

А. Н. Членов¹, Н. А. Рябцев², Т. А. Буцынская¹

(¹Академия ГПС МЧС России, ²НИЦ "Охрана" Росгвардии; e-mail: adbod@mail.ru)

РИСК ПРОНИКНОВЕНИЯ НАРУШИТЕЛЯ НА ОХРАНЯЕМЫЙ ПРОМЫШЛЕННЫЙ ОБЪЕКТ

Введён параметр риска несанкционированного проникновения, который позволяет дать комплексную оценку опасности совершения противоправных действий на охраняемом объекте. Полученные значения риска несанкционированного проникновения могут быть использованы при проектировании охранной сигнализации для обоснования параметров применяемых модулей технических средств, а также мер технической укреплённости и физической защиты объекта.

Ключевые слова: риск, несанкционированное проникновение, охраняемый объект.

Безопасность охраняемого объекта определяется возможностью **несанкционированного проникновения (НП)** нарушителя. После проникновения объекту может быть нанесён материальный ущерб в виде порчи имущества, поджога, террористического акта и других противоправных действий, независимо от результата его задержания сотрудниками охраны.

Таким образом, **потенциальный риск несанкционированного проникновения (далее – риск НП)** можно определить как количественную меру возможности реализации опасности совершения противоправных действий на объекте защиты и их последствий для людей и материальных ценностей.

Опасность объекту может быть ликвидирована, если произойдет своевременное обнаружение попытки проникновения – менее чем за время, необходимое для НП. Это время, связанное с прибытием сил реагирования, устанавливается нормативно для каждого объекта с учётом места его размещения, а также условий охраны.

Результаты и выводы, полученные при определении риска НП, могут быть использованы при проектировании системы охраны для обоснования параметров применяемых технических средств (подсистем) и мер технической укреплённости (физической защиты).

Характеристикой соответствия риска НП требуемому является неравенство [1].

$$Q_{\text{нп}} \leq Q_{\text{нп}}^{\text{н}}, \quad (1)$$

где $Q_{\text{нп}}^{\text{н}}$ – нормативное значение риска НП;

$Q_{\text{нп}}$ – расчётная величина риска НП.

Расчётная величина риска НП $Q_{\text{нп}i}$ для i -го сценария проникновения на объекты различных категории (А1, А2, Б1, Б2) может быть определена с использованием выражения:

$$Q_{\text{нп}i} = P_{\text{нп}i}(1 - P_{\text{эо}i})(1 - P_{\text{дп}i}), \quad (2)$$

где $P_{\text{нп}i}$ – оценка вероятности попытки проникновения на охраняемый объект для i -го сценария может быть определена на основании статистических данных как частота попыток проникновения на охраняемый объект данного вида (категории) в течение установленного времени [2];

$P_{эoi}$ – оценка вероятности эффективного обнаружения НП охранной сигнализацией для i -го сценария;

$P_{дпi}$ – оценка вероятности противодействия НП дополнительными подсистемами, входящими *интегрированную систему охраны (ИСО)* объекта, воздействующими на факторы НП, для i -го сценария.

Для типового состава ИСО, соответствующего ГОСТ Р 53704-2009 "Системы безопасности комплексные и интегрированные. Общие технические требования" и ГОСТ Р 56102.1-2014 "Системы централизованного наблюдения. Часть 1. Общие положения" в качестве подсистем, дополнительно противодействующих НП и формирующих $P_{дпi}$ могут быть подсистемы видеонаблюдения, технической укреплённости и инженерной защиты, а также контроля доступом [2]. Не следует исключать и возможное положительное влияние на $P_{дпi}$ и других систем безопасности промышленного объекта.

Все возможные сценарии S_i НП составляют конечное множество H , состоящее из k членов:

$$H \subseteq (S_1, S_2, \dots S_i, \dots S_k), \quad (4)$$

В общем случае случайные события реализации возможных сценариев НП являются независимыми, несовместными и образуют полную группу.

