасности информации, соответствуюшую данной организации. Для этой цели следует правильно организовать активы организации, как информационные, так и личностные и надлежащим образом ими управлять. Способстующим орудием для реализации этой цели будет установление и реализацция а также строгое соблюдение Системы Управения безопасностью Информаци (СУБИ). (СУБИ) - универсальная категория, опираюшаяся на подход, вытекающий из бизнес-риска, касающаяся установления, внедрения, эксплуатации, мониторинга, хранения и совершенствования безопасности информации. Она содержит организационную структуру, политику, планируемые действиия, сферу ответственности, правила, процедуры и ресурсы. Правильное выполнение (СУБИ) - одно из условий достижения конкурентного преимущества и успехов организации.

2. БЕЗОПАССНОСТЬ ИНФОРМАЦИИ И УПРАВЛЕНИЕ РИСКОМ В ОРГАНИЗАЦИИ

Организацция, которая в настоящее время желает надлежащим образом защитить свою информацию, должна применить системный подход, в рамках которого будет комплексно управлять имеющимися информационными активами, инфраструктурой, исспользуемой для ее обработки и риском, связаннным с безопасностью информациии. Безопасность информации, понимаемой, как активы организации, важно, как для частного, так и для публичного секторов. В обоих секторах инффформация часто действует как рычаг бизнеса. Взаимопроникновение обоих секторов и совместное использование информационых ресурсов осложняет удержание контроля за доступом. Безопасность информации должно опираться на следующие свойства:

- конфиденциальность,
- интегральность;
- доступность.

Конфиденциальность информации состоит в том, что информация не предоставляется и не раскрываетсся неуполномоченным лицам, субектам или процессам[2], Интегральность же это свойство, состоящее в обеспечении точности и комплектности активов[3]. Последним из обигаторных свойств безопасности информации является доступность, состоящая в том, что она доступна и полезна по требованию уполномоченого субъекта[4]. Дополнительными свойствами безопасноости информации, зависимыми от осуществляемой организацциией политики безопасности информацции, могут быть:

- возможность подсчета и расчета;
- иадежность,
- подлинноть,
- неоспоримость.

Об эффективности работы и развития организацции свидетельствует степень достижения намеченной цели. В этом процессе очень важно применение современных техник и технологий, орудий информационных систем и обработки и управления информацией. Информация, как важнейший из резурсов организацции, решающий о ее успехах, должна защищаться, как руковоством, так и другими сотрудниками организации. Фирмы, которые стого соблюдают этот приказ успешно работают в своей среде и динамически развиваются. При этом важно, чтобы обеспечить правильную защиту информации, то есть, обеспечить высокий уровень безопаности информационных систем. С этой целью следует адекватно организовать ресурсы

[2] Polska Norma *PN-ISO/IEC 27002*,PKN, Varshava, 2007, c. 9.
[3] Ibidem.
[4] Ibidem.

организации, эффективно ими управлять и свести к минимуму риск утечки ценнной для конкуренции информации. Связано это с правильно разработанной и строго соблюдаеемой политикой безопасности информации, которая является одним из условий дотижения успехов на рынке. Существенной особеностью управления безопасностью информацции является риск. Риск - объективизированная неуверенность возникновения нежелаемого события, риск меняется совместно с неуверенностью, а не с уровнем вероятности[5]. По мнению Samuelsona W. F и Marksa S.G.[6], риск или вместо него неуверенность, появляется тогда,когда имеется больше, чем один возможный результат нашего решения. Другое мнение высказывает T. Kaczmarek, который утверждает, что риск это возможность появления отсутствия успеха, в частноти возможноть возникновения событий, незаисимых от действущего субъекта, которых он не может точно преумостретть и не может предотвратить их возникновение, и, которые - путем сокращения полезных результатов и/или путем увеличения вложенных средств - лишают действия частично или полностью, свойств выгоды или экономичности[7]. Словацкий автор J. Mikołaj говорит, что риск определяется как что-то непостоянное, неопределенное, что связано с ходом явления и что нарушает его целевое стремление и подчеркивает, что риск, неуверенннность и неопределенность являются элементами действий человека в определенной среде. Риск связан с действиями человека, неуверенность же с состоянием среды или ограниченностью системы окружения[8]. Имеется много методов оценки риска. К ним принадлежат применяемые на практике, интуитивные методы,, указатеьные, точечные, упрощеннные, симулятувные, статистические, дискриминационые. В экономической деятельности полное устранеение риска невозможно, его можно только ограничить, путем правильного управления им. Управление риском это его идентификация, измерение, упправление и контроль за ним с целью максимального его ограничеиия или страхования от результатов риска[9]. Другое определение управления риском приводят W. Jaworski, Z. Zawadzka. По их мнению под управлением риском следует понимать мероприятия, имеющие своей целью плановый ии целевой анализ, упраление рисками, возникающими в процессе деятельносстти (банковской, экономической) и контроль за принимаемыми решениями[10].

