

С.П. Серёдкин¹¹ Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация**НАУЧНЫЕ ПОДХОДЫ К ОБОСНОВАНИЮ ИНВЕСТИЦИЙ В ЗАЩИТУ ИНФОРМАЦИИ**

Аннотация. В статье представлены практические рекомендации и механизм обоснования инвестиций на защиту информации для предприятий бизнеса. Проанализирован научный и практический подход к данной проблеме, приведены основные экономические методы обоснования инвестиций. Предложена методика обоснования инвестиций в защиту информации, основанная на оценке и вероятности реализации угроз информационной безопасности и совокупной стоимости затрат на ликвидацию последствий реализации угроз.

Ключевые слова: защита информации, стоимость информационных активов, инвестиции, затраты, риски, негативные последствия.

S.P. Seryodkin¹¹ Irkutsk State Transport University, Irkutsk, Russian Federation**APPROACHES TO THE JUSTIFICATION OF INVESTMENTS IN INFORMATION SECURITY**

Abstract. The article presents practical recommendations and a mechanism for justifying investment in information security for business enterprises. The scientific and practical approach to this problem is analyzed, the main economic methods of investment justification are given. A methodology for justifying investments in information security is proposed, based on the assessment and probability of the implementation of threats to information security and the total cost of costs for eliminating the consequences of the implementation of threats.

Keywords: information security, the cost of information assets, investments, costs, risks, negative consequences.

Введение. Сегодня в результате развития экономических и информационных сфер предприятий, расширения масштаба удаленного доступа сотрудников вопрос защиты информационных активов является наиболее актуальным. В условиях непростой экономической ситуации, когда перед организациями стоит задача развития и интеграции бизнеса, в условиях жёсткой конкурентности и возрастающего числа угроз, задача защиты информации (ЗИ) для обеспечения функционирования бизнес-процессов является наиболее актуальной.

Для подтверждения факта актуальности задачи обеспечения безопасности информационных активов воспользуемся данными результатов мониторинга сетевого трафика, проведенного компанией Positive Technologies, по приведенным данным количество атак в 2020 г. на протоколы для удаленного доступа выросло более чем в три раза [1].

Анализ этих данных не оставляет сомнений в необходимости вложений в обеспечение информационной безопасности (ИБ) предприятий бизнеса. Основной вопрос современного бизнеса – как оценить необходимый уровень вложений в ИБ для обеспечения максимальной эффективности инвестиций в данную сферу.

Целью исследования является разработка методики обоснования инвестиций в информационную безопасность. Для достижения данной цели необходимо последовательно решить следующие задачи:

1. Проанализировать современные подходы к оценке инвестиций;
2. Представить метод оценки стоимости информационных активов в денежном эквиваленте;
3. Предложить методику обоснования инвестиций.

Отсутствие обоснованных и общепринятых методов оценки эффективности инвестиций в организацию системы защиты информации зачастую создает противоречивую ситуацию. С одной стороны, ожидаемые результаты от инвестиций в денежном эквиваленте являются фактическими затратами, которые в ходе реализации планов развития бизнеса могут не совпадать по позиции с задачами оптимизации расходов, и как следствие сдерживают инвестиционные возможности компании.

К сожалению, до настоящего времени для оценки обоснования инвестиций в ЗИ применяются общепринятые в экономическом аспекте методики, которые не отражают реальную ситуацию и не могут быть объективными именно для целей защиты информационных активов от угроз.

Данная проблематика широко представлена в публикациях Петренко С.А., Бабенко А. А., Чачиной Е.Б., Курского В. А., Хомякова К.Г., Каницкой Л.В., Горбачева С, Руткаускаса Т.К. Авторами предлагаются подходы и методики по проблеме инвестиций, а также оценки эффективности вложений в защиту информации.

Практически большинство расчетов инвестиций основаны на общепринятых в экономической сфере методиках, рассмотрим некоторые из них:

1. ROI (от англ. *return on investment*) — финансовый коэффициент, показывающий уровень доходности или убыточности бизнеса, учитывая сумму сделанных в этот бизнес-инвестиций, процентное отношение прибыли (или экономического эффекта) от проекта к инвестициям:

$$ROI = \frac{E_1 - H}{(C_2 - C_1)/2},$$

где ROI – рентабельность инвестиций, $(E_1 - H)$ – показатель прибыли за вычетом налогов, H – величина ставки налогооблагаемой прибыли, C_1 – стоимость всех активов на начало периода, C_2 – стоимость всех активов на конец периода.

