Бондарь Ю.В., ст. препод.,
Степанова М.Н., канд. техн. наук, зав. лаб.,
Гревцев М.В., аспирант,
Павленко А.В., аспирант
Белгородский государственный технологический университет им. В.Г. Шухова

АНАЛИЗ РИСКОВ В ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЯХ*

zchs@intbel.ru

В статье проанализированы угрозы в отношении помещений высшего учебного заведения, угрозы безопасности людских ресурсов, угрозы информационным ресурсам, а также выделены модели нарушителя. Проведен анализ риска в высших учебных заведениях

Ключевые слова: *угроза, риск, безопасность, модель злоумышленника, алгоритм, метод.*

Введение. Проблема обеспечения безопасности каждого человека, любой страны, всего мирового сообщества является насущной, важнейшей потребностью современности, ибо речь идет о благополучном разрешении кризисной ситуации, об обеспечении выживания цивилизации и создании условий для ее дальнейшего устойчивого развития [1].

Решение этой сложнейшей проблемы требует объединения усилий всего мирового сообщества, всех международных организаций, каждого государства и, конечно, мировой науки и техники.

Для того чтобы обеспечить безопасность объекта защиты, нужно уметь противостоять угрожающим ему опасностям. В связи с этим при анализе проблемы безопасности любого объекта используются два основных понятия – «опасность» и «безопасность», которые нуждаются в соответствующих определениях (хотя, казалось бы, очевидно, что безопасность означает просто отсутствие всякой опасности) [2].

Эти два понятия в определенной степени связывает третье понятие – «риск», вокруг которого в последние десятилетия ведется оживленная полемика. Таким образом, в активно формирующейся в настоящее время теории риска и безопасности можно выделить основную триаду понятий: «Опасность – риск – безопасность» [3].

Методология. В процессе работы был использован системный подход, охватывающий методы обобщения и анализа факторов риска и методы математического моделирования.

Основная часть. На стадии концептуальной проработки вопросов безопасности вуза осуществляется рассмотрение общего состава потенциальных угроз. Определение и прогнозирование возможных угроз и осознание их опасности необходимы для обоснования, выбора и реализации защитных мероприятий, адекватных этим угрозам.

Для выделенных типов ресурсов характерны свои наборы воздействующих угроз (рис. 1). Источник угрозы может иметь как внутреннюю, так и внешнюю локализацию. Различают также случайные угрозы (пожары, аварии, непреднамеренная порча или уничтожение имущества) и преднамеренные угрозы (у источника угрозы – человека – есть мотив).

Угрозы в отношении помещений, зданий и материальных ресурсов проявляются как:

– хулиганские действия – повреждение и (или) уничтожение входных дверей, решеток, ограждений, оборудования, мебели, а также транспортных средств (личных и служебных);

– террористические акты или попытки их совершения;

– взрывы, пожары.

– кражи;

– хищение финансовых средств.

В общем плане к угрозам безопасности людских ресурсов относятся:

– хулиганские действия;

– террористические акты или попытки их совершения;

– взрывы, пожары.

Угрозы информационным ресурсам проявляются в виде:

– утечки информации ограниченного доступа через технические средства различного характера и исполнения;

– несанкционированного доступа к охраняемым сведениям;

– повреждения и (или) уничтожения носителей.

Осуществление угроз информационным ресурсам в электронном виде может быть произведено путем:

– несанкционированного доступа и съема информации ограниченного доступа;

– перехвата информации, циркулирующей в средствах и системах связи и вычислительной техники, несанкционированного доступа к ин-

формации и преднамеренных программно-математических воздействий на нее в процессе обработки и хранения.

Рис. 1. Таксономия угроз ресурсам вуза

Каждая из угроз может осуществляться нарушителем, поведение которого может быть описано одной из возможных моделей. Модель злоумышленника – это вербальное описание, включающее тип злоумышленника, его навыки по преодолению средств защиты и ограждающих конструкций, мотивацию. В случае вуза можно выделить следующие модели злоумышленника [4]:

1. Террорист.
2. Опытный вор.
3. Случайный посетитель.
4. Студент.
5. Сотрудник.

Указанные модели можно также разделить на два класса: внешнего и внутреннего нарушителя.

Для характеристики угроз используется свойство threat_prob (вероятность возникновения), а для характеристики злоумышленников – malefactor_prob (вероятность столкновения с определенным типом).