Для конкретного объекта M при учёте его конструктивных особенностей, а также имеющейся информации о вероятности реализации конкретных сценариев, количество членов множества H может быть сокращено:

$$H_M \subseteq (S_1, S_2, \dots S_i, \dots S_l), \quad L < K. \quad (5)$$

При формировании системы охраны объекта M условие (1) должно быть выполнено для каждого возможного сценария НП

$$Q_{нпi} \leq Q_{нп}^H, \quad i = 1, \dots, l. \quad (6)$$

При расчёте должен выбираться тот сценарий развития НП, при котором достигается худшее (максимальное) значение риска НП. Поэтому в дальнейшем индекс " i " можно не указывать.

Если для объекта M максимальное значение риска НП из всех возможных сценариев будет $Q_{нп}^M$, то условие (6) можно записать в виде:

$$Q_{нп}^M \leq Q_{нп}^H. \quad (7)$$

Таким образом, с учётом (2), условие эффективности системы обнаружения НП будет

$$P_{пп}(1 - P_{эo})(1 - P_{дп}) \leq Q_{нп}^H. \quad (8)$$

Докажем, что неравенство

$$P_{эo} \geq (1 - Q_{нп}^H/P_{пп}) \quad (9)$$

является необходимым и достаточным условием эффективности системы обнаружения НП.

Рассмотрим систему охранной сигнализации, функционирующую без дополнительных подсистем в составе ИСО, то есть положим $P_{дп} = 0$. В этом случае, преобразуя (9) относительно $Q_{нп}^H$, получим (7), что подтверждает необходимость (9) для выполнения условия (6) эффективности системы обнаружения НП.

Поскольку при наличии дополнительных подсистем в составе ИСО $P_{\text{дп}}$ в силу определения вероятности всегда ≥ 0 , неравенство (9) независимо от вида используемых подсистем только усиливается, что подтверждает достаточность условия (9) эффективности системы обнаружения НП.

Для типового состава ИСО $P_{\text{дп}}$ может быть представлена в виде:

$$P_{\text{дп}} = 1 - (1 - P_{\text{в}})(1 - P_{\text{т}})(1 - P_{\text{д}})(1 - P_{\text{б}}), \quad (10)$$

где $P_{\text{в}}$, $P_{\text{т}}$, $P_{\text{д}}$ – оценка вероятности противодействия НП подсистемами видеонаблюдения, технической укреплённости и инженерной защиты, а также контроля доступом соответственно, действующими в составе системы охраны;

$P_{\text{б}}$ – оценка вероятности противодействия НП системами безопасности промышленного объекта.

Графическое представление реализации условия (8) для конкретных выбранных значений параметров показано на рис. 1.

