УДК 331.108.2
DOI: 10.26140/anie-2019-0804-0048

МЕТОДИЧЕСКИЕ ПОДХОДЫ К ОЦЕНКЕ АКТУАЛЬНОСТИ УГРОЗ КАДРОВОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Кузнецова Наталья Викторовна, кандидат экономических наук, доцент кафедры государственного управления и управления человеческими ресурсами
Марасанова Анна Александровна, кандидат экономических наук, доцент кафедры государственного управления и управления человеческими ресурсами
Байкальский государственный университет
(664003, Россия, Иркутск, ул. Ленина, 11, e-mail: marasananna@mail.ru)

Аннотация. Систематический подход к оценке актуальных угроз кадровой безопасности организации необходим для формирования адекватной эффективной системы защиты от действий персонала, способных нанести ущерб интересам компании. В статье предложена модель угроз кадровой безопасности организации, используя которую можно разработать систему контрмер, снижающих риски кадровой безопасности до допустимых уровней и обладающих наибольшей эффективностью. Для идентификации угроз кадровой безопасности определены способы (методы) реализации угроз, в результате чего предложена обобщенная классификация форм и методов реализации угроз кадровой безопасности. Дана характеристика уязвимостям, которые могут использоваться при реализации угроз кадровой безопасности, а также описаны последствия от реализации угроз. Для оценки степени возможного ущерба от реализации угрозы кадровой безопасности предложено определять возможный результат реализации угрозы, вид ущерба, к которому может привести реализация угрозы безопасности, степень последствий от реализации угрозы безопасности для каждого вида ущерба. Рассмотренная методика анализа угроз и их оценки позволяет получать обоснованные оценки угроз, уязвимостей, эффективности мер защиты, ориентирована на выявление антропогенных угроз кадровой безопасности, возникновение которых обусловлено объективными и субъективными факторами. К ее преимуществам можно отнести относительную простоту, полноту учета различных видов потерь, универсальность. Используемые методы исследования: методы анализа и синтеза теоретических подходов, методы классификаций и группировок.

Ключевые слова: безопасность, кадровая безопасность, угрозы, угрозы безопасности, угрозы кадровой безопасности, оценка угроз безопасности, актуальность угроз, вероятность угроз, уязвимости, потенциал нарушителя безопасности.

METHODOLOGICAL APPROACHES TO EVALUATING THE ACTIVITY OF THREATS OF PERSONNEL SECURITY OF THE ORGANIZATION

Kuznetzova Natalia Victorovna, candidate of economic sciences, Associate Professor of the Department of Public Administration and Human Recourses Management,
Marasanova Anna Aleksandrovna, candidate of economic sciences, Associate Professor of the Department of Public Administration and Human Recourses Management,
Baikal State University
(664003, Russia, Irkutsk, Lenin street 11, marasananna@mai.ru)

Abstract. A systematic approach to assessing current threats to the personnel safety of an organization is necessary to form an adequate effective system of protection against personnel actions that could harm the interests of the company. The article proposes a model of threats to the personnel security of the organization, using which it is possible to develop a system of countermeasures that reduce the risks of personnel security to acceptable levels and are most effective. To identify threats to personnel security, methods (methods) for implementing threats have been identified, as a result of which a generalized classification of forms and methods for implementing threats to personnel security has been proposed. The characteristics of vulnerabilities that can be used to implement threats to personnel security are described, and the consequences of the implementation of threats are described. To assess the degree of possible damage from the implementation of the threat to human security, it is proposed to determine the possible result of the threat, the type of damage that the implementation of the security threat can lead to, the degree of consequences from the implementation of the security threat for each type of damage. The considered methodology for analyzing threats and assessing them allows one to obtain reasonable assessments of threats, vulnerabilities, effectiveness of protection measures, and is aimed at identifying anthropogenic threats to human security, the occurrence of which is due to objective and subjective factors. Its advantages include relative simplicity, completeness of accounting for various types of losses, versatility. Used research methods: methods of analysis and synthesis of theoretical approaches, methods of classifications and groupings.

