

Juliusz Piwowarski, Mariusz Rozwadowski

Система управления Безопасностью информации - эффективное орудие политики информационной безопасности

Security Dimensions. International & National Studies nr 1 (11), 241-251

2014

Artykuł został opracowany do udostępnienia w internecie przez Muzeum Historii Polski w ramach prac podejmowanych na rzecz zapewnienia otwartego, powszechnego i trwałego dostępu do polskiego dorobku naukowego i kulturalnego. Artykuł jest umieszczony w kolekcji cyfrowej bazhum.muzhp.pl, gromadzącej zawartość polskich czasopism humanistycznych i społecznych.

Tekst jest udostępniony do wykorzystania w ramach dozwolonego użytku.

СИСТЕМА УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ ИНФОРМАЦИИ - ЭФФЕКТИВНОЕ ОРУДИЕ ПОЛИТИКИ ИНФОРМАЦИОННОЙ 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 ABSTRACT

Система управления Безопасностью информации (СУБИ)- эффективное орудие политики информационной безопасности. Ее использование позволяет оценить риск, позволяет правильно обслуживать риск,, эффективно управлять безопасностью информации внутри организации и в контактах с посторонними. Очень важно при этом, чтобы обеспечить безопасность человеческих ресурсов и информации, компьютерных систем и особенно важных данных, Универсальный характер СУБИ) позволил использовать ее в организациях, 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 безопасности информации, система управления безопасностью информации, особо важные ресурсы

1. ВВЕДЕНИЕ

Уровень достижения намеченной цели свидетельствует об эффективности деятельности и развития организации, как частного, так и публичного секторов. В принадлежащим к второму столпу культуры безопасности¹ процессе

современных технологий, характерных для профиля работ организации. Информация - важнейший актив организации, часто, решающий о ее успехе или поражении. Поэтому она должна быть соответствующим образом защищена. Защитой важной для организации информации 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, соответствующую данной организации. Для этой цели следует правильно организовать активы организации, как информационные, так и личные и надлежащим образом ими управлять. Способствующим орудием для реализации этой цели будет установление и реализация а также строгое соблюдение Системы Управления безопасностью Информации (СУБИ). (СУБИ) - универсальная категория, опирающаяся на подход, вытекающий из бизнес-риска, касающаяся установления, внедрения, эксплуатации, мониторинга, хранения и совершенствования безопасности информации. Она содержит организационную структуру, политику, планируемые действия, сферу ответственности, правила, процедуры и ресурсы. Правильное выполнение (СУБИ) - одно из условий достижения конкурентного преимущества и успехов организации.

2. БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И УПРАВЛЕНИЕ РИСКОМ В ОРГАНИЗАЦИИ

Организация, которая в настоящее время желает надлежащим образом защитить свою информацию, должна применить системный подход, в рамках которого будет комплексно управлять имеющимися информационными активами, инфраструктурой, используемой для ее обработки и риском, связанным с безопасностью информации. Безопасность информации, понимаемой, как активы организации, важно, как для частного, так и для публичного секторов. В обоих секторах информация часто действует как рычаг бизнеса. Взаимопроникновение обоих секторов и совместное использование информационных 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 раскрывается неуполномоченным лицам, субъектам или процессам², Интегральность же это свойство, состоящее в обеспечении точности и комплектности активов³. Последним из обигаторных свойств безопасности информации является доступность, состоящая в том, что она доступна и полезна по требованию уполномоченного субъекта⁴. Дополнительными свойствами безопасности информации, зависимиыми от осуществляемой организацией политики безопасности информации, могут быть:

- возможность подсчета и расчета;
- надежность,
- подлинность,
- неоспоримость.

Об эффективности работы и развития организации 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 ресурсов организации, решающий о ее успехах, должна защищаться, как руководством, так и другими сотрудниками организации. Фирмы, которые строго соблюдают этот приказ успешно работают в своей среде и динамически развиваются. При этом важно, чтобы обеспечить правильную защиту информации, то есть, обеспечить высокий уровень безопасности информационных систем. С этой целью следует адекватно организовать ресурсы

² Polska Norma PN-ISO/IEC 27002, PKN, Warszawa, 2007, с. 9.

³ Ibidem.

⁴ Ibidem.