3. ПОЛИТИКА БЕЗОПАСНОСТИ ИНФОРМАЦИИ - ПОНЯТИЕ И СУЩНОСТЬ

Политика беопасности информаци (ПБИ) - совокупность согласованных, точных правил и процедур, согласно которым данная организация формулирует, управляет
и предоставляет ресурсы, а также информационные и информатические системы. ПБИ определяет, какие ресурсы и каким образом следует защищать. Она должна также указывать возможные виды нарушения безопасности (например,

[5] A.H. Willet, *The Economic Theory of Risk Insurance*, Philadelphia, 1951, c. 6.

[6] W.F. Samuelson, S.G. Marks, *Ekonomia menedżerska*, PWE, Warszawa, 1998, c. 323.

[7] T. Kaczmarek, *Zarządzanie ryzykiem handlowym i finansowym dla praktyków*, Ośrodek Doradztwa i Doskonalenia Kadr, Gdańsk, 1999, c. 11.

[8] J. Mikolaj, *Rizikovy manazment*, RVS FSI ZU, Żylina, 2001, c. 17.

[9] D. Dziawgo, *Zarządzanie ryzykiem w banku komercyjnym*, [в:] *Bankowość. Podręcznik dla studentów*, (ред.) J. Głuchowski, J. Szambelańczyk, WSB, Poznań, 1999, c. 351–398.

[10] W.L. Jaworski, Z. Zawadzka, *Bankowość. Podręcznik akademicki*, Poltext, Warszawa 2002, c. 607.

потеря данных, неавторизованный доступ), а также сценарии поведения в таких ситуациях и действия, которые позволят избежать повторения определенного инцидента. Политика безопасности должна точно определять способ использования ресурсов (счетов потребителей, данных, компьютерных программ), а также должна быть документом, составленнным в письменной форме и известным и понятным всем сотрудникам организации, пользующимся информациоными ресурсами. Она касаетсся также и клиентов организацции (тех, кто пользуется ее ресурсами). При проектировании (ПБИ) следует рассмотреть, сможет ли оганизация нести расходы по ее внедрению. Важнейшее меропприятие до внедрения (ПБИ) является проведение анализа риска и определение одобряемого допускаемого уровня риска. ПБИ должна касаться следующих воросов:

- что должно поддлежать защите в организации?
- как следует защищать критические ресурсы организации?

В каждой организации имется разнообразная информация, которая должна защищаться:

- для зашиты нтересов организации (например, информация, связанная со стратегическими бизнес-планами, финансовая информация, патенты и т.п.),
- в силу действия закона (личные данные, конфиденциальная информация)

Основная совокупность информации данной организации является открытой и касается всех вопросов, связанных с ее деятельностью. Это не значит, что она не должна защищаться, наоборот, каждая информация может подвергаться угрозе (уничтожения, фальсификации или нежелаемой модификации). Целью мероприятий по защите и безопасности информации в организации, является достижение такого организационного и технического уровня, который:

- обеспечит сохранение конффиденциальности защищаемой информации,
- обеспечит целостность защищаемой информации,
- обеспечит высокий уровень безопасности обрабатываемой информации,
- в максимальной степени ограничит возможность возникновения угроз для
- безопасности информации,
- обеспечит готовность предпринимать определенные действия в кризисных ситуациях.