Преимущества:

- рассматривается одновременно группа взаимосвязанных механизмов безопасности, которые поддерживают и дополняют друг друга, обеспечивая максимальный эффект;
- прост для понимания и включает несложные вычисления.

Недостатком метода является тот факт, что при расчете показателя возможно применение различных подходов, это затрудняет или сводит на нет попытку сопоставить данные, полученные из различных источников.

2. TCO (Total cost of ownership) или совокупная стоимость владения — общие расходы, которые возникают у компании из-за владения каким-либо активом, например, ИТ-инфраструктурой [3].

$$TCO = A_1 + A_2,$$

где A_1 – затраты на приобретение и внедрение (первоначальные затраты), A_2 – эксплуатационные затраты.

Преимущества:

- позволяет получить выводы о целесообразности реализации проекта в области информационной безопасности на основании оценки только затрат;
- предполагает оценку не только первоначальных затрат на создание системы ЗИ, но и тех затрат, которые могут иметь место на различных этапах всего жизненного цикла системы.

Недостатки:

- компании вынуждены более тщательно подходить к анализу и исчислению затрат;
- необходимо более глубокое понимание затрат, а именно их динамики и поведения в адаптации к видам деятельности;
- не учитывает риски и не соотносит технологию со стратегическими целями развития бизнеса и решением задачи повышения конкурентоспособности.

3. NPV (Net present value) или чистая приведенная стоимость – стоимость, которая показывает инвестору доход/убыток от инвестирования денежных средств в инвестиционный проект. Полученный доход можно сравнить с доходом в менее рискованный вид активов и рассчитать эффективность и целесообразность вложения в инвестиционный проект. Если NPV больше 0, то проект эффективен. После этого можно сравнить значение NPV с доходов от вклада в банк. Если $NPV > 0$ вклад в наименее рискованный проект, то инвестиции целесообразны.

$$NPV = \sum_{t=1}^n \frac{CF_t}{(1+r)^t} - \sum_{t=0}^n \frac{I_t}{(1+r)^t},$$

где CF_t – денежный поток, I_t – сумма инвестиционных вложений в проект в t -ом периоде, r – ставка дисконтирования.

Преимущества:

- позволяет менеджерам более «полно» оценить отдачу от проекта и не предполагает введения ограничений по сроку жизни проекта;
- практически применим для обоснования принятия одного проекта;
- наиболее корректный измеритель эффективности инвестиций.

Недостатки:

- недостаточная гибкость (метод расчета подразумевает принятие единственного решения в самом начале пути на основе прогнозных данных);
- не предполагает анализа рисков, поэтому после получения положительного значения NPV обязательна процедура анализа рисков проекта [2].

Оценка стоимости информационных активов с выражением в денежном эквиваленте ALE (Annualised Loss Expectancy) или метод ожидаемых потерь. Этот метод основан на том, что рассчитываются потери от нарушений политики безопасности, с которыми может столкнуться компания, данные потери сравниваются с инвестициями в защиту информации, направленными на предотвращение нарушений. Метод ожидаемых потерь основан на эмпирическом опыте [2].

Например, нарушения безопасности организаций приводят к следующим финансовым потерям:

- при ведении электронного документооборота потери, связанные с простоем и выходом из строя сетевого оборудования;
- нанесение ущерба репутации компании;
- оплата сверхурочной работы ИТ-персонала и/или оплата работ подрядчикам, занимающимся восстановлением информационной системы;
- оплата услуг внешних консультантов, которые решали вопросы по восстановлению данных, выполняли ремонт и оказывали юридическую помощь;
- оплата ремонта повреждений от виртуальных атак;
- судебные издержки при виртуальных преступлениях и нарушениях политики безопасности.

Чтобы снизить ожидаемый ущерб, компания должна инвестировать средства в системы безопасности: программное обеспечение и технические средства.

Если организация принимает решение по установке системы ИБ, то ее стоимость будет состоять из следующего:

- **Единовременные затраты.** Это стоимость оборудования и затраты на внедрение систем защиты информации;
- **Периодические затраты.** Здесь имеют место такие параметры, как техническая поддержка и сопровождение, заработная плата персонала, продление лицензий на ПО.

