|  |
| --- |
| **УДК 004.056.5** |
|  | **E.A. Шумаева,** *канд. наук гос. упр., доц.***Г.С. Джура** *ГОУВПО «Донецкий национальный технический университет»,* *Донецк, Донецкая Народная Республика****E.A. Shumaieva,G.S. Dzhura****Donetsk national technical university,**Donetsk, Donetsk People's Republic* |
|  |
| ОЦЕНКА УРОВНЯ КИБЕРБЕЗОПАСНОСТИ ОРГАНИЗАЦИИ ПРИ ФОРМИРОВАНИИ БЮДЖЕТА НА СИСТЕМУ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ |
|  |
| **ASSESSMENT OF THE ORGANIZATION'S CYBERSECURITY LEVEL WHEN FORMING A BUDGET FOR AN INFORMATION SECURITY SYSTEM** |

*Аннотация. Крайне важным, а в некоторых случаях и ключевым аспектом формирования эффективной системы обеспечения информационной безопасности организации является формирование бюджета на ее создание, поддержку и модернизацию. При формировании бюджета управленец всегда должен видеть объективную ситуацию и наиболее четко оценивать все возможные риски при принятии решения. Для этого необходим четкий, понятный и объективно отражающий реальность язык общения между высшим руководством и специалистами, занимающимися информационной безопасностью.*

*Ключевые слова: оценка уровня кибербезопасности, безопасность информации, система обеспечения информационной безопасности, бюджет.*

*Abstract. An extremely important, and in some cases a key aspect of the formation of an effective information security system of an organization is the formation of a budget for its creation, support and modernization. When forming a budget, the Manager should always see an objective situation and most clearly assess all possible risks when deciding. This requires a clear, understandable and objectively reflecting reality language of communication between senior management and specialists engaged in information security.*

*Keywords: assessment of the level of cybersecurity, information security, information security system, budget.*

**Постановка проблемы**. Реальность такова, что сложностей при обосновании бюджетирования сферы обеспечения информационной безопасности для руководителей (особенно на постсоветском пространстве), не смотря на все существующие тенденции, обосновывающие критичность сферы для бизнеса и государства, крайне много. Сегодня информационная безопасность (далее – ИБ) остается больше искусством, чем наукой.

**Анализ предыдущих исследований и публикаций.** Изучению опыта формирования бюджета на систему информационной безопасности посвящены научные труды многих российских и зарубежных ученых и институтов, в частности Дарбишева П. [1], Пискунов И. [2], А. Бирюков [3], в частности утверждает, что сегодня необходимо научиться оперировать рыночными категориями, экономически обосновывать расходы на ИТ-безопасность.

**Цель исследования**. Целью исследования является анализ практик, тенденций и методологий формирования бюджета на обеспечение информационной безопасности.

**Основные результаты исследования**. Существует масса практик по качественному оцениванию улучшений, в том числе в сфере инвестирования в ИБ, однако истина заключается в том, что даже приближенно точная оценка кибербезопасности остается недостижимой задачей при том, что на сегодняшний день согласованной и признанной экспертным сообществом системы измерений, которая хотя бы в первом приближении напоминала, к примеру, бухгалтерские принципы не существует. Исходя из этого можно сделать вывод, что с учетом необходимости формирования кибербезопасности с релевантно определенным распределением ресурсов и оценкой рисков, необходима система показателей, которая:

1. Максимально объективна.
2. Может быть количественно определена.
3. Соизмерима и совместима (интероперабельна) с различными подходами и системами.
4. Может быть использована лицами, принимающими решения в условиях распределения ограниченных средств.
5. Согласовано и одобрено в максимально возможном объеме в рамках соответствующих экспертных сообществ.

Стоит отметить, что современные частные и государственные организации в основном используют качественные, а не количественные показатели эффективности состояния ИБ. С учетом масштаба, комплексности и сложности формирования такой системы оценивания в современных условиях, необходим поэтапный подход.

Проводя исследование передовых методов формирования представления об уровне безопасности организаций, было определено что можно выделить 3 основных тенденции:

1 – существует строгое разделение между методами, которые формируются на предварительной основе и теми, которые применяются постфактум. Другими словами, некоторые методики измерения оценивают перспективы применения мер безопасности с тем, чтобы оценить, как изменения в области безопасности скажется на предприятии. Другие состоят в ретроспективном взгляде на уровень безопасности после того, как мера была реализована, а затем либо измеряется положительное влияние или, в некоторых случаях, ущерб, который был нанесен стоимостная оценка этого ущерба.

