УДК 004.056.53

Анализ вероятности проникновения нарушителя на объект через периметр

Герлинг Е. Ю.

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Санкт-Петербург, 193232, Российская Федерация

Постановка задачи: *Обеспечение информационной безопасности, особенно на объекте связи, является актуальной задачей, и важную роль здесь играет физическая защищенность объекта: невозможность для нарушителя проникнуть на охраняемую территорию незамеченным; периметральная сигнализация необходима для раннего обнаружения попыток проникновения на объект связи или промышленный объект; от ее эффективной и надежной работы зависит информационная безопасность, а также защищенность объекта от террористической атаки, сохранение жизни и здоровья людей и другие важные аспекты.* ***Цель работы*** *– проанализировать и сравнить вероятности проникновения нарушителя через ограждение при использовании на объекте извещателей периметральной сигнализации, основанных на различных принципах действия, а также комбинации данных извещателей.* ***Результат:*** *Проанализирована эффективность периметральной сигнализации при применении разных извещателей, а также при их комбинации. Кроме того, приведены расчеты вероятности преодоления нарушителем ограждения для рассмотренных случаев. Разобраны принципы обнаружения нарушителя извещателями периметральной сигнализации; различные принципы их действия позволяют обнаружить попытки проникновения разными способами, поэтому для повышения защищенности объекта рекомендуется комбинировать извещатели периметральной сигнализации.* ***Практическая значимость:*** *результаты исследования могут использоваться для выбора и комбинации извещателей периметральной сигнализации, позволяют повысить вероятность раннего обнаружения проникновения нарушителя на объект, что увеличивает его защищенность.*

Ключевые слова: *периметральная сигнализация, ограждение, вероятность проникновения нарушителя, извещатель, объект связи*

Введение

На информационную безопасность объекта связи влияет много факторов [1]. Говоря о защите информации, как правило, подразумевают непосредственную защиту данных, которые хранятся и передаются в цифровом виде. Предполагается защищать каналы от прослушивания, серверы от вторжения по цифровым каналам [2, 3]. Однако информационная безопасность начинается с физической защиты объекта связи или промышленного объекта, и прежде всего – с предотвращения проникновения нарушителя на объект, в серверную или к помещениям с кабельными линиями [4].

Информационная безопасность особенно актуальна на крупных промышленных объектах, где локальные сети являются неотъемлемой частью управления сложными технологическими процессами, а также непосредственно на объектах связи. В этом случае проникновение нарушителя в серверную или аппаратную (помещение, где расположено оборудование, контролирующее технологические про-

Библиографическая ссылка на статью:
Герлинг Е. Ю. Анализ вероятности проникновения нарушителя на объект через периметр // Вестник СПбГУТ. 2023. Т. 1. № 2. С. 4. EDN: JZIKZD

Reference for citation:
Gerling E. Analysis of the Probability of Intruder Penetration into the Facility through the Perimeter // Herald of SPbSUT. 2023. Vol. 1. Iss. 2. P. 4. EDN: JZIKZD

EDN: JZIKZD
URL: https://vestnik-sut.ru/2023-2/C04.pdf

цессы) может привести к незапланированной остановке производства, к глобальной экологической катастрофе, к обрыву каналов связи и к другим негативным последствиям [5].

Важной составляющей как защиты информации, так и безопасности сотрудников и посетителей является физическая безопасность объекта, которая обеспечивается взаимодействием нескольких объектовых систем [6]. Список необходимых для защиты систем зависит от особенностей объекта, но, как правило, включает в себя периметральную сигнализацию, охранную сигнализацию, систему контроля и управления доступом и систему охранного видеонаблюдения [7]. Правильно спроектированные и установленные системы физической безопасности объекта позволяют свести вероятность незамеченного проникновения нарушителя на объект почти к нулю, тем самым способствуя обеспечению информационной безопасности [8].

