DOI: 10.17117/na.2015.09.838

<http://ucom.ru/doc/na.2015.09.838.pdf>

Поступила (Received): 28.09.2015

Теплухин В.А., Соболев А.Н., Давыдов С.А. Некоторые аспекты аналитической модели нарушителя как многоуровневой информационной системы

Tepluhin V.A., Sobolev A.N., Davydov S.A.
**Some aspects of the analytical model of the
offender as a multilevel information system**

Статья посвящена вопросам адаптации аналитической модели нарушителя информационной безопасности в системе информационной безопасности объектов защиты. При всей разнообразности подходов к описанию модели нарушителя ранее не достаточно глубоко рассматривался вопрос описания этой модели как многоуровневой информационной системы

Ключевые слова: защита информации, аналитическая модель нарушителя, многоуровневая система, комплексный подход

Теплухин Владимир Анатольевич
Кандидат технических наук, доцент
Тульский университет
г. Тула, ул. Рязанская, 1

Соболев Александр Николаевич
Кандидат технических наук, доцент
Тульский университет
г. Тула, ул. Рязанская, 1

Давыдов Сергей Александрович
Кандидат технических наук, доцент
Тульский университет
г. Тула, ул. Рязанская, 1

The article is devoted to the adaptation of the offending model of information security system of information security facilities protection. Despite the variety of approaches to the description of model offender has not previously addressed the issue deeply enough to describe this model as a multi-level information system

Key words: protection of information, analytical model of the offender, multi-level, comprehensive approach

Tepluhin Vladimir Anatolievich
Candidate of Engineering Sciences, Associate Professor
Tula university
Tula, Ryazanskaya st., 1

Sobolev Alexander Nikolaevich
Candidate of Engineering Sciences, Associate Professor
Tula university
Tula, Ryazanskaya st., 1

Davydov Sergey Aleksandrovich
Candidate of Engineering Sciences, Associate Professor
Tula university
Tula, Ryazanskaya st., 1

Совершенствование технической оснащенности и способов преодоления рубежей охраны потенциальными нарушителями информационной безопасности приводят к тому, что для обеспечения защиты любого режимного объекта недостаточно просто проанализировать возможные угрозы и выявить каналы возможного выхода информации за пределы объекта [1]. Нужно еще хо-

рошо представлять облик нарушителя для включения его обнаружительных параметров как обязательных элементов комплексной модели информационной безопасности при разработке системы защиты.

Под **аналитической моделью нарушителя** в данной работе понимается совокупность количественных (вес, скорость передвижения, рост и т.п.) и качественных (цели и способы действия, степень осведомленности, подготовленности и т.п.) характеристик нарушителя. Для физического лица, которым является нарушитель, всегда присущи как антропометрические, так и биофизические и биохимические признаки [2].

Попробуем разделить признаки, которые используются для обнаружения нарушителя, применительно к традиционным уровням (рубежам) защиты объекта.

Первым уровнем защиты (или рубежом), как правило, считаются подступы к объекту, или так называемый предупредительный рубеж. Поэтому при моделировании системы защиты данного уровня в первую очередь важны оптические характеристики нарушителя для распознавания на фоне местности, а также антропометрические элементы модели нарушителя, такие, как рост, вес, общие габариты. В последнее время, в связи с широким использованием тепловизионных приборов, сюда можно отнести и его тепловые характеристики.

Вторым уровнем защиты является периметр объекта. Такие средства, как электронно-оптические лучевые, радиолучевые и радиоволновые применяются для блокирования периметров крайне избирательно с доскональным предварительным анализом климатических условий и электромагнитной обстановки.

Рис. 1. Основные информационные признаки нарушителя, используемые при разработке комплексной модели информационной безопасности

Поэтому из элементов модели нарушителя на данном рубеже наибольший вес имеют антропометрические (создание вибраций и одновременных сейсмических колебаний грунта при преодолении заграждений) и магнитные характеристики (инструмент для разрушения ограждений, оружие для возможного воздействия на физическую охрану и т. п.). А вот визуально-оптические уходят с первой позиции, поскольку зачастую сами конструкции ограждения периметров и инженерные заграждения на данном рубеже не позволяют их эффективно использовать для обнаружения нарушителя.