Следовательно, ПБИ – совокупность документов, определяющих методы и правиила защиты и обеспечения безопасности инфформации в органиизации. Говоря по-другому, ПБИ - совокупность едиинных, точных и соответствующих действующему законодательству правил и процедур, по которым данная организация собирает, управляет и предоставляет ресурсы и информационные системы[11].Она составляетсся на основании действующих законов и распоряжений, касающихся защиты информации (например, конфиденцальная информация, личные данные), При проектировании ПБИ для определенной организации следует учитывать:

- характер организации (хозяйственнная единица, контора, исследовательский институт),
- своеобразие функционирования организации (производственная, оказание
- услуг),

[11] M. Kowalewski, A. Ołtarzewska, *Polityka bezpieczeństwa informacji na przykładzie Instytutu Łączności,* http://www.itl.waw.pl/czasopisma/TiTI/2007/3-4/3 (11.04.2010).

- организационную структуру (уровни управления),
- процессы, которые проходят в данной организации.

ПБИ в организации должна касаться всех членов организации и всех ее сотрудников. Она должна быть документом открытым, постоянно пополняеныым, модифицированным и приспособлнным для потребностей данной организации. Одним из важнейших элементов ПБИ является Система Управления Безопасностью Информации.

4. СИСТЕМА УПРАВЛЕНИЯ БЕЗОПАССНОСТЬЮ ИНФОРМАЦИИ

Организация в рамках осуществляемой политики безопасности информации должна исспользовать процессуальный подход для установления, внедрения, эксплуатации, мониторинга и постоянного совершенствования подтвержденной Системы Управления Безопасностью Информации (СУБИ). ISMS англ. Information Security Menagement System), определяется, как часть целостной системы управления, опирающаяся на подход, вытекющий из бизнес-риска, касаюшаяся установления, внедрения, эксплуатации, мониторинга, получения и совершенствования безопасности информацции. Она содержит организационнную структуру, политику, планируемые действия, сферы ответственности, правила, процедуры, процессы и ресурсы[12]. При процессуальном подходе к СУБИ ее пользователи должны обратить особое внимание на:

- пониманиие требований по безопасности информации в организации,
- цнедрение и эксплуатацию зашиты с целью надлежащего управления риском,