Чтобы определить эффект от внедрения системы ИБ, нужно подсчитать показатель ожидаемых потерь (ALE). По оценкам экспертов, грамотно установленная и настроенная система защиты дает 85% эффективности в предупреждении или уменьшении потерь от

нарушений политики безопасности. Следовательно, финансовая выгода создается ежегодными сбережениями, которые получает компания при внедрении системы ИБ.

$$AS = ALE \times E - AC,$$

где AS (*Annular Saving*) – ежегодные сбережения, ALE (*Annualised Loss Expectancy*) – показатель ожидаемых потерь, E – эффективность системы защиты, обычно составляющая около 85%, AC (*Annual Cost*) – ежегодные затраты на безопасность.

Методика обоснования инвестиций в защиту информации. Имеющиеся методики подсчета инвестиций при создании системы информационной безопасности не могут быть убедительными для руководства компаний в силу их малой связи с целями экономической, хозяйственной и финансовой деятельности предприятий, поэтому не охотно принимаются руководителями компаний.

Используемые финансовые инструменты для оценки экономической эффективности финансовых вложений также практически не могут быть использованы при оценке необходимого объема инвестиций

Обеспечение необходимого уровня защиты информации предприятия в современных условиях является специфическим и не простым процессом, который подвержен воздействию важных факторов.

Какие факторы могут побудить руководителей бизнеса на инвестиции? На мой взгляд, в настоящее время таких причин всего несколько: это тревога, требования бизнеса и регулятора.

Тревога, страх- подтвержденные факты крупнейших успешных кибератак на мировые бизнес-системы и, как следствие, снижение темпов роста прибыли, а в иных случаях и потеря бизнеса.

Требование бизнеса – это интеграция в бизнес-среду и стратегическое развитие.

Невыполнение требований регуляторов влечет за собой штрафы, пристальное внимание со стороны государства, а также неизбежные репутационные риски.

При осуществлении бизнес-планирования деятельности предприятия расходы на реализацию мероприятий по ЗИ обычно рассматривают как затраты. Затраты – это, в первую очередь, «производственная необходимость», смысл которых всегда остается постоянным, т.е. это те расходы, которые в итоге снижают полученную прибыль. Поэтому отношение руководства и финансово-экономических служб предприятий к данному вопросу зачастую всегда отрицательное. Как изменить данное отношение? Какую методику предложить для убедительности обоснования необходимых инвестиций?

Предложенная методика обоснования инвестиций в защиту информации основана на оценке и вероятности реализации угроз ИБ и совокупной стоимости затрат по ликвидации последствий реализации угрозы.

Оценка угроз информационной безопасности.

Этапы моделирования угроз информационной безопасности представлены на рис. 1.

В ходе оценки угроз безопасности информации должны быть определены негативные последствия, которые могут наступить от реализации (возникновения) угроз безопасности информации [4].

ЭТАПЫ МОДЕЛИРОВАНИЯ УГРОЗ

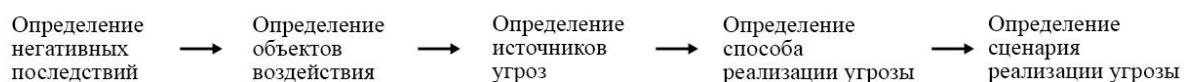


Рис. 1. Этапы моделирования угроз информационной безопасности

В ходе оценки угроз безопасности информации должны быть определены информационные ресурсы и компоненты систем и сетей, несанкционированный доступ к которым или воздействие на которые в ходе реализации (возникновения) угроз безопасности информации может привести к негативным последствиям – объекты воздействия (рис. 2).