Вероятность угрозы, в связи с отсутствием какой-либо адекватной статистики по кражам, хищениям, порче имущества вузов, будет определяться экспертным путем [5]. *Субъективная вероятность* – это степень уверенности ЛПР в том, что событие произойдет. Вероятность возникновения угроз будет определяться экспертами с использованием подхода, предложенного в [6].

Следует отметить, что такие угрозы, как пожар и теракт, могут иметь весьма малую вероятность, однако их возникновение может приводить к ощутимым людским и материальным потерям.

Для того чтобы обоснованно определить архитектуру КТСБ и обоснованно выдвинуть требования к его составу, необходимо оценить риск от воздействия угроз и определить наиболее уязвимые ресурсы. *Риск* – это потенциаль-

ный ущерб от реализации воздействия угроз на объект обеспечения безопасности. Анализ риска позволяет определить уязвимые места объекта защиты, возможные потери и меры противодействия им.

Одним из наиболее распространенных методов оценки риска является метод, основанный на модели системы «с полным перекрытием», представляющей собой триаду «угрозы – средства защиты – ресурсы» в виде трехдольного графа [7]. Удобство данной модели – возможность введения и анализа количественных мер уязвимости (вероятность преодоления средств защиты, ущерб от реализации угроз) на основе взвешивания вершин и ребер графа. Рассмотрим подробнее процесс анализа риска на основе данной математической модели. В общем виде модель нейтрализации угроз при наличии средств безопасности выглядит следующим образом «Угрозы – барьеры – ресурсы».

Введем некоторые изменения в данную модель. Для упрощения анализа будем рассматривать не отдельные материальные, информационные и людские ресурсы, а их совокупности – составные ресурсы-помещения.

Разработаем алгоритм анализа риска для ресурсов вуза при отсутствии каких-либо средств обнаружения и задержки (кроме простейших – окон и дверей). Первым шагом при проведении анализа риска ресурсам ВУЗа является расчет вероятности существования угрозы. При анализе риска ресурсам ВУЗа рассматриваются минимум 5 моделей злоумышленника. Обозначим множество типов злоумышленника как $D = \{d_k\}$. Вероятность столкновения с определенным типом злоумышленника определяется распределением вероятностей $P(d_k) = \{P_{d_k}\}$. Найдем общий риск для ресурсов вуза от всех типов злоумышленника P_{male}.

Злоумышленник определенного типа при воздействии на объект защиты может реализовывать одну из угроз множества $Q^k = \{q_i\}$. Вероятность выбора злоумышленником той или иной угрозы определяется распределением вероятностей $P^k(q_i) = \{p_i^k\}$ [8].

Для каждого из типов злоумышленника значения вероятности выбора одной и той же угрозы различны, то есть можно выделить подмножество угроз, характерных для определенного типа злоумышленника:

$$\boldsymbol{Q'^k = \{q_i', p_i^k \geq p_k'\}}, \quad (1)$$

где p_k' – заданная для к-го типа злоумышленника граница вероятности.

Для этого достаточно назначить экспертно для каждой из угроз определенного типа злоумышленника, затем проранжировать эти значения и определить границу характерности p_k'. В простейшем случае, в качестве характерной можно выделить единственную угрозу, обладающую максимальной вероятностью из множества Q^k:

$$\boldsymbol{P_i^k = maxP^k(q_i)}. \quad (2)$$

Риск от воздействия i-й угрозы, характерной для злоумышленника d_k, на определенный ресурс-помещение L_j будет рассчитываться следующим образом:

$$\boldsymbol{r_{ij}^k = p_i^k \cdot P_{np}^j \cdot C_{Lj}}, \quad (3)$$

где p_i^k – вероятность реализации k-м типом злоумышленника угрозы q_i; P_{np}^j – вероятность проникновения в помещение; C_{Lj} – суммарная стоимость ресурсов помещения L_j.

Риск от угроз, реализуемых к-м типом злоумышленника в отношении]- го помещения рассчитывается по формуле:

$$\boldsymbol{r_j^k = \sum_i r_{ij}^k}. \quad (4)$$

При анализе риска от воздействия внешнего нарушителя в отсутствие каких-либо средств обеспечения безопасности, вероятность проникновения в помещение будет зависеть от устойчивости физических барьеров (окон, решеток, дверей), которые злоумышленник встречает на своем пути. На каждом рубеже угрозы, реализуемые тем или иным типом злоумышленника, будут ослабляться с учетом устойчивости барьера. В качестве основной характеристики защитных барьеров используется интенсивность $\lambda_{i,j}$ событий преодоления барьера – двери или окна – при переходе из i-го в j-й элемент, определяемая по формуле:

$$\boldsymbol{\lambda_{i,j} = \frac{1}{T_{i,j}}}, \quad (5)$$

где $T_{i,j}$ – время преодоления барьера, мин.