Периметральная сигнализация, охранная сигнализация, видеонаблюдение, система контроля и управления доступом – это системы физической безопасности объекта связи или промышленного объекта (далее – объекта), которые необходимы для своевременного обнаружения попыток проникновения на объект. При попытках проникнуть на объект нарушитель встретится, прежде всего, с периметральной сигнализацией, которая будет подробно рассмотрена в данной работе.

Защита периметра объекта связи

Основной задачей периметральной сигнализации является обнаружение попыток проникновения злоумышленника на объект (сигнал тревоги) и информирование о данном инциденте соответствующих служб. При защите объекта важно минимизировать ошибки ложной тревоги, когда периметральная сигнализация дает сигнал тревоги при отсутствии попытки проникновения, а также минимизировать ошибки пропуска нарушителя. Последнее требование является особо актуальным на сегодняшний день, поскольку несанкционированное проникновение человека на объект может повлечь за собой как локальную катастрофу, так и глобальную, например, если объект информатизации является критической информационной инфраструктурой. В данной работе ставится задача рассчитать вероятность пропуска нарушителя на объект при использовании различных извещателей, а также при их комбинированном использовании.

Анализ периметральных извещателей

Периметральная сигнализация, как видно из названия, контролирует периметр объекта. Для предотвращения проникновения на объект злоумышленника по периметру устанавливается ограждение, но его можно сломать, через него можно перелезть, под ним можно сделать подкоп. Для контроля попыток преодоления ограждения используются периметральные извещатели, которые вместе с приемно-контрольными приборами составляют периметральную сигнализацию.

Работа разных извещателей основана на различных физических принципах действия. Рассмотрим наиболее популярные периметральный извещатели.

Для контроля целостности полотна ограждения применяются вибрационные извещатели, которые позволяют зафиксировать попытки разреза сетчатого или решетчатого полотна, пролома бетонного полотна, перелаза или подкопа под ограждения. Для предотвращения подкопа под ограждением зарывается противоподкопная решетка, на которую и устанавливается извещатель.

Пример установки извещателя вибрационного трибоэлектрического «ГЮРЗА» приведен на рисунке 1 [9]: показано размещение трибокабеля (чувствительный элемент извещателя вибрационного трибоэлектрического), который воспринимает малейшие колебания полотна ограждения, возникающие при попытках его перелаза или разреза. Вероятность обнаружения данным видом извещателя попытки проникновения постороннего на объект составляет не менее 98 % [9].

Еще один извещатель, позволяющий обнаружить проникновение нарушителя на объект, – проводноволновой извещатель. В зависимости от способа установки он может контролировать проникновение нарушителя через полотно ограждения или путем перелаза. На рисунке 2 представлены варианты установки и зоны контроля извещателя охранного линейного проводноволнового «Импульс-12» [10].