Keywords: security, personnel security, threats, security threats, threats to personnel security, assessment of security threats, the relevance of threats, the likelihood of threats, vulnerabilities, the potential of a security offender.

Постановка проблемы в общем виде и ее связь с важными научными и практическими задачами. Анализ угроз кадровой безопасности, прогнозирование наиболее вероятных из них являются важной задачей обеспечения кадровой безопасности и необходимы для своевременного принятия решений по предотвращению негативных воздействий на бизнес, формирования адекватной эффективной системы защиты от действий персонала, способных нанести ущерб интересам работодателя.

Актуальные угрозы включаются в модель, которая дает описание угроз, их источников, средств (методов) реализации угроз и возможных последствий. При этом актуальными признаются те угрозы, в отношении которых установлено, что потенциал нарушителя достаточен для реализации угроз, имеются потенциальные уязвимости, которые могут быть использованы для реализации угрозы безопасности, не исключаются возможности применения способов, необходимых для реализации угроз безопасности (известен возможный сценарий реализации угрозы), в результате реализации угрозы возможно возникновение негативных последствий (ущерба) [1-12].

Анализ последних исследований и публикаций, в которых рассматривались аспекты этой проблемы и на которых обосновывается автор; выделение неразрешенных раньше частей общей проблемы. Для идентификации угроз безопасности в теории и практике обеспечения безопасности определяются [13, с. 8; 14, с. 18; 15, с.176-177; 16, с. 43]:

- способы (методы) реализации угроз безопасности;
- возможности (тип, вид, потенциал) нарушителей, необходимые им для реализации угроз безопасности;

- уязвимости, которые могут использоваться при реализации угроз безопасности;
- объекты, на которые направлена угроза безопасности (объекты воздействия);
- результат и последствия от реализации угроз безопасности.

Используя эти положения, разработаем модель угроз кадровой безопасности организации (рис.).

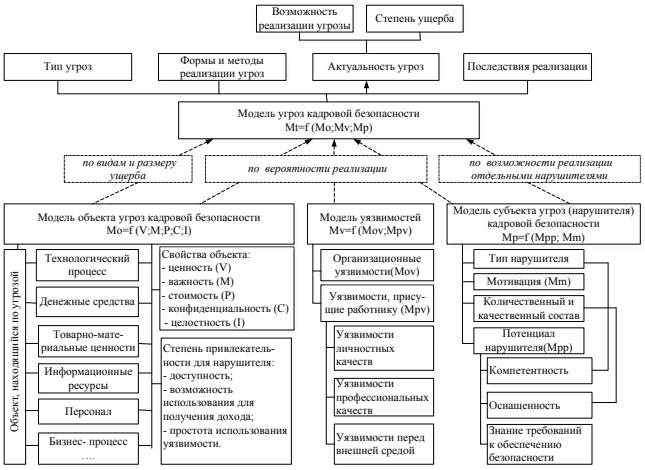

Рисунок 1 - Модель угроз кадровой безопасности организации

Как видно, процесс оценки актуальности угроз кадровой безопасности, исходящих от персонала и в его адрес, включает в себя: во-первых, оценивание возможных угроз кадровой безопасности, в том числе описание форм и методов их реализации и составление перечня угроз, ранжированного по вероятности их реализации; во-вторых, оценку потенциала субъекта в реализации угроз; в-третьих, идентификацию объекта угроз и оценивание тех его свойств, уменьшение (изменение) которых может оказать потенциально негативное воздействие на бизнес в случае реализации угроз; в-четвертых, оценку уязвимостей, что предполагает составление перечня условий и факторов, необходимых для реализации угроз.

В качестве угроз кадровой безопасности в модели выступают потенциально возможные негативные последствия от действий (бездействий) персонала, которые могут повлечь за собой причинение ущерба.

Цель статьи состоит в разработке методических подходов к формированию перечня угроз кадровой безопасности организации, способов (методов) их реализации и оценке степени их актуальности.