ОПРЕДЕЛЕНИЕ ОБЪЕКТОВ ВОЗДЕЙСТВИЯ

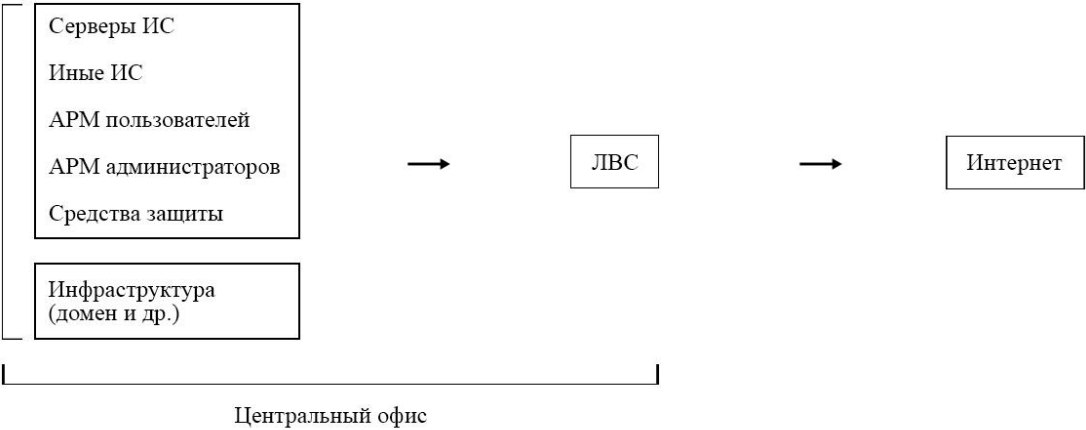


Рис. 2. Определение объектов воздействия

По результатам определения источников угроз безопасности информации должны быть определены:

- Виды актуальных нарушителей и возможные цели реализации ими угроз безопасности информации, а также их возможности;
- Категории актуальных нарушителей, которые могут реализовывать угрозы безопасности информации, в том числе непреднамеренные угрозы.

В ходе оценки угроз безопасности информации должны быть определены возможные способы реализации (возникновения) угроз безопасности информации, за счет использования которых актуальными нарушителями могут быть реализованы угрозы безопасности информации в системах и сетях, актуальные способы реализации (возникновения) угроз безопасности информации, т.е. негативные последствия (рис. 3).

ОПРЕДЕЛЕНИЕ НЕГАТИВНЫХ ПОСЛЕДСТВИЙ

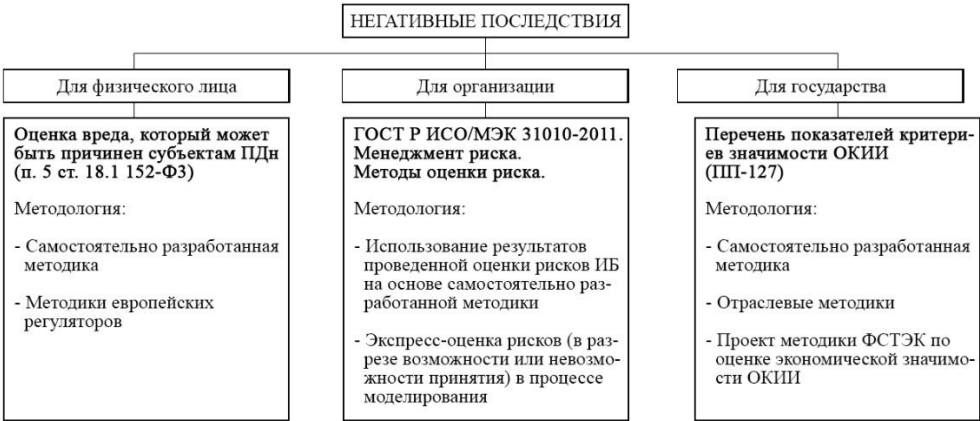


Рис. 3. Определение негативных последствий

Оценка вероятности реализации угрозы безопасности информации в ИС с учетом наличия уязвимостей и уровня их опасности представлены в табл. 1.

На основе анализа исходных данных, а также возможностей нарушителей определяются способы реализации (возникновения) угроз безопасности информации, актуальные для систем и сетей (рис. 4).