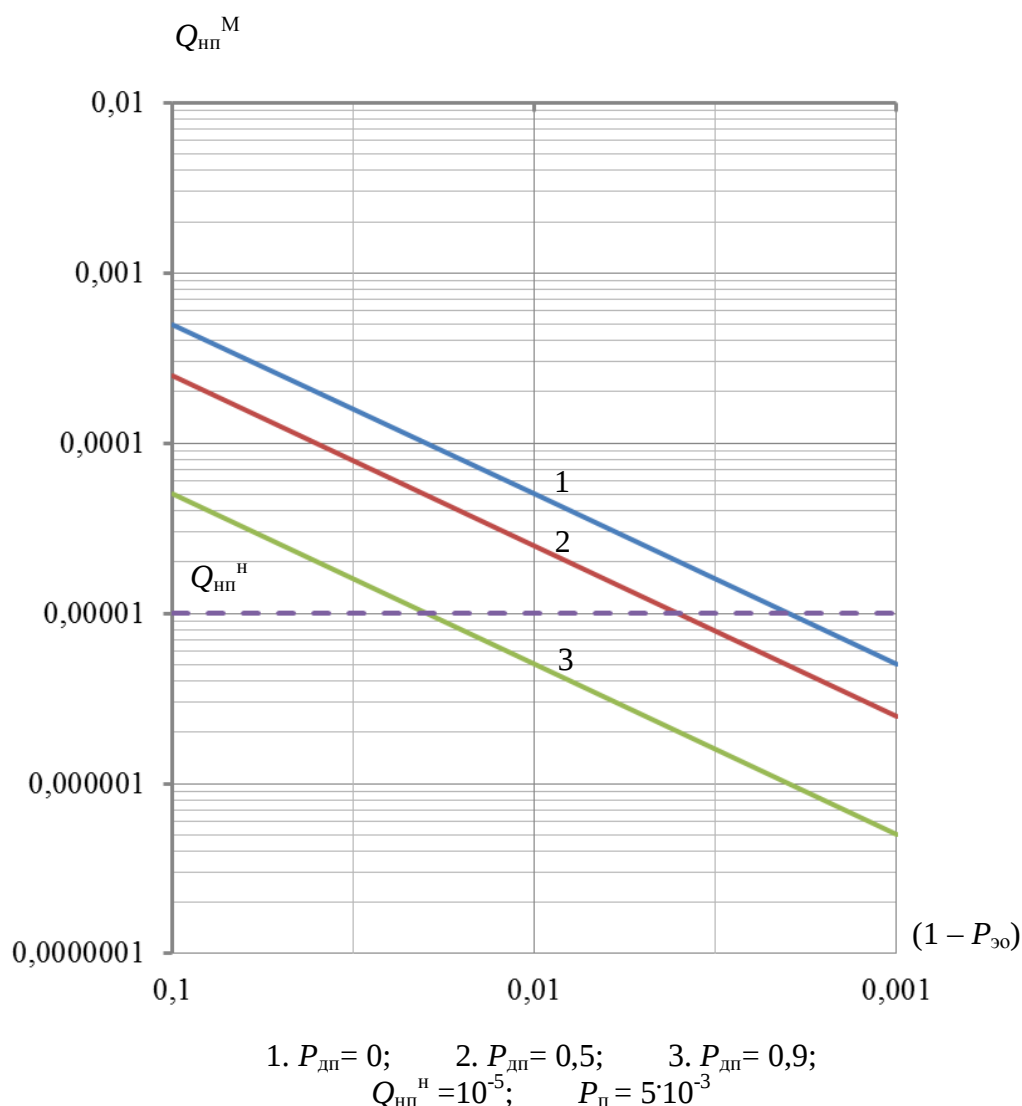


Рис. 1. Зависимость риска несанкционированного проникновения от вероятности эффективного обнаружения $Q_{\text{нп}}^M = f(1 - P_{\text{зо}})$

Из рис. 1 следует, что практическое снижение уровня риска НП до нормативного значения может быть достигнуто увеличением вероятности эффективного обнаружения нарушителя охранной сигнализацией $P_{зо}$, а также усилением положительного влияния дополнительных систем, входящих в ИСО [3].

В случае, если при большом значении вероятности попытки проникновения на охраняемый объект $P_{ппи}$ это не представляется возможным, в состав ИСО объекта могут быть включены (усилены) средства видеонаблюдения, технической укреплённости и инженерной защиты, контроля доступом, задействованные для защиты от НП.

Следует отметить, что в настоящее время официально принятого понятия риска НП как и его нормативного уровня не установлено [4].

Рассмотрим подробнее параметр $P_{зо}$, характеризующий вероятность эффективного обнаружения нарушителя охранной сигнализацией, и его составляющие.

Применительно к рассматриваемой задаче под модулем ТС обнаружения (охранной сигнализации) следует понимать комплекс взаимосвязанных ТС ОС, предназначенный для обнаружения нарушителя при i -м сценарии (варианте) проникновения его на объект. Минимальный состав модуля – один извещатель, максимальный – рубеж, объектовая подсистема.

Для $P_{зо}$ термин "эффективный" характеризует вероятность обнаружения с учётом комплекса воздействующих внутренних и внешних факторов.

В соответствии с этим, выражение для $P_{зо}$ будет иметь вид:

$$P_{зо} = (1 - P_{от}) \cdot (1 - P_{но}) \cdot (1 - P_c), \quad (11)$$

где $P_{от}$ – вероятность технического отказа ТС на период обнаружения;

$P_{но}$ – вероятность пропуска цели (не обнаружения);

P_c – вероятность саботажа.

