Список використаних джерел:

1. Стайкуца С. В. Анализ уровня безопасности современных систем видеонаблюдения / С. В. Стайкуца, А. В. Кочетков, М. Н. Лущан. // Матеріали 72-ї науково-технічної конференції професорсько-викладацького складу, науковців та студентів ОНАЗ ім. О. С. Попова. – 2017. – С. 147-150.
2. Системы аналогового видеонаблюдения высокой четкости: HDCVI, HDTVI и AHD [Електронний ресурс] // Информационный портал Geektimes. – 2015. – Режим доступу до ресурсу: https://geektimes.ru/post/246190/.
3. Стайкуца С. В. Анализ угроз, рисков и уязвимостей современных систем видеонаблюдения / С. В. Стайкуца, С. О. Дігол, К. В. Поліщук. // Матеріали другої науково-практичної конференції «Перспективні напрями захисту інформації». – 2016. – С. 73-76.
4. Стайкуца С. В. Анализ дефиниций понятия видеоаналитика / С. В. Стайкуца, К. С. Седов, В. С. Глушейко. // Сучасні тенденції розвитку науки. Матеріали III Міжнародної науково-практичної конференції. – Херсон : Видавництво «Молодий вчений». – 2018. – С. 48-53.
5. Стайкуца С. В. Анализ типов и критериев оценки систем видеоаналитики / С. В. Стайкуца, К. О. Осадчук, В. Я. Бордан. // Тези доповідей п'ятої міжнародної науково-технічної конференції «Проблеми інформатизації». – 2017. – С. 23-24.

Стайкуца С.В.
кандидат философских наук, доцент;
Лемеха Т.Н.
преподаватель;
Онищенко Н.С., Коваленко В.Д.
студенты,
Одесская национальная Академия связи имени А.С. Попова

ОБОСНОВАНИЕ ВЫБОРА ОПТИМАЛЬНИХ ТЕХНИЧЕСКИХ СРЕДСТВ ОХРАНЫ В СОСТАВЕ СИСТЕМ БЕЗОПАСНОСТИ ОБЪЕКТОВ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Телекоммуникационная сеть – это совокупность компонентов, которые взаимодействуют между собой на ряде уровней. Непрерывность работы элементов телекоммуникационной сети, надежность связей между ними – основа модели оператора связи. По аналогии с моделью OSI стоит отметить роль безопасности телекоммуникационного оборудования, в задачи которого входит обеспечение физического уровня передачи информации.

Как отмечается в [1], угрозы могут быть направлены на структурные элементы сети. К ним относятся информационная сеть компании, здания и сооружения (помещения инфраструктуры), инженерная инфраструктура сети, офисные помещения и персонал. Уровень защищенности каждого здания, сооружения или помещения в целом влияет на непрерывность работы телекоммуникационной сети и на общий уровень безопасности.

По статистике, в течение 10-ти месяцев 2018 года зарегистрировано 16579 криминальных правонарушений по факту кражи имущества мобильных операторов [2]. Так, в «Vodafone Украина» количество правонарушений выросло на 15% в сравнении с 2017 годом. В компании Киевстар отмечают, что количество правонарушений с имуществом оператора вызвало убытков на сумму 1,1 млрд. грн. Динамика краж, представленная в официальных отчетах ПАО «Укртелеком» показывает увеличение количества инцидентов на 412% в период 2014-2017 г., при этом компания ежегодно несет убытки в размере от 250 до 300 млн. грн. [3].

При этом основной проблемой выступает тот факт, что на фоне роста количества правонарушений присутствует низкий% раскрытия дел и фактов наказания преступников. При такой ситуации защита объектов инфраструктуры ложится на плечи операторов связи. Правонарушение всегда проще предотвратить, нежели после расследовать и пытаться компенсировать потери. К тому же, оператор несет не только прямые убытки, связанные с кражей оборудования. К негативным последствиям относятся юридические и репутационные риски, ущерб от потери абонентской базы из-за отсутствия сервиса и т.д. В данном случае действенной мерой защиты может стать применение технических средств охраны (ТСО).