ОБЩАЯ СХЕМА ОЦЕНКИ УГРОЗ

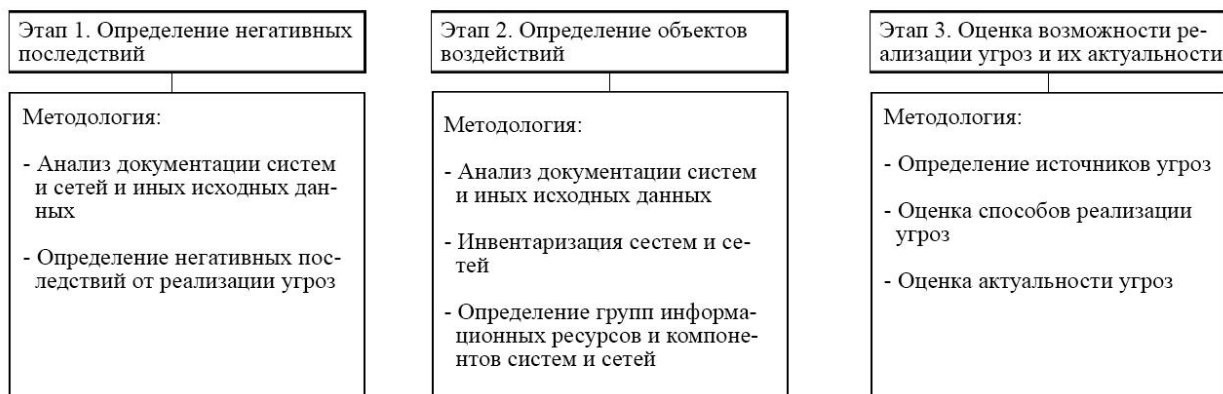


Рис. 4. Общая схема проведения оценки угроз

Выявленные актуальные угрозы на объекты воздействия (критичные информационные активы предприятия) и негативные последствия на них являются доказательным основанием для разработки плана защиты информационной системы (табл.2).

Таблица 1

Оценка вероятности реализации угрозы безопасности информации в ИС с учетом наличия уязвимостей и уровня их опасности

Вероятность реализации угрозы безопасности информации без учета уровня опасности уязвимости	Наличие и уровень опасности уязвимостей (по CVSS)				
	отсутствует	низкий	средний	высокий	критический
отсутствует	отсутствует	отсутствует	отсутствует	отсутствует	отсутствует
низкая	отсутствует	отсутствует	низкая	средняя	средняя
средняя	низкая	низкая	средняя	высокая	высокая
высокая	средняя	средняя	высокая	высокая	высокая

Таблица 2

Оценка актуальности сценария (пути) реализации угрозы безопасности информации в ИС

Вероятность реализации i -й угрозы j -м сценарием (P_{ij})	Степень возможного ущерба (X_i) от реализации i -й угрозы безопасности информации в ИС (в соответствии с таблицей 1)			
	отсутствует	низкая	средняя	высокая
отсутствует	неактуальный	неактуальный	неактуальный	неактуальный
низкая	неактуальный	неактуальный	неактуальный	актуальный
средняя	неактуальный	неактуальный	актуальный	актуальный
высокая	неактуальный	актуальный	актуальный	актуальный

Таким образом, общая последовательность моделирования угроз представляется в следующем виде:

- моделирование нарушителя безопасности информации в рассматриваемой ИС;
- построение множества всех возможных угроз для рассматриваемой ИС;
- построение модели атак для каждой угрозы с выявлением актуальных сценариев

- реализации угрозы для нарушителей с различным базовым потенциалом;
- формирование множества (перечня) актуальных угроз для рассматриваемой ИС [5].

Расчет совокупной стоимости затрат по ликвидации последствий реализации угроз.

Совокупная стоимость затрат. В рамках предложенной модели оцениваются следующие параметры стоимости затрат:

- ликвидации последствий реализации угрозы;
- упущенной выгоды;
- реализации мероприятий на обеспечение непрерывности и восстановления деятельности предприятия после сбоев (разработка плана, замена и ремонт оборудования, оплата специалистов, судебные издержки и др.);
- потери производительности (вынужденного простоя).

Оценка совокупной стоимости затрат M ликвидации последствий реализации угрозы и иных причин вывода из строя СЗИ производится по формуле:

$$M = \sum_{i=1}^m C_i,$$

где C_i – стоимость i -ой меры, m – общее число принятых мер.

Оценка суммарных выплат C_i -источников финансирования формируется по формуле:

$$C_i = \sum_{j=1}^n A_{i,j},$$

где C_i – суммарные выплаты j -ому источнику финансирования, $A_{i,j}$ – выплаты j -ому источнику финансирования, n – число источников финансирования.

Упущенная выгода рассчитывается по формуле:

$$V = R - D,$$

где V – упущенная выгода, R – доходы, которые могли бы быть получены в случае отсутствия нарушения права (потенциальные доходы), D – расходы, которые могли бы быть понесены при получении потенциального дохода (потенциальные расходы).