Изложение основного материала исследования. Целью определения возможных способов реализации угроз кадровой безопасности является формирование предположений о возможных сценариях реализации угроз безопасности, описывающих алгоритм (последовательность) действий отдельных нарушителей (или их групп) и применяемых ими методах (средствах) реализации угроз [13, с. 17-18].

Формы и методы реализации угроз кадровой безопасности в обобщенном виде представлены в таблице 1.

При определении возможных способов реализации угроз безопасности необходимо исходить из следующих условий:

- нарушитель может действовать один или в составе нарушителей;
- внутренний нарушитель может действовать совместно с внешним нарушителем;
- потенциал нарушителя выше, если реализация угрозы осуществляется при содействии нарушителя с внешними контрагентами;
- для достижения своей цели нарушитель выбирает наиболее слабое звено в системе защиты.

В связи с этим актуальной задачей представляется формирование представлений о нарушителе и уязвимостях кадровой безопасности [18-22]. Очевидно, что возможные способы реализации угроз во многом зависят от функционала работника, занимаемой им должности, определяющих доступ к ресурсам (активам, правам, информации и т.д.) организации, а также от особенностей систем управления персоналом и обеспечения кадровой безопасности.

Таблица 1 - Обобщенная классификация форм и методов реализации угроз кадровой безопасности организации

Формы реализации угроз	Методы реализации угроз	Примеры реализации
Мошенничество и воровство	Хищение товарно-материальных ценностей Хищение денежных средств и прочих высоколиквидных активов	Фальсификация финансовых документов, отчетности, незаконное присвоение вверенного имущества, растрата вверенного имущества
Внутреннее предпринимательство	Использование ресурсов организации в личных целях Организация и ведение параллельного бизнеса	Незаконный инсайдерский трейдинг Работа на другую компанию
Дача и получение коммерческого подкупа	Дача коммерческого подкупа, получение откатов	Дача взятки за совершение действий, вымогательство, заключение убыточных для работодателя сделок
Нарушение прав интеллектуальной собственности	Нарушение авторских, патентных, разглашение секретов производства («know-how») прав	Нарушение авторских прав на произведения литературы, искусства, науки, программы ЭВМ и т.д., присвоение авторства; нарушение патентных прав на: изобретение, полезную модель, промышленный образец и т.д.
Разглашение, повреждение, уничтожение конфиденциальной информации	С помощью компьютерных вирусов С помощью «враждебных» программ с целью записи и передачи информации Нарушение правил работы с конфиденциальной информацией, позволяющее заинтересованным лицам получить к ней несанкционированный доступ	Продажа / передача информации конкурентам Передача компрометирующей информации надзорным или налоговым органам
Недостаточная квалификация и недобросовестное отношение к выполняемой работе, ошибки в процессе выполнения работы	Повреждение или уничтожение имущества организации Нанесение вреда жизни и здоровью клиентам организации	Выполнение неразрешенных операций, повлекших убытки Несоблюдение установленных порядков и процедур, законодательства Отступление от установленных правил эксплуатации оборудования, технических и пр. систем

В качестве источника, на основе которых определяется перечень угроз безопасности, может служить как документальная информация (отчеты об аудите, выявленные факты недостачи, расхождения нормативной и фактической материалоемкости и т.д.), так и обзорные системы видеонаблюдения и видеозаписи, результаты рейдов, выборочный досмотр сотрудников на проходной, опросы персонала и т.д.

Для оценки степени возможного ущерба от реализации угрозы безопасности определяются возможный результат реализации угрозы, вид ущерба, к которому может привести реализация угрозы безопасности, степень последствий от реализации угрозы безопасности для каждого вида ущерба [17; 13, с. 28-29].