организации, эффективно ими управлять и свести к минимуму риск утечки ценной для конкуренции информации. Связано это с правильно разработанной и строго соблюдаемой политикой безопасности информации, которая является одним из условий достижения успехов на рынке. Существенной особенностью управления безопасностью информации является риск. Риск - объективизированная неуверенность возникновения нежелаемого события, риск меняется совместно с неуверенностью, а не с уровнем вероятности⁵. 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 Т. Kaczmarek, который утверждает, что риск это возможность появления отсутствия успеха, в частности возможность возникновения событий, независимых от действующего субъекта, которых он не может точно преумостреть 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 экономичности⁷. 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, неуверенность и неопределенность являются элементами действий человека в определенной среде. Риск связан с действиями человека,

неуверенность же с состоянием среды или ограниченностью системы окружения⁸. Имеется много методов оценки риска. К ним принадлежат применяемые на практике, интуитивные методы,, указательные, точечные, упрощенные, симулятивные, статистические, дискриминационные. В экономической деятельности полное устранение риска невозможно, его можно только ограничить, путем правильного управления им. Управление риском это его идентификация, измерение, управление и контроль за ним с целью максимального его ограничения или страхования от результатов риска⁹. Другое определение управления риском приводят W. Jaworski, Z. Zawadzka. По их мнению под управлением риском следует понимать мероприятия, имеющие своей целью плановый и целевой анализ, управление рисками, возникающими в процессе деятельности (банковской, экономической) и контроль за принимаемыми решениями¹⁰.

3. ПОЛИТИКА БЕЗОПАСНОСТИ ИНФОРМАЦИИ - ПОНЯТИЕ И СУЩНОСТЬ

Политика безопасности информации (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, с. 6.

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

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

⁸ J. Mikołaj, *Rizikovy manazment*, RVS FSI ZU, Žylna, 2001, с. 17.

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

¹⁰ W.L. Jaworski, Z. Zawadzka, *Bankowość. Podręcznik akademicki*, Poltext, Warszawa 2002, с. 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, составленным в письменной форме и известным и понятным всем сотрудникам организации, пользующимся информационными ресурсами. Она касается также и клиентов организации (тех, кто пользуется ее ресурсами). При проектировании (ПБИ) следует рассмотреть, сможет ли организация нести расходы по ее внедрению. Важнейшее мероприятие до внедрения (ПБИ) является проведение анализа риска и определение одобряемого допустимого уровня риска. ПБИ должна касаться следующих вопросов:

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

В каждой организации имеется разнообразная информация, которая должна защищаться:

- для защиты интересов 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 нежелательной модификации). Целью мероприятий по защите и безопасности

информации в организации, является достижение такого организационного и технического уровня, который:

- обеспечит сохранение конфиденциальности 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 правила защиты и обеспечения безопасности информации в организации. Говоря по-другому, ПБИ – совокупность единых, точных и соответствующих действующему законодательству правил и процедур, по которым данная организация собирает, управляет и предоставляет ресурсы и информационные системы¹¹. Она составляется на основании действующих законов и распоряжений, касающихся защиты информации (например, конфиденциальная информация, личные данные). При проектировании ПБИ для определенной организации следует учитывать:

- характер организации (хозяйственная 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 пополняемым, модифицированным и приспособленным для потребностей данной организации. Одним из важнейших элементов ПБИ является Система Управления Безопасностью Информации.

4. СИСТЕМА УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ ИНФОРМАЦИИ

Организация в рамках осуществляемой политики безопасности информации должна использовать процессуальный подход для установления, внедрения, эксплуатации, мониторинга и постоянного совершенствования подтвержденной Системы Управления Безопасностью

Информации (СУБИ). ISMS (англ. Information Security Management System), определяется, как часть целостной системы управления, опирающаяся на подход, вытекающий из бизнес-риска, касающаяся установления, внедрения, эксплуатации, мониторинга, получения и совершенствования безопасности информации. Она содержит организационную структуру, политику, планируемые действия, сферы ответственности, правила, процедуры, процессы и ресурсы¹². При процессуальном подходе к СУБИ ее пользователи должны обратить особое внимание на:

- понимание требований по безопасности информации в организации,
- внедрение и эксплуатацию защиты с целью надлежащего управления риском,

