УДК 338.47:656+ 338.24.01

Обоснование оптимальных решений при создании систем информационной безопасности для интранет учебного заведения

С.Н. Горячев, А.А. Ананин, Н.М. Букалов
Профессор, д.т.н. В.А. Харитонов

Пермский национальный исследовательский политехнический университет, Пермь

В статье решается задача технико-экономического обоснования выбора оптимальной по соотношению затрат и уровня безопасности системы защиты информации для интранет учебного заведения, отличающаяся проблемой приведения возможных потерь от рисковых событий к качественной шкале.

Ключевые слова: оптимальная система защиты информации, потери от рисковых событий, рисковая шкала.

Введение

Интранет современных учебных заведений характеризуется достаточно сложной структурой (рис.1) и различием требований к информационной безопасности её элементов. Данное обстоятельство позволяет считать актуальной задачей комплексную оценку уровня информационной безопасности всего интранета в целом, решение которой позволило бы ранжировать по данному критерию различные варианты построения системы информационной безопасности и осуществлять обоснованный выбор наиболее предпочтительного из них, либо сформулировать техническое задание на разработку новой системы информационной безопасности с желаемой комплексной оценкой уровня информационной безопасности [1].

Для учебных заведений с ограниченным бюджетом особую роль играют стоимостные характеристики расходов на разработку и содержание системы информационной безопасности (защищенности интранет), которые должны быть сбалансированы с уровнем полезности этих систем, трудноприводимым к денежному выражению.

В докладе решается актуальная задача обоснования выбора оптимальной по соотношению затрат и уровня безопасности системы защиты информации для интранет учебного заведения, отличающаяся дополнительным проблемным обстоятельством, связанным с

невозможностью в условиях ВУЗа приведения возможных потерь от рисковых событий к денежному выражению.

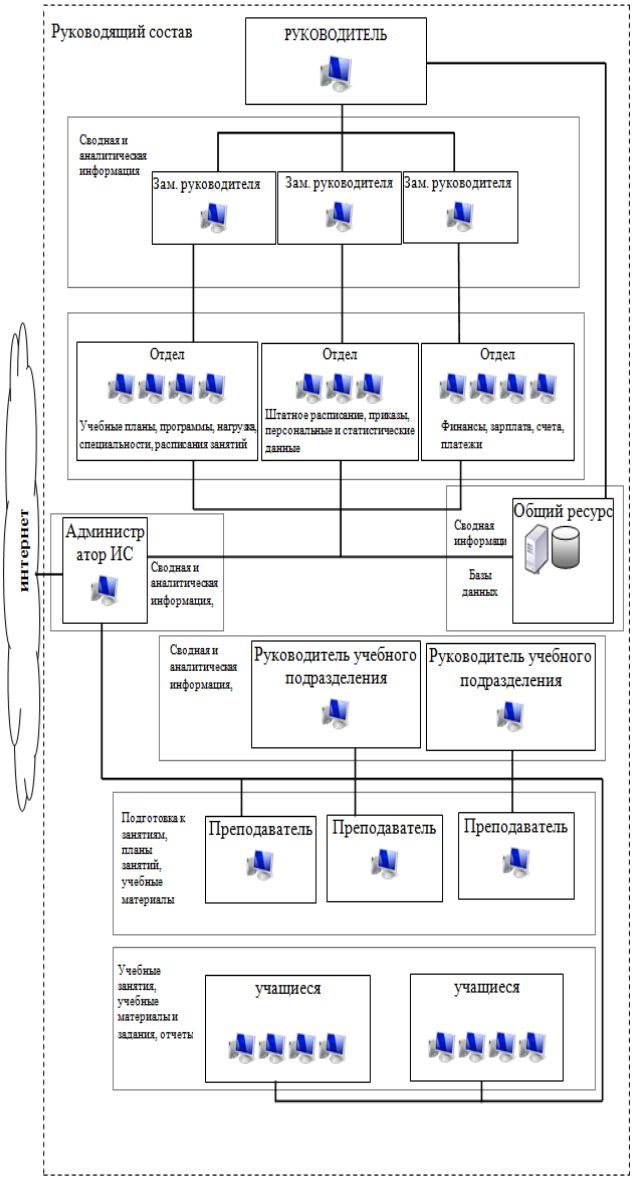

Рис. 1. Интранет современного учебного заведения

Для решения поставленной задачи предлагается использовать известный подход к определению уровня риска, учитывающий его двухаспектность: возможность и последствия рисковых событий.

1. Измерение уровня защищенности интранет

На первом этапе решения данной задачи составим агрегированный список пользователей интранет, различающихся требованиями к возможности (вероятности) возникновения угроз и ожидаемым потерям косвенно экономического характера.