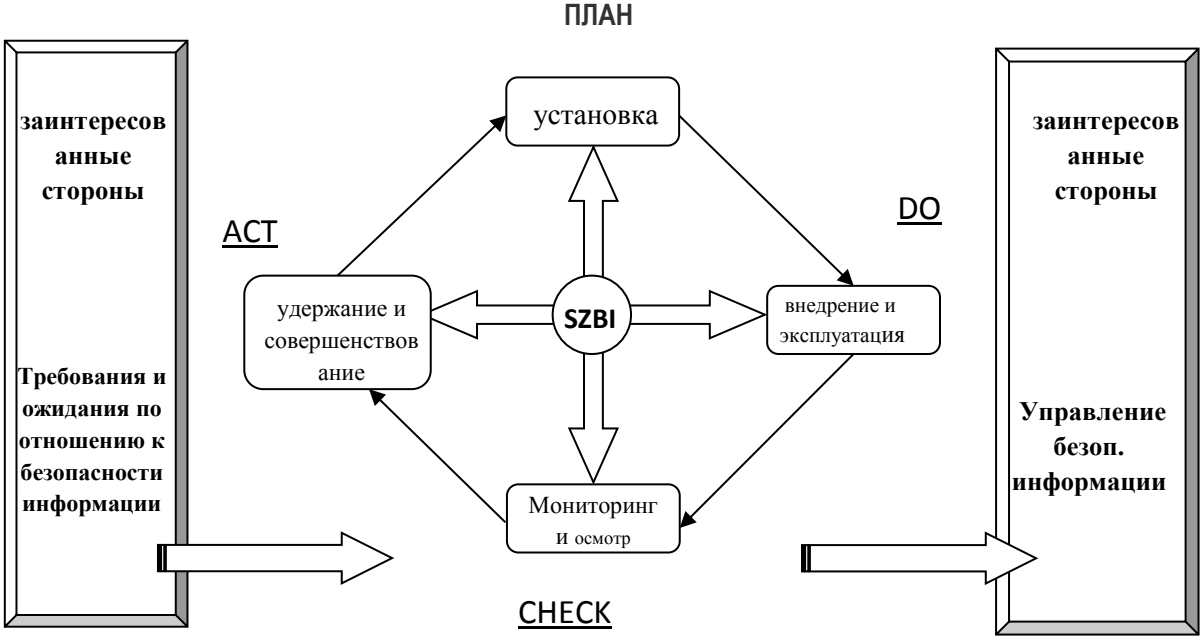

Рис. 1. Модель PDCA, используемая в процессах СУБИ Источник; собств.разраб. на основаании PN-ISO/IEC 227001, PKN, Warszawa 2007, с. 7.

[12] Ibidem, с. 9.

- мониторинг производительности и эффективноости СУБИ,

Внедрение эффективной СУБИ в организацци возможно, благодаря использованию нормы ISO/IEC 27002, предстацляющей процессуальный подход, показанный на рис. 1. Он показывает, каким образом СУБИ воспринимает требования по безопасности информацции, как исходную величину и через опеделеные процессы поставвляет исходную информацию, которая соответствует этим требованиям и ожиданиям

Модель PDCA (англ. _Plan-Do-Check-Act) Запланируй, Сделай, Проверь, Действуй, это схема, которая иллюстрирует основной принцип постояннного улучшения (постояннного совершенствования, Kaizen), созданную В. Демингом[13]. американским специалистом-статистиком, работающим в Японии. Он содержит четыре сектора, в рамках которых выполняютсся определенные действия.

В рамках сектора -Запланируй (установление СУБИ) выполяются следуюие дейстия:

- установление СУБИ,
- определние целей, процессов и процедур, важных для управления риском, оценки риска и совершенствования безопасноти информации.

В секторе - Сделай- (внедрение и эксплуатация СУБИ):

- внедрение СУБИ, защиты, процессов и процедур
- экаплуатация СУБИ, защиты, процессов и процедур

В секторе Проверяй (мониторинг и обзор СУБИ):

- оценка,
- постоянное совершенствование, основанниое на объективном измерении.
- измерение производительности процессов по отношению к СУБИ,
- передача руководству отчетов для рассмотрения .

В секторе же - Дейстуй - (сохранение и совершенсвование СУБИ):

- выполнение исправляющих и предотвращающих действий, на основании
- аудита или другой важной информации;
- постоянное совершенствование СУБИ на базе аудита и обзора, проведенного руководством.
-

Данная норма предусмотрена для организаций всех видов, как для бизнес-субеъктов, так и для субъектов публичной администрацции. Междунадная норма ISO 27002 (Информационная техника - Практические правила управления безопаноостью информации), определяет указания, связанные с установлением, внедрением, эксплуатацией, мониторингом, обзором, сохранением и совершенствованием СУБИ. Конструкция этой нормы строго связана с контрукцией приложения А нормы ISO/IEC 27001, Для каждого требования, определенного в этом приложении в норме ISO 27002 содержатся сооётветстущие рекомендации. Она содержит набор лучших приемов, которые можно применить в организации с целью повышения уровня безопасности информации. Она была разделена на 11 секторов, содержащих в общем итоге 39 категорий безопаноости, каждый сектор содержит определенное количество категорий безопасности. Сектора, содержащиеся в норме, это:

- политика безопасности иинформацции,
- организация безопасности информацции,
- управление активами,

[13] A. Hamrol, W. Mantura, *Zarządzanie jakością – teoria i praktyka*, Wydawnictwo Naukowe PWN, Warszawa 2002, c. 93.

- безопасность человеческих ресуурсов,
- физическая безопасность и безопасность среды;
- управленеи системами и сетями,
- контроль за доступом;
- приобретение, развитие и содержание информационных систем,
- управление инцидентами, связанными с безопасностью информации,
- управление постоянным продолжением деятельности;
- сответствие[14].