Под саботажем понимаем результат преднамеренных действий нарушителя, приводящий к нарушению функций обнаружения НП системой охраны.

Таким образом, введение параметра риска НП позволяет дать комплексную оценку опасности совершения противоправных действий на охраняемом объекте.

Существующие на сегодняшний день теоретические и экспериментальные методы позволяют провести количественную оценку риска НП на этапе проектирования системы охраны.

$P_{пп}$ может быть определена на основании статистических данных как частота попыток проникновения на охраняемый объект данного вида (категории). Например, в [5] приводится методика и пример расчёта вероятности появления нарушителя на объектах разной категории. Согласно оценкам профессора Шепитько Г.Е., вероятность появления нарушителя на объектах $P_{ц}$ составляла на период исследования от 0,005 (особо важные объекты), 0,05 (музеи и простые объекты) до 0,12 (важные объекты) в год.

В ряде опубликованных работ авторами получены математические выражения, пригодные для расчёта параметров, входящих в выражение (11). Данные выражения приведены в табл. 1.

Таблица 1

Формулы для расчёта P_{Σ}

Параметр	Математическое выражение	Характеристика входящих в формулу членов	Источник
$1 - P_{от}$	$\frac{T_{но}}{T_{но} + T_{в}} e^{-\frac{t_n}{T_{но}}}$	$T_{но}$ – среднее время наработки на отказ; $T_{в}$ – среднее время восстановления, t_n – время наблюдения	Буцынская Т. А., Николаев В. А., Рябцев Н. А. Комплексный показатель технической эффективности системы тревожной сигнализации // Матер. 25-й междунар. науч.-техн. конф. "Системы безопасности – 2016". М.: Академия ГПС МЧС России, 2016. С. 386, 387
$1 - P_{но}$	$e^{-g_0 t_d}$ * при установлении полного приборного контакта	g_0 – мгновенная плотность вероятности обнаружения; t_d – время обнаружения	Рябцев Н. А., Буцынская Т. А. О вероятности обнаружения нарушителя системой тревожной сигнализации // Технологии техносферной безопасности. Вып. 1 (71). 2017. С. 312-316
$1 - P_c$	$\prod_{j=1}^m g_j$	m – количество вариантов саботажа; g_j – относительное количество обнаруженных попыток саботажа данного вида	Николаев В. А., Рябцев Н. А. Условие повышения надёжности системы тревожной сигнализации объекта особой важности // Матер. 25-й междунар. науч.-техн. конф. "Системы безопасности – 2016". М.: Академия ГПС МЧС России, 2016. С. 390, 391

Полученные значения риска НП могут быть использованы при проектировании системы охраны для обоснования параметров применяемых подсистем (модулей, технических средств обнаружения), а также мер технической укреплённости и физической защиты объекта [6].

Литература

1. Королев В. Ю., Шоргин С. Я., Бенинг В. Е. Математические основы теории риска: учеб. пос. М.: Физматлит, 2011. 620 с.
2. Гмурман В. Е. Теория вероятностей и математическая статистика: учебник для СПО. М.: Юрайт, 2016. 480 с.
3. Членов А. Н., Самышкина Е. В., Новосельцев Б. Г., Канзафарова М. Е. Современное состояние разработки и производства технических средств тревожной сигнализации в России // Технологии техносферной безопасности. 2015. Вып. 1 (59). С. 51-54. <http://academygps.ru/ttb>.
4. Антоненко А. А., Буцынская Т. А., Членов А. Н. Нормативное обеспечение систем комплексной безопасности объектов // Технологии техносферной безопасности. 2010. Вып. 2 (30). 7 с. <http://academygps.ru/ttb>.
5. Шепитько Г. Е. Исследование характеристик модели нарушителя // Технические средства охраны: сб. научн. тр. М.: ВНИИПО МВД России, 1992. С. 41-49.
6. Мокшанцев А. В., Тетерин И. М., Топольский Н. Г. Модели, методы и алгоритмы поддержки принятия управленческих решений при поиске и обнаружении пострадавших под завалами, образующимися в результате чрезвычайных ситуаций, аварий, пожаров и взрывов // Технологии техносферной безопасности. 2013. Вып. 5 (51). 17 с. <http://academygps.ru/ttb>.