Реализация мероприятий по обеспечению непрерывности и восстановлению деятельности предприятия после сбоев. После того как были проанализированы требования к непрерывности, необходимо предложить и обосновать возможные технические и организационные решения. В процессе выбора решения необходимо детально рассмотреть возможные действия в отношении помещений, технологий, информационных активов, контрагентов, а также партнеров. Данные решения, как правило, выбираются с целью:

- защиты приоритетных видов деятельности компании;
- их эффективного восстановления;
- смягчения последствий инцидентов, разработки ответных и превентивных мер.

Выбор решения должен основываться на стоимости восстановления и стоимости простоя (рис. 5).

Стоимость восстановления рассчитывается на основе затратного метода и включается в план (рис. 6).

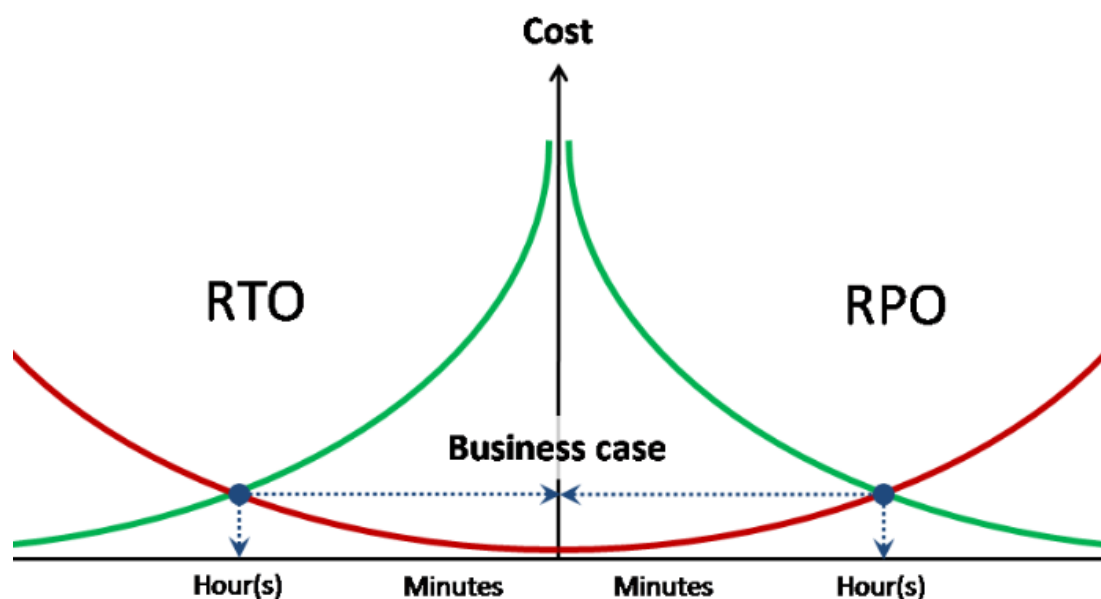


Рис. 5. Зависимость стоимости восстановления и стоимости простоя

Потери производительности труда  ▪ Количество сотрудников, затронутых простоем ▪ Продолжительность простоя ▪ Средняя ставка оплаты труда со всеми налогами ▪ Процент потери производительности во время простоя	Потеря дохода  ▪ Прямые потери ▪ Компенсационные выплаты ▪ Потери будущих доходов ▪ Инвестиционные потери
Финансовые показатели  ▪ Потерянные скидки ▪ Необходимость предоставлять обеспечение оплаты или поставки ▪ Снижение кредитного рейтинга ▪ Цена акций	 Стоимость простоя
Потери репутации и лояльности  ▪ Клиенты ▪ Поставщики ▪ Финансовые рынки ▪ Банки ▪ Деловые партнеры	Прочие расходы  ▪ Временные работники ▪ Аренда оборудования и площадей ▪ Затраты на сверхурочную работу ▪ Дополнительные расходы по доставке

Рис. 6. Потеря производительности (вынужденного простоя)

После того как будут оценены вышеперечисленные параметры, необходимо представить затраты на ЗИ как инвестиции в развитие предприятия. Главным аргументом может стать расчет необходимости реализации мероприятий по обеспечению непрерывности и восстановлению деятельности предприятия после сбоев, т.е. событий, которые могут произойти в результате воздействия кибератак на ИС.