Особого внимания заслуживает сектор, касающийся продолжения деятельности организацции, действия. осуществляемые в рамках этого сектора создают возможность функционирования организации и воспроизведения функциональности оборудования для обработки информации и самой информации после возникновения катастроф или инцидентов. Система Управления Безопасностью Информации внедряемая в организиациях по норме PN-ISO/IEC 27001 приносит очевидную пользу, что показано в таблице 1. Представленные там данные подтверждают основные предпосылки для внедрения СУБИ, опирающейся на нормах ISO. Внедрение и использование СУБИ будет связано с возникновнием затрат, иногда даже очень большик. Поэтому, до внедрения СУБИ следует присмотреться к потребностям собственной организации и подумать о том, что предлагает норма ISO/IEC 27001 дает ли она гарантии надлежащей защиты активов организации.

Отсутствие в организаци СУБИ может вызвать рост затрат, что показано на рис. 2. Общая стоимость затрат в результате возникновения происшествий, потери репутации, дополнительной человеческой работы, связанной с физическим обеспечением информации, расходы по содержанию структур безопасности, часто значительно превышают расходы по внедрению и эксплуатации СУБИ. Могут возникнуть также и другие случаи, которые заставят организацию внедрить СУБИ. Ими могут стать:

- утечка конфиденциальной бизнес-информации из организации,
- потеря руководством организации контроля за безопаностью информации, важной с точки зрения деятельноти, осуществляемой организацией,
- отсутстве безопасного управления системами и сетями, безопасностью человеческих ресурсов и создание безопасных секторов,
- невозможность внедрния и поддержания оответствующего уровня безопасности информации, поставляемой третьими лицами.

[14] Zob. Polska Norma *PN-ISO/IEC 27002,* PKN, Warszawa 2007, c. 14.

ЧАСТНЫЙ СЕКТОР	ПУБЛИЧНЫЙ СЕКТОР	ПОЛЬЗА
1	2	3
+	+	• выполнение требований законов: • закона о защите личных данных • закона о доступе к публичной информации; • закона об авторских правах и смежных правах
+	+	• избежание штрафа за нарушение безопасности информации
+	+	• защита информации, находящейся в обороте в рамках организации
+	+	обеспечение информации на случай катастроф, аварий происшествий.
+	+	упорядочение информацции, обрбатываемой организацией
+	+	рост сознания сотрудников по вопросу о безопассности информации
+	+	убеждение клиентов,что их данные правильно защищены
+	+	требования к торгам
+	+	достовернось организации по отношению к клиенту
+	+	управление продолжительностью деятельности
+	+	выполнение юридических требований по безопасности информации, и определение полтики безопасности информации
+	+	оценка рииска, связанного с управлением информацией
+	+	организация физической и информационной безопасности информации
+	+	управлние информационными системами и компьютерными сетями с точки зрения безопассности информации
+	+	определение в виде процедур поведениия по ходу обычного функционирования и поведения в кризисных ситуациях.

Таблица 1. Польза, возникающая в результате применения нормы PN-ISO/IEC 27001 в организациях.
ПО: Собств. разработка на основании PN-ISO/IEC 27001 и PN-ISO/IEC 27002.

Приложение А к норме ISO27001 и которые следует выполнить, чтобы ISO27002 содержит целый ряд действий, организация могла обеспечить

безопасность своих человеческих и информационных активов. Там имеются записи, касающиеся достижения следуюших целей организации:

- убеждение в том, то руководство поддерживает и управляет безопасностью имформации, согласно бизнес-требованиям и соответствующим постановлениям закона и внутренними регулировками,
- управление безопасностью информации внутри организации,
- удержание безопасности информациии, являющейся собтвенностью организации, которой управляют третьи лица,
- достижение и удержание ссоответсвующего уровня защиты активов организации,
- убеждение, что сотрудники, исполнители и потребители, представвляющие третью сторону понимают свои обязаннпсти, осознают угрозу и другие аспекты безопасности информации,