Основные виды ущерба и возможные негативные последствия от реализации угроз кадровой безопасности:

- экономический (снижение экономических показателей деятельности организации, в том числе недополучение ожидаемой (прогнозируемой) прибыли, потеря (кража) финансовых средств, товарно-материальных ценностей и прочих ликвидных активов, необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) на основании постановлений (решений) судов, решений органов, уполномоченных в соответствии с законодательством Российской Федерации или компенсаций, в том числе собственные судебные издержки, выплаты по решению суда, компенсации судебных издержек, убытки в результате небрежности или непреднамеренного невыполнения профессиональных обязательств либо в результате природы продукта (например, скоропортящиеся или легкообесценивающиеся товары) или конструкции продукта (хрупкость и прочее), необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт оборудования, прочих средств), необходимость дополнительных (незапланированных) затрат на восстановление деятельности и устранение последствий реализации угроз, необходимость дополнительных затрат, связанных с судебными разбирательствами, расследованием преступлений, потеря клиентов, поставщиков; потеря

конкурентного преимущества, невозможность (срыв) заключения договоров, соглашений; другие прямые или косвенные финансовые потери);

- социальный (увольнения, увеличение количества жалоб в контрольно-надзорные и правоохранительные органы, органы государственной власти и (или) местного самоуправления);

- репутационный (нарушение законодательных и подзаконных актов, нарушение деловой репутации, неспособность выполнения договорных обязательств, другие последствия, приводящие к нарушению репутации);

- технологический (невозможность или снижение эффективности решения задач бизнеса, замедление темпов развития компании и качества производимой продукции / оказываемых услуг; простой оборудования, информационной системы и пр.)

Кроме того, возможно нанесение и морального вреда (ухудшение морального климата в коллективе, снижение уровня доверия и т.д.).

Степень возможного ущерба от реализации угроз безопасности определяется экспертным методом как высокая, если в результате реализации угрозы возможны существенные негативные последствия, в результате возникновения потерь организация уже не сможет функционировать в прежнем режиме. Средняя степень присваивается в том случае, когда результате реализации угрозы возможны негативные последствия, сопровождающиеся потерями, неспособными значимо повлиять на жизнеспособность организации. Низкая степень определяется тогда, когда в результате реализации угрозы возможны незначительные потери, неспособные повлиять на жизнеспособность организации.

Оценка возможности реализации угрозы кадровой безопасности осуществляется на основе оценки уровня защищенности корпоративных ресурсов организации от угроз, исходящих от персонала и в его адрес, а также потенциала нарушителя. Вероятность того, что угроза реализуется, определяется привлекательностью объекта, возможностью его использования для получения дохода, а также простотой использования уязвимости при реализации угрозы.

Для оценки возможности (вероятности) реализации угрозы введем три вербальных показателя:

1. Высокий уровень защищенности (низкая вероятность) – отсутствуют объективные предпосылки к реализации угрозы, статистика по фактам реализации угрозы (возникновения инцидентов безопасности), мотивация для реализации угрозы. С высокой оперативностью могут быть приняты меры защиты, нейтрализующие угрозу.

2. Средний уровень защищенности (средняя вероятность) – существуют предпосылки к реализации угрозы, имеется статистика (т.е. зафиксированы случаи) по фактам реализации угрозы (возникновения инцидентов безопасности), существуют признаки наличия мотивации в реализации угрозы. Оперативно могут быть приняты меры защиты, нейтрализующие угрозу.

3. Низкий уровень защищенности (высокая вероятность) – существуют объективные предпосылки к реализации угрозы, имеется достоверная статистика по фактам реализации угрозы (возникновения инцидентов безопасности), у нарушителя есть мотивы для реализации угрозы. Не могут быть оперативно приняты меры защиты, нейтрализующие угрозу.

В результате возможность реализации угрозы кадровой безопасности в зависимости от уровня защищенности ресурсов организации и потенциала нарушителя определяется как высокая, средняя или низкая (табл. 2).