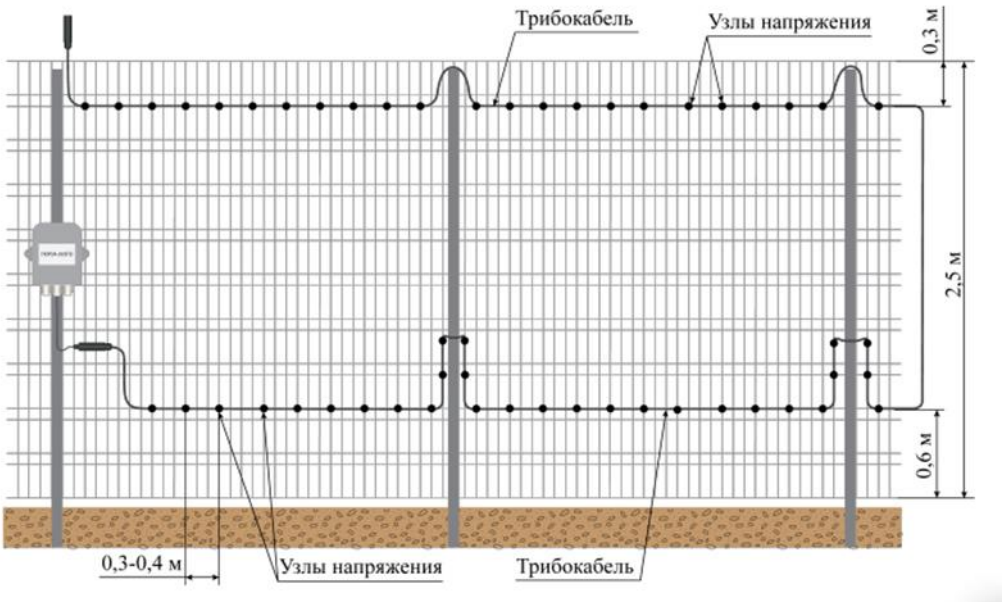
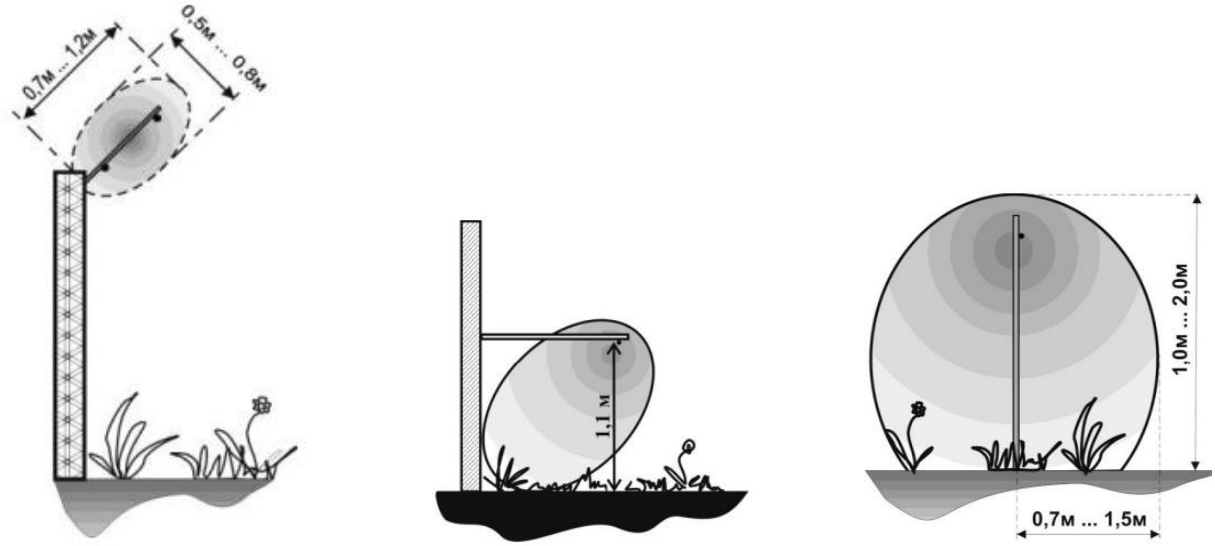


Рис. 1. Пример установки извещателя вибрационного трибоэлектрического



а) б) в)

Рис. 2. Варианты установки и зоны контроля извещателя охранного линейного проводноволнового:
а) в верхней части заграждения; б) вдоль заграждения; в) вдоль поверхности земли

Рассмотрим подробнее вариант установки извещателя проводноволнового. На рисунке 2а показана установка извещателя на противоперелазный козырек: такой метод установки позволяет обнаружить попытки перелаза ограждения. На рисунке 2б показан вариант контроля попыток проникновения через полотно ограждения, а также, в определенных случаях, с помощью подкопа. На рисунке 2в показан вариант монтажа извещателя не на ограждении, а на отдельно стоящих столбах. Подобная установка позволяет контролировать периметр, когда физического ограждения нет, а также – около существующего ограждения на расстоянии. В последнем случае можно обнаружить проникновение нарушителя на объект через полотно ограждения или методом перелаза. Вероятность обнаружения данным видом извещателя попытки проникновения постороннего на объект составляет не менее 98 % [10].