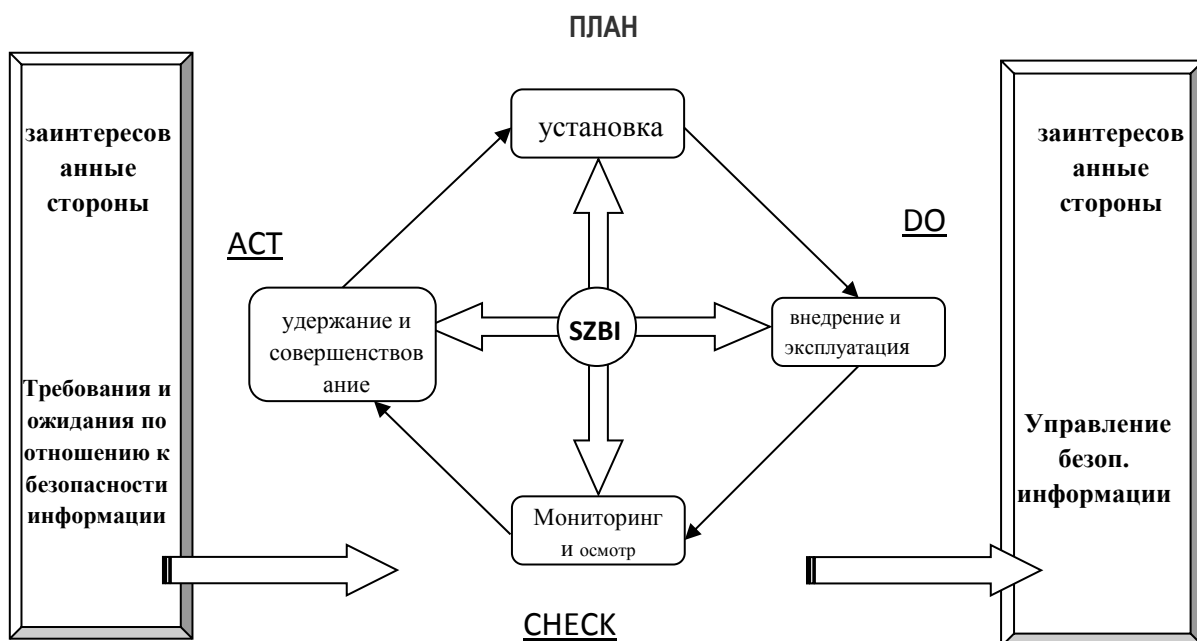


Рис. 1. Модель PDCA, используемая в процессах СУБИ Источник; собств.разраб. на основании PN-ISO/IEC 227001, PKN, Warszawa 2007, с. 7.

¹² Ibidem, с. 9.

- мониторинг производительности и эффективности СУБИ,

Внедрение эффективной СУБИ в организации возможно, благодаря использованию нормы ISO/IEC 27002, представляющей процессуальный подход, показанный на рис. 1. Он показывает, каким образом СУБИ воспринимает требования по безопасности информации, как исходную величину и через определенные процессы поставяет 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 постоянного улучшения (постоянного совершенствования, Kaizen), созданную В. Демингом¹³. америкским специалистом-статистиком, работающим в Японии. Он содержит четыре сектора, в рамках которых выполняются определенные действия.

В рамках сектора -Запланируй (установление СУБИ) выполняются следующие действия:

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

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

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

В секторе Проверь (мониторинг и обзор СУБИ):

- оценка,

- постоянное совершенствование, основанное на объективном измерении.

- измерение производительности процессов по отношению к СУБИ,
- передача руководству отчетов для рассмотрения .

В секторе же - Действуй - (сохранение и совершенствование 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-субъектов, так и для субъектов публичной администрации. Международная норма ISO 27002 (Информационная техника - Практические правила управления безопасностью информации), определяет указания, связанные с установлением, внедрением, эксплуатацией, мониторингом, обзором, сохранением и совершенствованием СУБИ. Конструкция этой нормы строго связана с конструкцией приложения А нормы ISO/IEC 27001, Для каждого требования, определенного в этом приложении в норме ISO 27002 содержатся соответствующие 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 безопасности, каждый сектор содержит определенное количество категорий безопасности. Сектора, содержащиеся в норме, это:

- политика безопасности информации,
- организация безопасности информации,
- управление активами,

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

- безопасность человеческих ресурсов,
- физическая безопасность и безопасность среды;
- управление системами и сетями,
- контроль за доступом;
- приобретение, развитие и содержание информационных систем,
- управление инцидентами, связанными с безопасностью информации,
- управление постоянным продолжением деятельности;
- соответствие¹⁴.

Особого внимания заслуживает сектор, касающийся продолжения деятельности организации, 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 организациях 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 возникновением затрат, иногда даже очень больших. 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 организации 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 безопасностью информации, важной с точки зрения деятельности, осуществляемой организацией,
- отсутствие безопасного управления системами и сетями, безопасностью человеческих ресурсов и создание безопасных секторов,
- невозможность внедрения и поддержания соответствующего уровня безопасности информации, поставляемой третьими лицами.

¹⁴ Zob. Polska Norma PN-ISO/IEC 27002, PKN, Warszawa 2007, с. 14.