Материал поступил в редакцию 21 июня 2018 г.

Для цитирования: Членов А. Н., Рябцев Н. А., Буцынская Т. А. Риск проникновения нарушителя на охраняемый промышленный объект // Технологии техносферной безопасности. – Вып. 2 (84). – 2019. – С. 132-137. DOI: 10.25257/TTS.2019.2.84.132-137.

A. N. Chlenov, N. A. Ryabtsev, T. A. Butcinskaya
RISK OF ENTRY OF THE OFFENDER
TO A PROTECTED INDUSTRIAL FACILITY

The article deals with the design of a security system that ensures guaranteed protection of an industrial facility according to the standard criterion of compliance with the risk of unauthorized entry to the statutory established risk. The object of the study is to ensure the safety and security of an industrial object, and the subject is the process of forming an alarm system. A new parameter has been introduced – the risk of unauthorized entry, which is a quantitative measure of the possibility of realizing the danger of committing unlawful actions at the object of protection and their consequences for people and wealth. Existing theoretical and experimental methods that allow make a quantitative assessment of the risk of unauthorized entry during the design of the security system are considered. The obtained values of the risk of unauthorized entry can be used when designing an alarm system to substantiate the parameters of the used technical detection equipment, as well as measures of technical strengthening and physical protection of the object.

Key words: risk, unauthorized entry, protected facility.

References

1. Korolev V. Yu., SHorgin S. Ya., Bening V. E. *Matematicheskie osnovy teorii riska: ucheb. pos.* [Mathematical foundations of risk theory: textbook]. Moscow, Fizmatlit Publ., 2011, 620 p.
2. Gmurman V. E. *Teoriya veroyatnostej i matematicheskaya statistika: uchebnik dlya SPO* [Probability theory and mathematical statistics: textbook]. M.: Yurajt Publ., 2016, 480 p.
3. Chlenov A. N., Samyshkina E. V., Novoselcev B. G., Kanzafarova M. E. Current state of development and production of alarm technical means in Russia. *Tehnologii tekhnosfernoj bezopasnosti / Technology of technosphere safety*, 2015, vol. 1 (59), pp. 51-54. Available at: <http://academygps.ru/ttb> (in Russian).
4. Antonenko A. A., Butcinskaya T. A., Chlenov A. N. Regulatory support of systems integrated safety of objects. *Tehnologii tekhnosfernoj bezopasnosti / Technology of technosphere safety*, 2010, vol. 2 (30), 7 p. Available at: <http://academygps.ru/ttb> (in Russian).
5. Shepitko G. E. *Issledovanie harakteristik modeli narushitelya* [Investigation of the characteristics of the model of the offender]. *Tekhnicheskie sredstva ohrany: sb. nauchn. tr.* [Proceed. of Conference " Technical means of protection"], Moscow, Higher engineering fire-technical school of Internal Affairs of Russia Publ., 1992, pp. 41-49.
6. Mokshantsev A. V., Teterin I. M., Topolsky N. G. Models, methods and algorithms of support of decision-making in the search and find survivors under the rubble, formed in the result of emergency situations, accidents, fires and explosions. *Tehnologii tekhnosfernoj bezopasnosti / Technology of technosphere safety*, 2013, vol. 4 (51), 17 p. Available at: <http://academygps.ru/ttb> (in Russian).

For citation: Chlenov A. N., Ryabtsev N. A., Butcinskaya T. A. Risk of entry of the offender to a protected industrial facility. *Tekhnologii tekhnosfernoj bezopasnosti / Technology of technosphere safety*, vol. 2 (84), 2019, pp. 132-137 (in Russian). DOI: 10.25257/TTS.2019.2.84.132-137.