Для защиты периметра объекта также применяются извещатели радиоволновые двухпозиционные (передатчик и приемник). Их принцип действия основан на создании в пространстве между передатчиком и приемником электромагнитного поля, формирующего объемную зону обнаружения в виде вытянутого эллипсоида вращения и регистрации изменений этого поля при пересечении зоны обнаружения нарушителем. На рисунке 3 представлены варианты установки и зоны контроля извещателя охранного радиоволнового двухпозиционного «Барьер» [11].

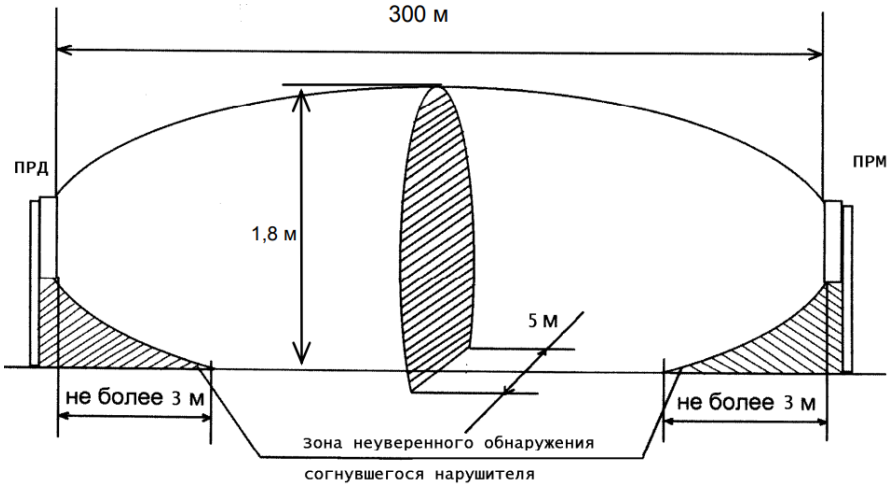


Рис. 3. Варианты установки и зоны контроля извещателя охранного радиоволнового двухпозиционного (ПРД – передатчик, ПРМ – приемники)

На рисунке 3 показано размещение приемника и передатчика извещателя охранного радиоволнового двухпозиционного: высота контролируемой зоны составляет не менее 1,8 м, ширина – не менее 5 м. Вероятность обнаружения данным видом извещателя попытки проникновения постороннего на объект составляет не менее 98 % [11].

Рассмотрим еще один популярный для защиты периметра извещатель – извещатель охранный инфракрасный двухпозиционный (передатчик и приемник) активный. Извещатель формирует в пространстве между передатчиком и приемником невидимые инфракрасные лучи, при прерывании которых нарушителем выдается сигнал тревоги. На рисунке 4 представлена схема лучей извещателя охранного инфракрасного двухпозиционного «МИК» [12].