2 – некоторые меры оценивают безопасность исключительно как процесс создания стоимости интегрированных систем безопасности и чек-листов из факторов, которые, как считается, повышают безопасность и измерение показателей соответствия этим показателям. В таком случае гораздо меньше усилий направлено на обеспечение безопасности напрямую. Фактор безопасности достигается через внедрение нового дополнения к системе безопасности предприятия, которое увеличивает вероятность противодействия вторжению или иной угрозе.

3 – пока некоторые из мер ориентированы исключительно на показатели, некоторые направлены вместо этого на «гибкость» системы. Иными словами, по крайней мере один показатель количественной оценки кибербезопасности должен быть направлен не на то, сколько угроз было нейтрализовано или предупреждено, а на то, как быстро была восстановлена система. Если предприятие определяет минимальный перечень критериев для оценки, то наиболее фундаментальным и критичным фактором является именно этот. Таким образом, на каком-то уровне, необходимо будет определиться, является ли «превентивность» или «гибкость» системы более превалирующим критерием обеспечения безопасности.

Используя сформированную конструкцию, были определены и классифицированы несколько различных методов, использующихся в настоящее время для количественной оценки кибербезопасности. Данные методы были систематизированы в следующие группы:

1. **Методологии и системы показателей.** В основном сосредоточены на измерении соответствия некоторых базовых наборов лучших практик. Некоторые работают на перспективной основе, другие на ретроспективной.
2. **Страховые метрики.** Являются относительно уникальным подмножеством многих других, используемых в качестве моделей в рамках страховой отрасли с целью количественной оценки риска и установки страховых взносов. Как таковые, они включают в себя аспекты других систем измерения и широко варьируются.
3. **ROI/ROSI (возврат инвестиций) [4].** Данные методы основаны на традиционных бизнес-моделях измерения возврата инвестиций для предприятия. С момента улучшения безопасности трудно определить количественно, некоторые системы окупаемости могут быть изменены для измерения «возврата от инвестиций в безопасность». Почти все эти модели носят предполагаемый и предиктивный характер.
4. **Киберпреступность.** Альтернативный метод измерения снижения риска, заключающийся в попытке измерить его напрямую путем предварительного сбора ущерба и со временем измерения сокращения в этой метрике. Большинство усилий такого рода связанные с кибербезопасностью и получены от метрики измеряющей потери от киберпреступности.
5. **CYRIE.** Проект «Экономика киберрисков» поддерживает исследования в области экономики киберугроз и информационной безопасности с особым акцентом на измерение и оценку воздействия инвестиций в обеспечение безопасности на вероятность возникновения риска и эффективность средств управления безопасностью.
6. **Другие.** Также существует масса иных измерительных систем, которые не попадают не в одну легко определяемую категорию.

В связи с тем, что сложно точно оценить киберриски в понятном количественном выражении, многие компании полагаются на отраслевые стандарты, с которыми можно сравнивать состояние своих показателей. Компании могут создавать собственные списки показателей или передавать их формирование на «аутсорсинг».

Методологии и списки показателей несмотря на приносящую пользу могут использоваться не верно. По своему характеру методологии носят широкий характер и могут не всегда способствовать выбору организациями конкретных инвестиций в обеспечение безопасности. Эмпирические исследования эффективности интегрированных систем и списков показателей носят ограниченный характер, поскольку широкое распространение получили недавно. Не правильно применяемые методологии и критерии могут предоставить компаниям ложное чувство безопасности, так как менеджеры считают себя более защищенными, чем на самом деле.

Потребность в соответствии с набором заранее определенных критериев может также нанести ущерб безопасности и производительности компании, если будут установят новые программы безопасности без удаления старых. Однако, не смотря на все вышеперечисленное, вариант использования лучших стандартизированных практик, разрабатываемых ведущими институтами, остается краеугольным как при формировании системы обеспечения информационной безопасности (СОИБ) в целом, так и при формировании бюджета на СОИБ, в частности.

В таблице 1 приведен список наиболее распространенных методологий и списков показателей в сфере ИБ.