Третий рубеж защиты представляет собой конструкции зданий и сооружений, для оснащения которых наряду с инженерными элементами (укрепление стен, потолков, оконных проемов, дверей и т. п.) применяются различные акустические (звук при разрушении конструкций), и вибрационные системы обнаружения (воздействие на конструкции при разрушении). Широко используются повсеместно визуально-оптические средства (видеокамеры), но эффект от этих средств на территории объекта, особенно при современной плотной застройке еще менее значителен, чем на периметре.

Таблица 1. Категорирование обнаружительных признаков нарушителя применительно к рубежам защиты объекта

Уровень (рубеж) защиты	Расположение объекта	
	В черте населенного пункта	Вне населенного пункта
	признаки обнаружения нарушителя	
1.Подступы к периметру	как правило, рубеж отсутствует	визуально-оптические; сейсмические; антропометрические
2.Периметр объекта	антропометрические; вибрационные; магнитные; сейсмические; радиообнаружительные; визуально-оптические	антропометрические; вибрационные; магнитные; сейсмические; радиообнаружительные; визуально-оптические
3.Здание, сооружение	акустические; антропометрические; визуально-оптические	акустические; антропометрические; визуально-оптические
4.Помещение	тепловые; радиообнаружительные; видеообнаружительные; аутентификационные; визуально-оптические; альфатронные; радиационные	тепловые; радиообнаружительные; видеообнаружительные; аутентификационные; визуально-оптические; альфатронные; радиационные
5.Отдельный предмет	аутентификационные; вибрационные; емкостные; тепловые	аутентификационные; вибрационные; емкостные; тепловые

Поэтому приоритет на данном уровне защиты целесообразно отдать акустическим и антропометрическим характеристикам, а затем уже визуально-оптическим и всем остальным. Прямо-противоположная картина наблюдается

на следующем, **четвертом уровне** защиты, который представляют собой. На данном уровне первое место необходимо отдать тепловым характеристикам нарушителя, а также его непрозрачности и отражательной способности для волн оптического и СВЧ – диапазона. Кроме этого, в силу специфики объектов охраны, немаловажную роль могут играть аутентификационные, радиационные и альфатронные элементы модели. А вот такой элемент модели, как акустический, уходит на данном уровне на нижние позиции, особенно, если лица физической охраны контролируют только территорию объекта снаружи зданий. **Пятый уровень** защиты принято связывать с отдельными интересующими нарушителя предметами – компьютерами, сейфами и т. п. Здесь на передний план выходят аутентификационные признаки, которые нарушитель должен представить системе защиты или обойти эту систему.

Однако немаловажными являются и электрические характеристики нарушителя, поскольку каждый металлический предмет можно использовать в качестве антенны емкостного средства обнаружения. Вибрационные и магнитные характеристики также играют определенную роль, поскольку являются составляющими при воздействии на отдельные предметы.

Таким образом, оптимальное распределение обнаружительных признаков в модели нарушителя, привязанной к уровням защиты объекта охраны, позволит разгрузить комплексную модель информационной защиты путем отдачи приоритетов и тем самым в конечном итоге повысить ее эффективность.

Список используемых источников:

1. Шабуров А.С., Юшкова С.А., Бодерко А.В. Моделирование оценки угроз безопасности информационных систем. Пермский национальный исследовательский политехнический университет. Пермь, 2013.
2. Бузинов А.С., Жигулин Г.П., Шабает Р.И. Моделирование и прогнозирование информационных угроз как составная часть Концепции информационной безопасности РФ // Известия Российской академии ракетных и артиллерийских наук. 2010. № 4(66).
URL: <http://faculty.ifmo.ru/ikvo/MPES/downloads/modinfygr.doc>

© 2015, Теплухин В.А., Соболев А.Н., Давыдов С.А.
Некоторые аспекты аналитической модели
нарушителя как многоуровневой информационной
системы

© 2015, Tepluhin V.A., Sobolev A.N., Davydov S.A.
Some aspects of the analytical model of the offender
as a multilevel information system