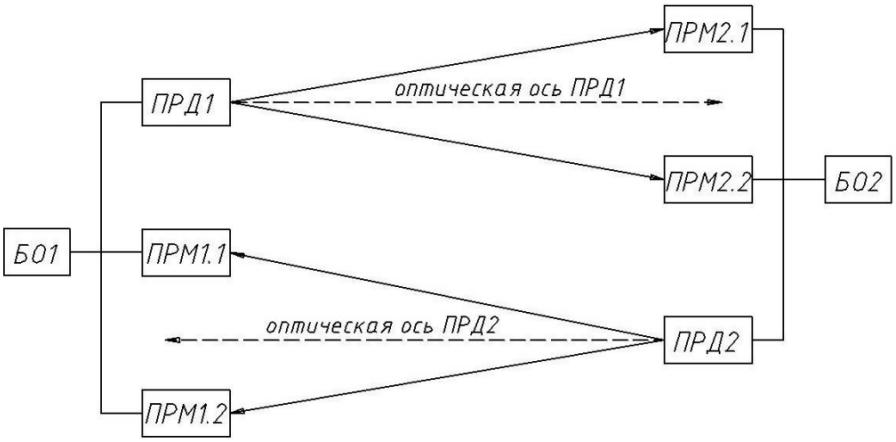


Рис. 4. Схема лучей извещателя охранного инфракрасного двухпозиционного (ПРД – передатчик, ПРМ – приемник, БО – блок обработки)

На рисунке 4 показаны инфракрасные лучи и оптические оси извещателей охранных инфракрасных двухпозиционных. Вероятность обнаружения данным видом извещателя попытки проникновения постороннего на объект составляет не менее 99 % [12].

Вероятность успешного преодоления периметра объекта

Сведем данные по вероятности обнаружения проникновения нарушителя на объект и вероятности пропуска нарушителя в единую таблицу (см. таблицу 1).

Таблица 1. Вероятности обнаружения и пропуска нарушителя периметральными извещателями

Извещатель	Вероятность обнаружения проникновения нарушителя на объект, %	Вероятность пропуска нарушителя, %
Вибрационный	98	2
Проводноволновой	98	2
Радиоволновой	98	2
Инфракрасный	99	1

Ранее была рассмотрена вероятность обнаружения попытки проникновения постороннего на объект для различных периметральных извещателей. Как правило, на периметре устанавливаются два периметральных извещателя с разными принципами действия. Вероятность пропуска нарушителя при проникновении на объект можно рассчитать по формуле:

$$P_{2\text{ПН}} = P_{\text{ПН.1}} \cdot P_{\text{ПН.2}},$$

где $P_{2\text{ПН}}$ – вероятность пропуска нарушителя при двух извещателях; $P_{\text{ПН.1}}$ – вероятность пропуска нарушителя первого извещателя; $P_{\text{ПН.2}}$ – вероятность пропуска нарушителя второго извещателя.

Рассчитаем вероятность проникновения нарушителя на объект при комбинации различных периметральных извещателей. Отметим, что на практике не рекомендуется использовать комбинацию из проводноволнового и радиоволнового извещателей, поскольку они обладают схожими принципами обнаружения нарушителя. Результаты расчета приведены в таблице 2.

Таблица 2. Вероятность обнаружения и пропуска нарушителя комбинацией из двух периметральных извещателей

Извещатели	Вероятность обнаружения проникновения нарушителя на объект, %	Вероятность пропуска нарушителя, %
Вибрационный и проводноволновой	99,96	0,04
Вибрационный и радиоволновой	99,96	0,04
Вибрационный и инфракрасный	99,98	0,02
Проводноволновой и инфракрасный	99,98	0,02
Радиоволновой и инфракрасный	99,98	0,02

При комбинировании вибрационного извещателя с проводноволновым или радиоволновым вероятность пропуска нарушителя на объект будет составлять 0,04 %. Комбинация инфракрасного извещателя с вибрационным, проводноволновым или радиоволновым даст вероятность пропуска нарушителя на объект равную 0,02 %. При применении на периметре сразу двух извещателей с разным принципом действия вероятность пропуска нарушителя на объект снижается в 50 раз, а вероятность обнаружения попытки проникновения возрастает. Именно поэтому на современных объектах связи и промышленных объектах необходимо оборудовать периметральное ограждение как минимум двумя разными типами извещателей с различными принципами обнаружения проникновения.