Объем данных расходов и финансовых потерь можно представить как аргумент необходимого объема инвестирования в ЗИ, т.е. объем ущерба, который может получить предприятие, не реализова систему защиты информации.

Таким образом, необходимость инвестирования в систему организации ЗИ для современных компаний должна быть продиктована рядом целей:

- обеспечить организацию непрерывности бизнеса и его восстановления после сбоя;

- повысить конкурентоспособность путем совершенствования систем менеджмента;
- реализация эффективности IT системы;
- соответствие требованиям регуляторов к объектам критической информационной инфраструктуры, обработке персональных данных, сведений, составляющих конфиденциальную информацию.

Выводы. Обоснование необходимости инвестиций в защиту информации - это сложная и ответственная проблема, которая требует системности и научности в подходах. Предложенная методика позволяет с практической точки зрения подойти системно к вопросу обоснования инвестиций в защиту информации. Использование предложенного механизма позволяет более доступно аргументировать необходимость инвестиций, базируясь на оценке угроз и стоимости затрат на восстановление информационной системы предприятия. Есть надежда на то, что изложенные в статье идеи найдут понимание и применение в различных сферах бизнеса.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Сайт компании Positive Technologies [Электронный ресурс]. – Москва. – 2002 г. – Режим доступа : <https://www.ptsecurity.com>, свободный.
2. Петренко, С. А. Управление информационными рисками. Экономически оправданная безопасность / С. А. Петренко, С. В. Симонов – Москва.: ДМК Пресс, 2018. – 396 с.
3. Сайт региональной организации «Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления» [Электронный ресурс]. – Санкт-Петербург. – 1991 г. – Режим доступа : <http://spoisu.ru>, свободный.
4. Методика оценки угроз безопасности : методический документ / сост. ФСТЭК России. – Москва, 2021. – 83 с.
5. Дроботун, Е. Б. Построение модели угроз безопасности информации в автоматизированной системе управления критически важными объектами на основе сценариев действий нарушителя / Е. Б. Дроботун, О. В. Цветков – Тверь, 2016. – 9 с.

REFERENCES

1. Positive Technologies. Company website. Moscow, 2002. Access mode: <https://www.ptsecurity.com>.
2. Petrenko, S. A., & Simonov, S. V. Upravlenie informacionnymi riskami. Economicheskii opravdannaya bezopasnost. Moscow, DMK Press, 2018, 396 p.
3. Regionalnaya organizaciya «Sankt-Peterburgskoye obshestvo informatiki, vychislitel'noj tehnici, system cvyazi i upravleniya». Website. St. Petersburg, 1991. Access mode: <http://spoisu.ru>.
4. Metodika ocenki ugroz bezopasnosti. Methodological document. FSTEK Rossii. Moscow, 2021, 83 p.
5. Drobotun, E. B., & Cvetkov, O.B. Postroyenie modeli ugroz bezopasnosti informacii v avtomatizirovannoj sisteme upravleniya kriticheski vazhnymi objektami na osnove scenarijev dejstvij narushitelya. Tver, 2016, 9 p.

Информация об авторе

Серёдкин Сергей Петрович – к. э. н., доцент кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: sseryodkin2008@yandex.ru.

Author

Seryodkin Sergei Petrovich – Ph. D. in Economics, Associate Professor, the Subdepartment of Information systems and information security, Irkutsk State Transport University, Irkutsk, e-mail: sseryodkin2008@yandex.ru.

Для цитирования

Серёдкин С.П. Научные подходы к обоснованию инвестиций в защиту информации // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2021. – №3(11). – С. 67-76 – DOI: 10.26731/2658-3704.2021.3(11). 67-76 – Режим доступа: <http://ismm-irgups.ru/toma/311-2021>, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 01.09.2021)

For citations

Seryodkin S.P. Scientific approaches to the justification of investments in data security // Informacionnye tehnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami: ehlektronnyj nauchnyj zhurnal [Information technology and mathematical modeling in the management of complex systems: electronic scientific journal], 2021. No. 3(11). P. 67-76. DOI: 10.26731/2658-3704.2021.3(11). 67-76. [Accessed 01/09/21]