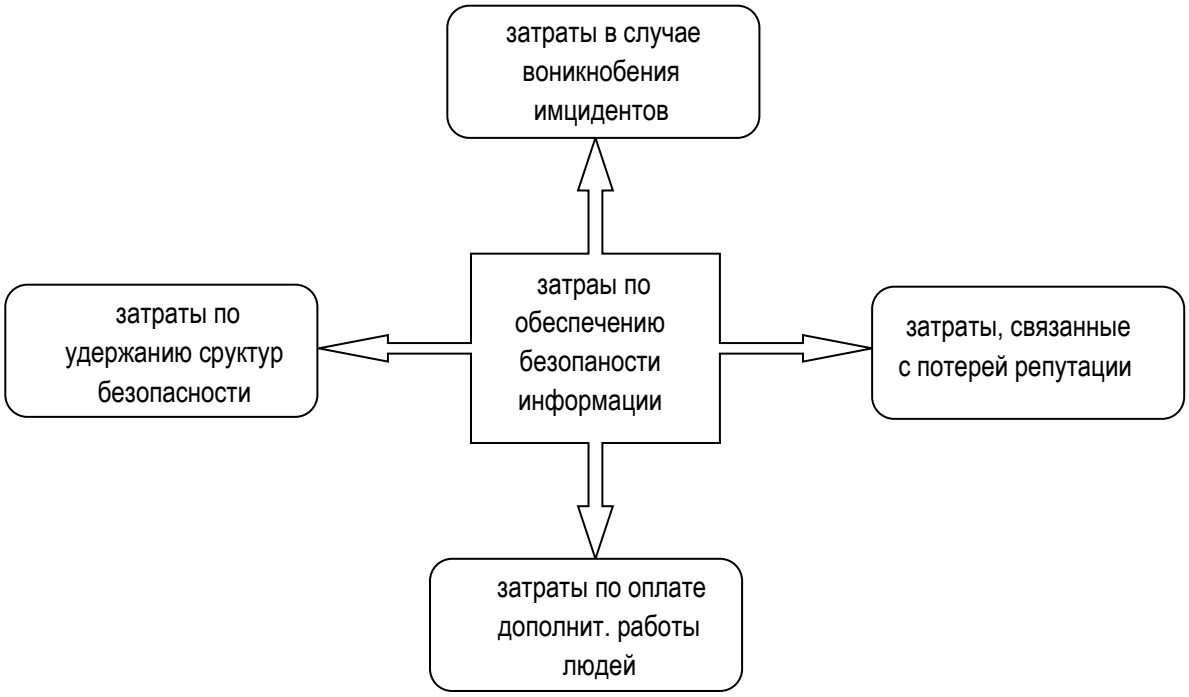

Рис. 2. Виды расходов, возникшие в результате отсутсвия СИБИ.
ПО: Собств. Разработка.

- обеспечение зашиты перед несанкционированным физическим доступом,
- повреждением или препятствиями по месту нахождения организации и по
- отношению к организации,
- онеспечение правильной и безопасной эксплуатации информационных систем
- и оборудования,
- обеспечение контроля за доступом к информации, к информациионным
- системам,
- предотвращение нарушения безопасности или кражи информации и средств
- передачи информации,
- убеждение, что применяется единый и эффективный подход к управлению

происшествиями, связанными с безопасностью информации,
- обеспечение продолжения деятельности организации,
- обеспечение соответствия систем со стандартами и политикой безопассности организации[15].
- Цели, описанне в норме, являются общими и поэтому могут применяться во всех типах организаций, как частного, так и публичного секторов. Они определяют требования, касающиеся установления, внедрения, эксплуатации, осмотра и совершенствования СУБИ. Составленная на основании этой нормы СУБИ дает гарантии безопасности всех активов организации и предоставляет возможность добиться доверия контрагентов.