Таблица 1

Наиболее распространенные методологии и списки показателей в сфере ИБ

|  |  |
| --- | --- |
| **Методологии, стандарты, разработчики** | **Описание** |
| **1** | **2** |
| NIST (National Institute of Standards and Technology) [5] | Созданный в 2014 году во исполнение указа 13636, Национальный институт стандартов и технологий (NIST) создал одну из наиболее известных и широко принятых интегрированных систем. Данный подход разбивает процесс доступа к кибернетическим мощностям и потребностям компании на пять основных шагов (выявление, защита, обнаружение, реагирование и восстановление), но отмечается, что каждой организацией нужно будет применять интегрированную систему различными способами, чтобы наилучшим образом обслуживать свои собственные уникальные потребности. |
| ISO (International Organization for Standardization) [6] | Семейство стандартов ISO/IEC 270000 было разработано совместно Международной организацией по стандартизации (ISO) и Международной электротехнической комиссией (IEC) для оказания организациям помощи в защите конфиденциальной информации путем управления рисками, создаваемыми людьми, процессами и ИТ-системами. Организации также могут выбрать проверку и сертификацию в соответствии с этими стандартами для подтверждения соответствия. |
| FAIR (The Factor Analysis of Information Risk, FAIR Institute) [7] | Модель факторного анализа информационных рисков (FAIR) отличается от других интегрированных систем тем, что она представляет собой аналитическую модель риска, а не модель зрелости потенциала или контрольный перечень элементов управления. Соответственно, вместо предоставления организации рейтинга или списка передовых практик, модель FAIR предназначена для получения «финансовых результатов». Доступные инструменты FAIR включают вышеупомянутую книгу и онлайн-программу обучения, известную как FAIR-U. |
| COBIT (Control Objectives for Information and Related Technologies, ISACA) [8] | Контрольные цели для информационных и смежных технологий (COBIT) были разработаны Ассоциацией информационных систем и контроля (ISACA) в 1996 году. COBIT 5 был выпущен в 2012 году; последнее обновление, COBIT 2019, вышло в декабре 2018 года и было обновлено с тем, чтобы включить новые технологии и системы для лучшего соответствия нынешним глобальным стандартам и включения модели с открытым исходным кодом, с целью обеспечения постоянной обратной связи и обновлений. |
| Продолжение табл.1 |
| **1** | **2** |
| CIS (Center for Information Security) [9] | Центр информационной безопасности предлагает свои средства контроля CIS и контрольные показатели CIS в качестве инструментов для измерения безопасности организации. CIS Controls — это список из двадцати средств управления организацией, которые можно использовать для лучшей защиты от кибератак. CIS Controls предоставляют собой всеобъемлющие методологии, адаптированные к целевой системе. Эти критерии разработаны благодаря волонтерским усилиям различных специалистов по информационной безопасности. |
| GSA (Global Cyber Alliance) [10] | Инструментарий GCA нацелен на малые и средние предприятия и предназначен для использования (CIS Control – п. 5), создан, чтобы дать возможность снизить распространенные киберриски. CIS Control – это рекомендуемый набор действий, созданный и постоянно обновляемый с использованием текущей информации об угрозах и экспертных рекомендаций для предотвращения и/или сокращения наиболее распространенных кибератак. |
| TC CYBER (European Telecommunications Standards Institute) [11] | Технический комитет по кибербезопасности ETSI (известный как TC CYBER) был создан в 2014 году, с целью фокусирования на обеспечении международных стандартов, в частности в Европе. Данная серия стандартов охватывают безопасность целого ряда объектов инфраструктуры, устройств и услуг; комитет также включает подгруппу, в которой особое внимание уделяется рискам, создаваемым квантовыми компьютерами для криптографии. |
| ISF (Information Security Forum) Standard of Good Practice for Information Security [12] | С 1990-х годов Форум информационной безопасности (ISF) публикует список информации рекомендации по безопасности, которые они обновляют каждые два года. Издание 2018 года обсуждает стандарты, установленные ISO/ IEC 27002: 2013, NIST Cybersecurity Framework, CIS Top 20, PCI DSS и COBIT 5. |
| SWIFT Customer Security Control Framework (SWIFT publishes cybersecurity counterparty risk guide, SWIFT, 2019) [13] | Система контроля безопасности клиентов (CSCF) SWIFT «устанавливает основу безопасности обязательных и консультативных мер контроля для всего сообщества пользователей, в отношении которых пользователи SWIFT обязаны ежегодно подтверждать свое соответствие». SWIFT недавно выпустила руководство «Оценка рисков кибербезопасности контрагента» на основе интегрированной системы. Оценка риска контрагента является особенно важной проблемой, учитывая, что многие компании могут использовать у себя различные стандарты и средства контроля для своей кибербезопасности. Таким образом, риск контрагента увеличивается с увеличением числа внешних партнерств). |
| BSA software framework (The Software Alliance) [14]  | Программная методология BSA — это попытка оценить безопасность программного обеспечения на протяжении всего жизненного цикла программного обеспечения. Он особенно новаторский в том смысле, что он пытается определить желаемое конечное состояние для проблем безопасности жизненного цикла программного обеспечения таким образом, чтобы можно было проводить экспресс-измерения. |
| Продолжение табл.1 |
| **1** | **2** |
| American Public Power Association [15] | На основе модели зрелости потенциала кибербезопасности субсектора энергетики Департамента энергетики — это онлайновый инструмент самооценки, предназначенный для коммунальных служб, чтобы «оценивать киберриски, планировать улучшения, определять приоритеты инвестиций и оценивать их положение в области безопасности». |