ЧАСТНЫЙ СЕКТОР	ПУБЛИЧНЫЙ СЕКТОР	ПОЛЬЗА
1	2	3
+	+	<ul style="list-style-type: none"> • 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 информации, обрабатываемой организацией
+	+	рост сознания сотрудников по вопросу о безопасности информации
+	+	убеждение клиентов, что их данные правильно защищены
+	+	требования к торгам
+	+	достоверность организации по отношению к клиенту
+	+	управление продолжительностью деятельности
+	+	выполнение юридических требований по безопасности информации, и определение политики безопасности информации
+	+	оценка риска, связанного с управлением информацией
+	+	организация физической и информационной безопасности информации
+	+	управление информационными системами и компьютерными сетями с точки зрения безопасности информации
+	+	определение в виде процедур поведения 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 следующих целей организации:

- убеждение в том, что руководство поддерживает и управляет безопасностью информации, согласно бизнес-требованиям и соответствующим постановлениям закона и внутренними регуляторами,
- управление безопасностью информации внутри организации,

- удержание безопасности информации, являющейся собственностью организации, которой управляют третьи лица,

- достижение и удержание соответствующего уровня защиты активов организации,

- убеждение, что сотрудники, исполнители и потребители, представляющие третью сторону понимают свои обязанности, осознают угрозу и другие аспекты безопасности информации,

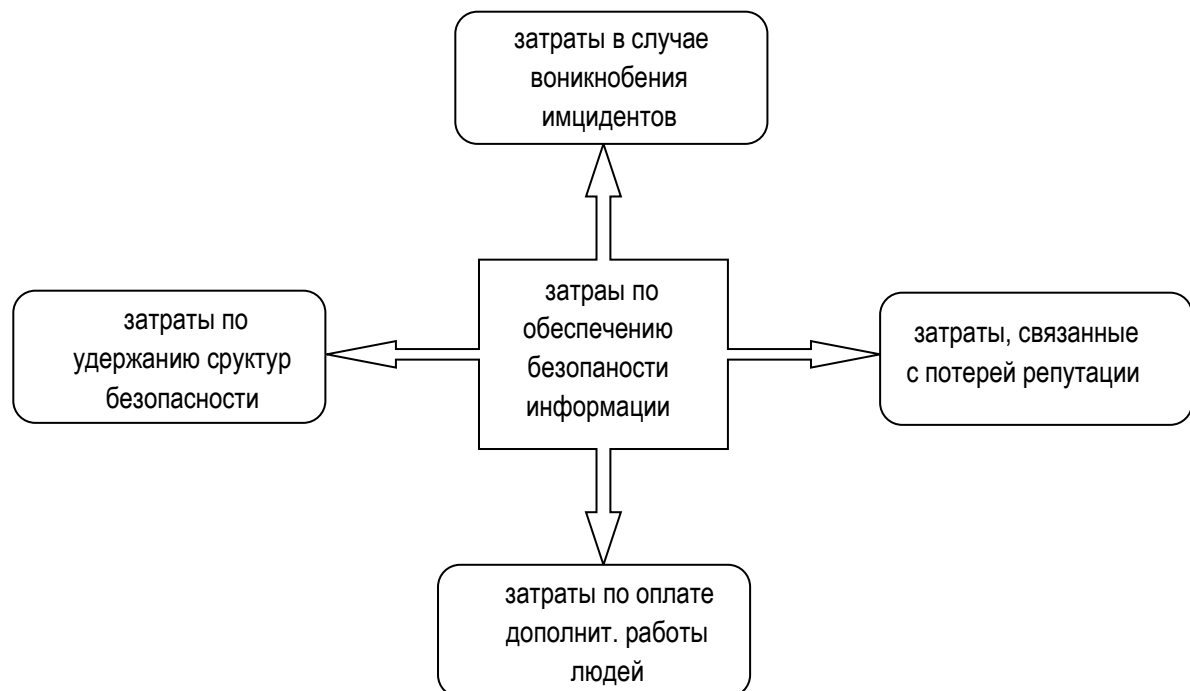


Рис. 2. Виды расходов, возникшие в результате отсутствия СИБИ.
ПО: Собств. Разработка.

- обеспечение защиты перед несанкционированным физическим доступом,
- повреждением или препятствиями по месту нахождения организации и по отношению к организации,
- обеспечение правильной и безопасной эксплуатации информационных систем и оборудования,
- обеспечение контроля за доступом к информации, к информационным 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 безопасности организации¹⁵.
 - Цели, описанные 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, соответствующую требованиям закона. Она позволяет 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. Обеспечивает 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 реализации „процессуального подхода”, связанного с применением в организации системы процессов, совместно с их идентификацией и интеракцией.

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/TIT/2007/3-4/3>.
6. Mikolaj J., *Rizikovy manazment*, RVS FSI ZU, Žylyna 2001.
7. Pivowarski 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.

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

AUTHORS

Доктор Юлиус Пивоваркий - ректор Школы общественной и индивидуальной безопасности "Apeiron" в Кракове, научные специальности: философия безопасности, член Международной боевые искусства 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 безопасностью 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 индивидуальной "Apeiron".