5. ЗАКЛЮЧЕНИЕ

Информация и поддерживающие ее процессы, системы и сети это важные бизнес-факторы, как для частного, так и публичного секторов. Правильная идентификация, внедрение, сохранение и совершенствование безопасности информации необходимы для организации, стремящейся удержать высокую конкурентную позицию на рынке, финансовую ликвидность и деятельность, сооотвествующую требованиям закона. Она позвооляет также удержать репутацию организации, особенно важную для публичного сектора. Правильно созданная Система Управления Безопасностью Информации позволяет оценить риск и дает возможность правильно поступать в случае возникновения риска, введение соответствующей организации политики безопасности информации, правильное управление безопасностью информации внутри организации. Обеспечиает также безопасность информации в контактах с третьими лицами. Важной чертой СУБИ является обеспечение безопасности человеческих ресурсов, информационных систем, сетей и носителей данных. Внедрение СУБИ должно стать для каждой организации стратегическим решением, необходимым для обеспечения ее эффективного функционирования и реализаци „процессуального подхода", связанного с применением в организации системы процессов, совместно с их идентификациией и интеракцией.

[15] Polska Norma *PN-ISO/IEC 27002,* PKN, Warszawa, 2007, c. 17–112.

ЛИТЕРАТУРА

REFERENCES

1. Dziawgo D. , *Zarządzanie ryzykiem w banku komercyjnym*, [в:] *Bankowość. Podręcznik dla studentów*, (ред.) Głuchowski J., Szambelańczyk J., WSB, Poznań 1999.
2. Hamrol A, Mantura W, *Zarządzanie jakością – teoria i praktyka*, Wydawnictwo Naukowe PWN, Warszawa 2002.
3. Jaworski W.L., Zawadzka Z., *Bankowość. Podręcznik akademicki*, Poltext, Warszawa 2002.
4. Kaczmarek T., *Zarządzanie ryzykiem handlowym i finansowym dla praktyków*, Ośrodek Doradztwa i Doskonalenia Kadr, Gdańsk 1999.
5. Kowalewski M, Ołtarzewska A, *Polityka bezpieczeństwa informacji na przykładzie Instytutu Łączności,* http://www.itl.waw.pl/czasopisma/TiTI/2007/3-4/3.
6. Mikolaj J., *Rizikovy manazment*, RVS FSI ZU, Żylina 2001.
7. Piwowarski J., *Kultura bezpieczeństwa*, [в:] „Kultura bezpieczeństwa. Praktyka – Nauka – Refleksje" Apeiron WSBPiA, No. 12, Kraków 2012.
8. Polska Norma *PN-ISO/IEC 27001,*PKN, Warszawa 2007.
9. Polska Norma *PN-ISO/IEC 27002,*PKN, Warszawa 2007.
10. Samuelson W.F., Marks S.G., *Ekonomia menedżerska*, PWE, Warszawa 1998.
11. Willet A.H., *The Economic Theory of Risk Insurance*, Philadelphia 1951.

AUTHORS

Доктор Юлиус Пивоварkий - ректор Школы общественной и индивидуальной безопасности "Apeiron" в Кракове, научные специальности: философия безопасности, член Международной боевых искусств и боевого спорта научное общество (IMACSSS), 9 дан каратэ, кикбоксинг 8 дан, 5 дан джиу-джитсу.

Мариуш Розвадовский Доктор экономических наук в дисциплине науки управления. Специализируется в науке о безопасности и управления безопасностью. Он является автором ряда публикаций по вопросам управления безопасности в общественных организациях, управления информацией, защиты информации стратегического предприятия и комплексную политику безопасности. Он является преподавателем Краков школы бизнеса в Университете экономики в Кракове, проводит занятия в различных областях последипломного Краковского школы бизнеса в области экономической разведки и контрразведки. Университет Экономики в Кракове, используют в качестве представителя ректора Безопасность и защита конфиденциальной информации.

Он учит объем интегрированной политики безопасности на всех областях исследования. Он имеет ряд специализированной подготовки в области защиты секретной информации, персональных данных и управления безопасностью, организованном Национальной ассоциацией по защите секретной информации и Агентства внутренней безопасности, является экспертом Центральной экзаменационной комиссии. Он преподаватель в Школе общественной безопасности и индивидуальный "Апейрон".