Таблица 2 - Матрица оценки возможности реализации угрозы кадровой безопасности

Потенциал нарушителя	Уровень защищенности объекта угроз		
	Низкий	Средний	Высокий
Низкий	Высокая	Средняя	Низкая
Средний	Высокая	Высокая	Средняя
Высокий	Высокая	Высокая	Высокая

В качестве результата реализации угрозы рассматриваются непосредственное или опосредованное воздействие на свойства объекта угрозы (ценность, важность, стоимость, конфиденциальность и т.д.) и на основе этого определяется актуальность угроз кадровой безопасности (табл. 3).

Таблица 3 - Определение актуальности угрозы кадровой безопасности

Вероятность (возможность) реализации угрозы	Степень возможного ущерба		
	Низкая	Средняя	Высокая
Низкая	Неактуальная	Неактуальная	Актуальная
Средняя	Неактуальная	Актуальная	Актуальная
Высокая	Актуальная	Актуальная	Актуальная

Процесс определения актуальности угроз кадровой безопасности должен носить систематический характер, рекомендуется пересматривать угрозы не реже одного раза в год. По результатам анализа проводится уточнение (при необходимости) модели угроз безопасности.

Пересмотр (переоценка) угроз кадровой безопасности, как минимум, осуществляется в случаях:

- изменения требований законодательства, в том числе в трудовой сфере, о защите информационных, финансовых ресурсов организации и т.д.

- выявления новых уязвимостей, приводящих к возникновению новых угроз или повышению возможностей их реализации;

- появления сведений о новых возможностях нарушителей;

- мониторинг жизненных обстоятельств и психологического состояния работников с целью выявления групп риска.

Систематический подход к оценке угроз необходим для формирования адекватной эффективной системы защиты от действий персонала, способных нанести ущерб интересам работодателя.

На основе построенной модели можно обоснованно выбрать систему контрмер, снижающих риски до допустимых уровней и обладающих наибольшей эффективностью.

Выводы исследования и перспективы дальнейших изысканий данного направления. Рассмотренная методика анализа угроз и их оценки позволяет получать обоснованные оценки угроз, уязвимостей, эффективности мер защиты, имеет такие преимущества, как относительная простота, полнота учета различных видов потерь, универсальность.

Перспективные аспекты в использовании методики можно свести к следующему:

- Несмотря на то, что методика является универсальной, стоит отметить, что для проведения высококачественного анализа и оценки угроз обязательна ее конкретизация применительно к конкретной организации.

- Большим сдерживающим фактором при проведении оценки угроз является высокая ее трудоемкость, которая может превышать выгоду от реализации рекомендаций. Поэтому важным вопросом является поиск оптимального соотношения между вероятными потерями организации в результате реализации угроз со стороны тех или иных должностных лиц компании (и в их адрес) и необходимыми затратами для их предотвращения и минимизации.

- При оценке потенциала нарушителя и вероятности реализации угроз исходным является предположение, что действия нарушителя тщательно спланированы и подготовлены. Вместе с тем нельзя исключить случайный характер реализации угрозы, которые не имеют статистической природы, реализованы впервые, соответственно, не могут быть оценены с высокой вероятностью.

- Предложенная методика оценки ориентирована на выявление антропогенных угроз кадровой безопасности, возникновение которых обусловлено объективными и субъективными факторами. Вместе с тем нельзя исключать возможность реализации угроз природного и

техногенного характера.

СПИСОК ЛИТЕРАТУРЫ:

1. Тулупьева Т.В., Тулупьев А.Л., Пащенко А.Е., Азаров А.А., Степашкин М.В. Социально-психологические факторы, влияющие на степень уязвимости пользователей информационных систем, с точки зрения социоинженерных атак // Труды СПИИРАН. 2010. Вып. 1(12). С. 200-214.

2. Кузнецова Н.В. Кадровая безопасность организации: сущность и механизм обеспечения [Текст] / Н.В. Кузнецова. Иркутск: Изд-во БГУЭП, 2013. 288 с.

3. Кузнецова Н.В. Тимофеева А.Ю. Проблемы выявления и оценки уязвимостей кадровой безопасности организации // Управление персоналом и интеллектуальными ресурсами в России. 2016. Т. 5. №. 4. С. 11-18.