Рассчитаем вероятность проникновения нарушителя на объект при комбинации трех периметральных извещателей по формуле:

$$P_{3\text{ПН}} = P_{\text{ПН.1}} \cdot P_{\text{ПН.2}} \cdot P_{\text{ПН.3}},$$

где $P_{3\text{ПН}}$ – вероятность пропуска нарушителя при трех извещателях; $P_{\text{ПН.1}}$ – вероятность пропуска нарушителя первого извещателя; $P_{\text{ПН.2}}$ – вероятность пропуска нарушителя второго извещателя; $P_{\text{ПН.3}}$ – вероятность пропуска нарушителя третьего извещателя.

Результаты расчета приведены в таблице 3.

Таблица 3. Вероятности обнаружения и пропуска нарушителя комбинацией из трех периметральных извещателей

Извещатели	Вероятность обнаружения проникновения нарушителя на объект, %	Вероятность пропуска нарушителя, %
Вибрационный, проводноволновой и инфракрасный	99,996	0,004
Вибрационный, радиоволновой и инфракрасный	99,996	0,004

Как видно из таблицы 3, вероятность пропуска нарушителя тремя периметральными извещателями меньше, чем при использовании комбинации из двух извещателей. При этом стоит помнить, что и стоимость самой периметральной сигнализации в этом случае возрастает. Поэтому для большинства объектов рекомендуется применять на периметре два извещателя различного принципа действия. Если объект требует особо надежной защиты, например принадлежит к критической информационной инфраструктуре или проникновение на него может привести к глобальной катастрофе, необходимо применять комбинацию из трех извещателей различного принципа действия.

Заключение

Из приведенных выше данных можно сделать выводы, что чем больше рубежей периметральных извещателей различного принципа действия установить на ограждение, тем меньше вероятность проникновения нарушителя на объект. Причем при добавлении одного извещателя вероятность проникновения нарушителя на объект уменьшается на 2 порядка. Однако стоит учитывать и стоимость самого оборудования: необходимо построить достаточно защищенную систему, не превышая разумный бюджет.

При разработке и проектировании важно определить максимально возможную вероятность проникновения нарушителя на объект и оптимизировать систему периметральной сигнализации, исходя из выбранного значения.

В дальнейших предполагается исследовать пропуск извещателями нарушителя при различных погодных условиях, а также при попытках нарушителя замаскироваться от различных извещателей. Данные исследования и расчет вероятностей пропуска нарушителя позволят эффективно размещать и настраивать извещатели периметральной сигнализации, что позволит снизить вероятность пропуска нарушителя.

Также при построении комплексной системы безопасности необходимо учитывать, что помимо рассмотренной в данной работе периметральной сигнализации на объектах связи создается и ряд других систем – система видеонаблюдения, система контроля и управления доступом. Работа систем безопасности в комплексе позволяет снизить вероятность пропуска нарушителя на объект.

Литература

1. Стельмашонок Е. В., Бройдо В. Л., Бугорский В. Н., Буйневич М. В., Васильева И. Н. и др. Безопасность современных информационных технологий. СПб.: СПбГИЭУ, 2012. 406 с.

2. Герлинг Е. Ю., Кулишкина Е. И., Бирих Э. В., Виткова Л. А. Модели нарушителей информационной безопасности // Известия высших учебных заведений. Технология легкой промышленности. 2017. Т 35. № 1. С. 27–30.

3. Буйневич М. В., Покусов В. В., Израилов К. Е. Способ визуализации модулей системы обеспечения информационной безопасности // Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России: Научно-аналитический журнал. 2018. № 3. С. 81–91.

4. Кочетков А. А., Казанцева Я. Ю., Чернышева И. Н. Цифровизация производственных процессов на крупных промышленных предприятиях // Управление качеством. 2022. № 2. С. 22–29.

5. Багринцева О. В., Толстых О. В. Никитина Ю. С. Криминальные и террористические посягательства на потенциально опасные объекты топливно-энергетического комплекса // Охрана, безопасность, связь. 2019. Т. 1. № 4 (4). С. 12–15.