Время преодоления барьера определяется экспертным путем или на основе нормативных документов.

Риск для ресурсов j-го помещения от столкновения со всеми типами злоумышленников будет равен:

$$\boldsymbol{r_j = \sum_{k=1}^{5} r_j^k \cdot P_{d_k}}. \quad (6)$$

Для того чтобы найти суммарный риск от действий злоумышленников всех типов (Дтак) используется формула:

$$\boldsymbol{R_{male} = \sum_{j=1}^{m} r_j}, \quad (7)$$

где m – общее количество защищаемых помещений.

Для каждого из помещений полученное значение риска сравнивается с допустимым значением риска $r_{доп}$, которое назначается, исходя из индивидуальных особенностей объекта.

Выводы. Если рассчитанное значение риска превышает ограничение, то для обеспечения безопасности ресурсов данного помещения используются соответствующие средства и меры безопасности. Таким образом формируется архитектура комплекса технических средств безопасности.

**Работа выполнена в рамках программы стратегического развития БГТУ им. В.Г. Шухова на 2012 – 2016 годы.*

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Радоуцкий В.Ю., Шаптала В.Г., Шульженко В.Н., Добровольский В.С., Овечкин А.Н. Комплексная безопасность высших учебных заведений: монография. Петербург: Изд-во «Инфо - да», 2008. 120с.

2. Радоуцкий В.Ю., Шаптала В.Г. Характеристика внутренних опасностей и унроз образовательных учреждений высшего профессионального образования // Вестник Белгородского государственного технологического университета им. В.Г. Шухова. 2009. №3м. С. 124–126.

3. Радоуцкий В.Ю., Шаптала В.Г. Предупреждение риска террористических акций в области техносферы // Вестник Белгородского государственного технологического университета им. В.Г. Шухова. 2009. № 1. С. 141–142.

4. Васильев, В. И., Иванова, Т. А. Разработка методологических основ создания и внедрения комплексной системы безопасности вуза // Вестник УГАТУ, №2(18), 2006. С. 40–42.

5. Литвак, Б. Г. Экспертные оценки и принятие решений. М. ¡Патент, 1996. 271 с.

6. Герасименко, В.А. Защита информации в автоматизированных системах обработки данных. В 2-х кн.: Кн. 1. М.: Энергоатомиздат, 1994. 400 с.

7. Хоффман, Л.Дж. Современные методы защиты информации. М.:Сов.радио, 1980. 264 с.

8. Арьков, П.А. Исследование оптимальности проекта системы защиты информации на игровой модели // Материалы X Международной научно-практической конференции «Информационная безопасность». Ч. 1. Таганрог: Изд-во ТТИ ЮФУ, 2008. С. 33–34.

Bondar Yu.V., Stepanova M.N., Grevtsev M.V., Pavlenko A.V.
ANALYZING RISKS IN HIGHER EDUCATION INSTITUTIONS

The article analyzes hazards in higher education institutions premises, security hazards for human resources, hazards for informational resources, and singles out the threat actor models. The analysis of risks in higher education institutions has been carried out.

Key words: *hazard, risk, safety, threat actor model, algorithm, method.*

Бондарь Юрий Васильевич, старший преподаватель кафедры защиты в чрезвычайных ситуациях.
Белгородский государственный технологический университет им. В.Г. Шухова.
Адрес: Россия, 308012, Белгород, ул. Костюкова, д. 46

Степанова Мария Николаевна, кандидат технических наук, зав. лаб. кафедры защиты в чрезвычайных ситуациях.
Белгородский государственный технологический университет им. В.Г. Шухова.
Адрес: Россия, 308012, Белгород, ул. Костюкова, д. 46

Гревцев Максим Валерьевич, аспирант кафедры защиты в чрезвычайных ситуациях.
Белгородский государственный технологический университет им. В.Г. Шухова.
Адрес: Россия, 308012, Белгород, ул. Костюкова, д. 46.

Павленко Алексей Вячеславович, аспирант кафедры защиты в чрезвычайных ситуациях.
Белгородский государственный технологический университет им. В.Г. Шухова.
Адрес: Россия, 308012, Белгород, ул. Костюкова, д. 46.
E
-
m
a

H
Y
P
E
R