4. Туренко Б.Г., Туренко Т.А. Методические подходы к оценке надежности и конкурентоспособности персонала предприятия // Известия Байкальского государственного университета. 2016. №26. С. 434-440.

5. Adekola B. The Impact of Organizational Commitment on Job Satisfaction: A Study of Employees at Nigerian Universities // International Journal of Human Resource Studies. 2012. no 2. pp. 1-17.

6. Campbell J.-L., Göritz A. Culture Corrupts! A Qualitative Study of Organizational Culture in Corrupt Organizations // Journal of Business Ethics. 2014. vol. 120. no 3. pp. 291-311.

7. Суходолов А.П., Иванцов С.В., Борисов С.В., Спасенников Б.А. Актуальные проблемы предупреждения преступлений в сфере экономики, совершаемых с использованием информационно-телекоммуникационных сетей // Всероссийский криминологический журнал. 2017. Т. 11, № 1. С. 13-21.

8. Солодова Н.Г. Модели поведения персонала в неустойчивых деловых организациях [Текст] / Н.Г. Солодова // Известия Иркутской государственной экономической академии. 2004. №1. С. 72-75.

9. Озерникова Т. Г.Тенденции трансформации социальной ответственности бизнеса в условиях экономического кризиса // Известия Иркутской государственной экономической академии. 2010. №4. С. 165-176.

10. Самаруха В.И., Хитрова Е.М., Гуляева Л.В. Мониторинг экономической безопасности Иркутской области // Известия Байкальского государственного университета. 2003. № 1 (34). С. 55-61.

11. Судакова Т.М., Васильева М.К. О некоторых криминологических параметрах обеспечения антинаркотической безопасности // Всероссийский криминологический журнал. 2019. Т. 13, № 2. С. 223-233.

12. Шободоева А. В. Вызовы и угрозы экологической безопасности Российской Федерации: теоретико-методологические аспекты // Baikal Research Journal. 2018. Т. 9, № 3. Режим доступа: http://brj-bguep.ru/reader/article.aspx?id=22244 (дата обращения: 5.02.2019).

13. Методика определения угроз безопасности информации в информационных системах : методический документ (утвержден Федеральной службой по техническому и экспортному контролю России, 2015.

14. Бояринцев А., Редькин В. Определение и ранжирование угроз объектам // БДИ. 2007. № 2 (71). С. 14- 19.

15. Соколов С. С. Модель угроз информационной безопасности организаций / С. С. Соколов // Журнал университета водных коммуникаций. Выпуск 2. С. 176-177;

16. Барабанов А.В., Гришин М.И., Кубарев А.В. Моделирование угроз безопасности информации, связанных с функционированием скрытых во вредоносных компьютерных программах // Вопросы кибербезопасности. 2014. № 4 (7). С. 41-48.

17. Миронова С. Ю. Система управления операционным риском в российских коммерческих банках и ее совершенствование: дисс… канд. экон. наук. М., 2014. 198 с.

18. Астахова Л. В. Проблема оценки HR-уязвимости объекта защиты информации // Вестник УрФО. Безопасность в информационной сфере. 2011. № 1. С. 26-33.

19. Алавердов А. Р. Управление кадровой безопасностью организации. М. : Маркет ДС, 2010. 176 с.

20. Устин П. Н. Возможности преодоления деструктивных тенденций в поведении человека // Ученые записки Казанского государственного университета. 2007. Т. 149. кн. 1. С. 197-208.

21. Антонян Ю. М. Личность преступника. Криминологопсихологическое исследование. М. : Норма : Инфра-М, 2010. 368 с.

22. Зеркалов Д. В. Разведка : хрестоматия, кн. 1 / Д.В.Зеркалов. К. : Наук. світ, 2008. С. 59-61.

Статья поступила в редакцию 26.08.2019
Статья принята к публикации 27.11.2019