6. Корнев Д., Машера А., Михайловский Н., Чернышева И. Современные технологии в области промышленной безопасности и охраны труда // Главный энергетик. 2022. № 2. С. 65–67.

7. Кривошея Д. Г., Ефименко В. Л. Средства контроля и физической защиты периметра потенциально опасных объектов // Пожарная и техносферная безопасность: проблемы и пути совершенствования. 2020. № 1 (5). С. 368–375.

8. Миняев А. А., Красов А. В. Методика оценки эффективности системы защиты информации территориально-распределенных информационных систем // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 3. С. 26–32. DOI: 10.46418/2079-8199_2020_3_4

9. Извещатели охранные периметровые трибоэлектрические «ГЮРЗА-035ПЗ» и «ГЮРЗА-035ПЗ» исполнение 1. Руководство по эксплуатации. URL: https://www.skichel.ru/images/Docementacia/РЭ_Гюрза_035ПЗ.pdf (дата обращения 20.04.2023)

10. Извещатели охранные линейные для периметров «Импульс-12К». Руководство по монтажу и эксплуатации. URL: https://www.umirs-m.ru/wp-content/uploads/2019/06/RM-Imp-12k-22.12.15-GK-Omega.pdf (дата обращения 20.04.2023)

11. Извещатели охранные линейные радиоволновые двухпозиционные «БАРЬЕР» (общего назначения). Руководство по эксплуатации. URL: https://forteza.ru/files/uploads/Manuals/2022/series%20BARIER/BARIER_RE_2022.09.19.pdf (дата обращения 20.04.2023)

12. Извещатель (прибор) охранный оптико-электронный «МИК-03». Руководство по эксплуатации. URL: https://forteza.ru/files/uploads/Manuals/2019/ МИК/МИК-03_РЭ_2019.11.06.pdf (дата обращения 20.04.2023)

Статья поступила 30 ноября 2023 г.
Одобрена после рецензирования 14 декабря 2023 г.
Принята к публикации 18 декабря 2023 г.

Информация об авторе

Герлинг Екатерина Юрьевна – кандидат технических наук, доцент, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича. E–mail: gerling.eu@sut.ru

Analysis of the Probability of Intruder Penetration into the Facility through the Perimeter

E. Gerling

The Bonch-Bruevich Saint Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Task statement: *ensuring information security, especially at a communication facility, is an urgent task. An important role here is played by the physical security of the object: the inability of the intruder to enter the protected territory undetected. Perimeter alarm is necessary for early detection of attempts to penetrate a communications facility or industrial facility. Information security depends on its effective and reliable work, as well as the protection of the object from a terrorist attack, the preservation of the life and health of people and other important aspects.* ***Purpose:*** *analyze and compare the probabilities of intruder penetration through the fence when using perimeter alarm detectors on the site, based on different principles of operation, as well as when using a combination of these detectors.* ***Results:*** *analyzed the effectiveness of perimeter alarm when using detectors based on different principles of operation, as well as when combining these detectors. The calculations of the probability of the intruder overcoming the fence for the cases considered are also given. The principles of detecting the intruder by perimeter alarm detectors based on various principles of operation have been disassembled. Different principles of operation make it possible to detect different attempts to penetrate, therefore, to increase the security of the object, it is recommended to combine different detectors of perimeter alarm.* ***Practical relevance:*** *study results are used to select and combine different perimeter alarm detectors. They make it possible to increase the likelihood of early detection of penetration into the object by the intruder, which increases the security of the communication object or industrial object. When using the test results, the selection of detectors is justified by mathematical calculations of the probability of the intruder entering the object unnoticed.*

Key words: *perimeter alarm, fencing, probability of intruder penetration, detector, communication object*

Information about Author

Gerling Ekaterina – Ph.D. of Engineering Sciences, Associate Professor. Associate Professor at the Department of Secure Communication Systems (The Bonch-Bruevich Saint Petersburg State University of Telecommunications). E–mail: gerling.eu@sut.ru