**Выводы.** Стоит отметить, что не смотря на все преимущества, стандартизированные методологии могут стимулировать предприятие к чрезмерному инвестированию в кибербезопасность - вполне могут возникнуть некоторые киберриски, которые крайне маловероятны, или наоборот, которые приведут к таким небольшим потерям, что для компании будет нерентабельно защищать от них.

Методологии и списки показателей могут служить хорошим индикатором уязвимостей для менеджеров и владельцев организации, которые обеспокоены отсутствием средств управления кибербезопасностью. Особенно для малых и средних предприятий, список показателей может стать простым способом быстрого повышения уровня кибербезопасности путем определения наиболее уязвимых областей. Однако подходить в формирование бюджета при распределении средств на информационную безопасность необходимо гибко, предварительно оценив все риски, и имея глубокое представление как о современном состоянии дел, так и о всех процессах и аспектах функционирования организации.

|  |
| --- |
|  |
| **Список литературы** |
|  | Дарбишева П. Формирование бюджета на обеспечение информационной безопасности предприятия / Дарбишева П. // Научно-практическая конференция «Прикладные научные исследования и экспериментальные разработки, основанные на результатах фундаментальных и поисковых исследований» – 2016. – С. 46-49.  |
|  | Пискунов И. Планирование затрат на информационную безопасность. [Электронный ресурс] / И. Пискунов – Режим доступа: [https://www.anti-malware.ru/analytics/ Technology\_Analysis/economic\_planning](https://www.anti-malware.ru/analytics/%20Technology_Analysis/economic_planning). |
|  | Бирюков А. Окупаемость ИБ-систем. Какую прибыль может принести система ИБ / А. Бирюков – Режим доступа: <http://samag.ru/blog/art/No_number/16>. |
|  | Индекс глобальной конкурентоспособности [Электронный ресурс]. – Режим доступа: <https://www.csoonline.com/article/3229887/how-to-calculate-your-return-on-security-investments.html>. |
|  | Мэтью П. Барретт, Концепция улучшения кибербезопасности критической инфраструктуры 1.1, Национальный институт стандартов и технологий (NIST), 16 апреля 2018 г. – Режим доступа: [https://nvlpubs.nist.gov/nistpubs/CSWP/ NIST.CSWP.04162018.pdf](https://nvlpubs.nist.gov/nistpubs/CSWP/%20NIST.CSWP.04162018.pdf). |
|  | «ISO/IEC 27000 family - Information security management systems» International Organization for Standardization, 2018 – Режим доступа: <https://www.iso.org/isoiec-27001-information-security.html>. |
|  | Джек Фрейнд и Джек Джонс, Измерение и управление информационным риском: подход FAIR (Баттерворт-Хайнеманн, 2014 г.) – Режим доступа: <https://www.fairinstitute.org/fair-book>. |
|  | Обзор стандарта COBIT (Control Objectives for Information and related Technology) v. 4.1. – Режим доступа: <https://www.itexpert.ru/rus/biblio/cobit/>.  |
|  | «Cybersecurity Tools» Center for Information Security, 2019 – Режим доступа: <https://www.cisecurity.org/cybersecurity-tools/>.  |
|  | GCA Cybersecurity Toolkit for Small Business,” Global Cyber Alliance, 2019 – Режим доступа: <https://gcatoolkit.org/smallbusiness/>. |
|  | «Cyber security» European Telecommunications Standards Institute, 2019 – Режим доступа: <https://www.etsi.org/technologies/cyber-security>. |
|  | The ISF Standard of Good Practice for Information Security 2018, Information Security Forum, 2018 – Режим доступа: <https://www.securityforum.org/tool/the-isf-standard-good-practice-information-security-2018/>.  |
|  | «SWIFT publishes cybersecurity counterparty risk guide» SWIFT, 2019 – Режим доступа: <https://www.swift.com/news-events/news/swift-publishes-cybersecurity-counterparty-risk-guide>.  |
|  | «BSA Framework for Secure Software» BSA, 2019 – Режим доступа: <https://www.bsa.org/reports/bsa-framework-for-secure-software>.  |
|  | «Cybersecurity Scorecard» American Public Power Association, 2019.<https://www.publicpower.org/resource/cybersecurity-scorecard>.  |