Пусть для учебного заведения определен список: P1,C1 – сервер общего ресурса; P2,C2 – сервер администратора; P3,C3 – автоматизированные рабочие места руководящего состава; P4,C4 – сеть отделов и служб; P5,C5 – персональные компьютеры руководителей учебных подразделений (деканы и их заместители); P6,C6 – персональные компьютеры профессорско-преподавательского состава; P7,C7 – автоматизированные рабочие места учащихся, где, *Pi*, *Ci*, i=1÷7 – возможности (вероятности) возникновения угроз и ожидаемые потери косвенно экономического характера, соответственно.

На втором этапе определяются оценки возможности (вероятности) P^* возникновения угроз из документации на подсистему, либо устанавливаются экспертами подсистем. В любом случае, необходимо строить функции приведения характеристик P^* к стандартной шкале комплексного оценивания, например [1,4], то есть, в качественную форму X_P^* (рис. 2).

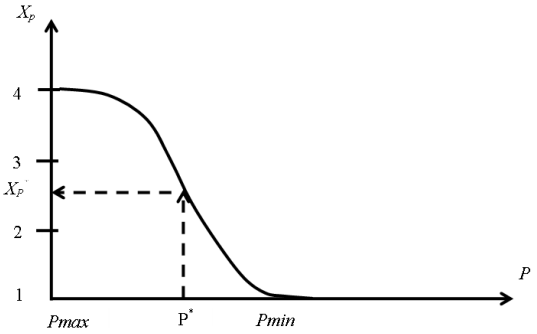

Рис. 2. Функция приведения оценок возможности возникновения угроз к стандартной шкале комплексного оценивания [1,4], P-вероятность рискового события, X_P-уровень вероятности рискового события

Сметным подходом определяются затраты $C(j)$, $j=1\div J$, связанные с установкой каждого варианта системы информационной защиты. Затем, аналогично рисунку 2, экспертно устанавливается функция приведения количественной величины расходов $C(j)$, необязательно материальных, к некоторой шкале этих расходов $X_C(j)$.

На следующем шаге по известной методике [2] оценивается уровень риска $R(j)$ интранет для множества $j=1\div J$ вариантов систем защиты информации, исходящими из линериазованной модели комплексного оценивания уровня риска интранет.

2. Решение задачи выбора оптимального варианта СЗИ

Для оценивания уровня привлекательности вариантов СЗИ R необходимо построить матричную свертку, входами которой является уровень расходов $X_C(j)$ и уровень риска $P(j)$.

Следует заметить, что оба аргумента свертки несут негативную информацию о вариантах СЗИ. Поэтому выбор варианта осуществляется по наименьшему значению свертки.

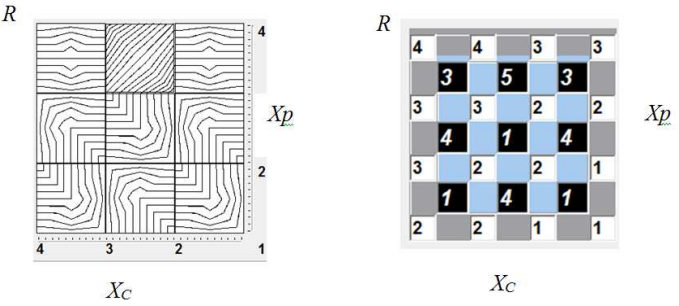

Рис. 4. Иллюстрация свертки уровней затрат X_C и риска Xp, связанных с выбором СЗИ интранет, в комплексную оценку P

Заключение.

Отсюда следует, что актуальная задача технико-экономического обоснования выбора оптимальной по соотношению затрат и уровня безопасности СЗИ для интранет учебного заведения решена.

Список литературы

1. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – ТИД Диа Софт, М., 2002.

2. Интеллектуальные технологии обоснования инновационных решений: монография / В.А. Харитонов и др.; под науч. ред. В.А. Харитонова. – Пермь: Изд-во Перм. гос. техн. ун-та, 2010. – 342 с.

Justification of optimum decisions at creation of information security systems for the intranet educational institution

S. N. Goryachev, A.A. Ananin, N. M. Bukalov, V.A. Haritonov

Perm national research polytechnic university, Perm

In article the problem of the feasibility study on a choice optimum on a ratio of expenses and level of safety of system of information security for the intranet educational institution, differing in a problem of reduction of possible losses from risk events to a qualitative scale is solved.

Keywords: optimum system of information security, loss from risk events, a risk scale.

References

1. Domarev V. V. *Bezopasnost' in formatsionnuch technologiy. Metodologiua sozdaniya system zashchsity* [Safety of Information Technologies. Methodology of Creation of Protection Systems]. Moscow, Dia Soft Publ., 2002.
2. VA. Kharitonov *Intellektuak'nye technologii obosnovanita innovatsionnychkh resheniy. Monografiya* [Intellectual Technologies of Justification of Innovative Solutions: Monograph], Perm, Perm Gos. Tecnh. Un.. 2010., 342 p.