Как отмечается в [4], для защиты оборудования БС применяются системы охранно-тревожной сигнализации, пожарной сигнализации и пожаротушения. В случае, когда кроме охранных функций, необходимо проводить мониторинг состояния оборудования и инженерных систем БС, возможно применение систем удаленного мониторинга состояния систем БС путем контроля более 10-ти функций (контроль и управление ОПС и АСПС, контроль напряжения, состояния датчиков дизель-генератора, показатели климат-контроля и т.д.).

Несомненно, применение указанных ТСО повышает уровень безопасности элементов сети, но при этом стоит помнить, что указанные ТСО не защищают от противоправных действий. Инциденты, которые, к примеру, фиксируются видеокамерами, расследуются уже после совершения правонарушения. Если в нашем случае стоит задача не расследовать, а предотвратить нарушение и действовать превентивно, необходимо закрывать 1-й рубеж, с которым будет взаимодействовать нарушитель – периметр. Из подсистем ТСО такая задача лежит в сфере функционала систем охраны периметра (СОП).

Системы охраны периметра позволят обеспечить контроль периметров территорий, удаленных объектов сети (НРП, БС, места установки антенно-фидерных устройств) и т.д. Классификация СОП обширна и базируется на разных технологиях и методах работы. Как отмечается в [5], при таком многообразии технологий, способов реализации, особенностей проектирования, монтажа и обслуживания систем охраны периметра обоснование выбора должно базироваться на критериях выбора оптимальных решений. При этом выбор оптимального варианта построения СОП осуществляется на основе сравнительного анализа их основных характеристик, к которым относятся эффективность и стоимость. Говоря об эффективности, принимается, что вероятность обнаружения нарушителя системой охраны должна быть

максимальной, а вероятность ложных срабатываний – минимальной. Опираясь на результаты, представленные в [5] видно, что максимальным потенциалом выявления нарушителя при использовании различных способов преодоления периметра обладают сейсмические СОП. Учитывая количество базовых станций (БС) на сетях операторов мобильной связи, распределенную географию размещения, нехватку персонала, статистику краж и хищений применение сейсмических СОП может стать эффективным решением для повышения уровня защиты объектов.

К настоящему времени сейсмические системы охраны периметра производились в 5-ти странах мира: США, России, Израиль, Великобритания и Япония. Сегодня Украина также присоединилась к странам-лидерам с сейсмической системой охраны периметра собственной разработки под названием «Arctium». Среди преимуществ стоит выделить скрытность установки, надежность, вероятность обнаружения нарушителя не ниже 95%, полный контроль территории, возможность применения на разном ландшафте, применение принципа нейронных сетей [6]. Для объективности проведем сравнение популярных методов охраны, которые используются для защиты периметров объектов. Результаты представлены в табл. 1.

Таблица 1

Сравнение способов охраны периметров объектов по базовым критериям

	Системы видеонаблюдения	**Извещатели Optex**	**СОП Arctium**
Скрытность установки	нет	нет	да
Возможность использования без инженерных конструкций	нет	нет	да
Независимость от погодных условий (туман, снег, время суток и т.д.)	нет	нет	да
Превентивность (раннее обнаружение)	частично	нет	да
Защита от повреждений	нет	нет	да
Определение конкретно человека, а не просто абстрактный объект	нет	нет	да
Контроль территории, а не только линейного участка	да	нет	да
Точность локации нарушителя	В зависимости от ТТХ камеры, правильности монтажа, погодных условий и т.д.	В рамках секции между оптическими датчиками, в среднем – 30 метров	5 метров
Независимость от растительности на участке	нет	нет	да

Как отмечалось выше, к базовым характеристикам СОП относятся эффективность и стоимость. Сравнение стоимости разных типов систем охраны периметра, в том числе – и с детализацией по сейсмическим системам охраны, представлено на рис. 1. Стоит отметить, что при использовании систем охраны периметра с наземным типом установки датчика следует дополнительно учесть стоимость построения ограждения.

Применение систем охраны периметра в системе безопасности объектов, в том числе – входящих в инфраструктуру телекоммуникационных компаний, дает возможность оперативного реагирования на инциденты, добавляет к общей системе безопасности функцию превентивности и оптимальна по базовым характеристикам.

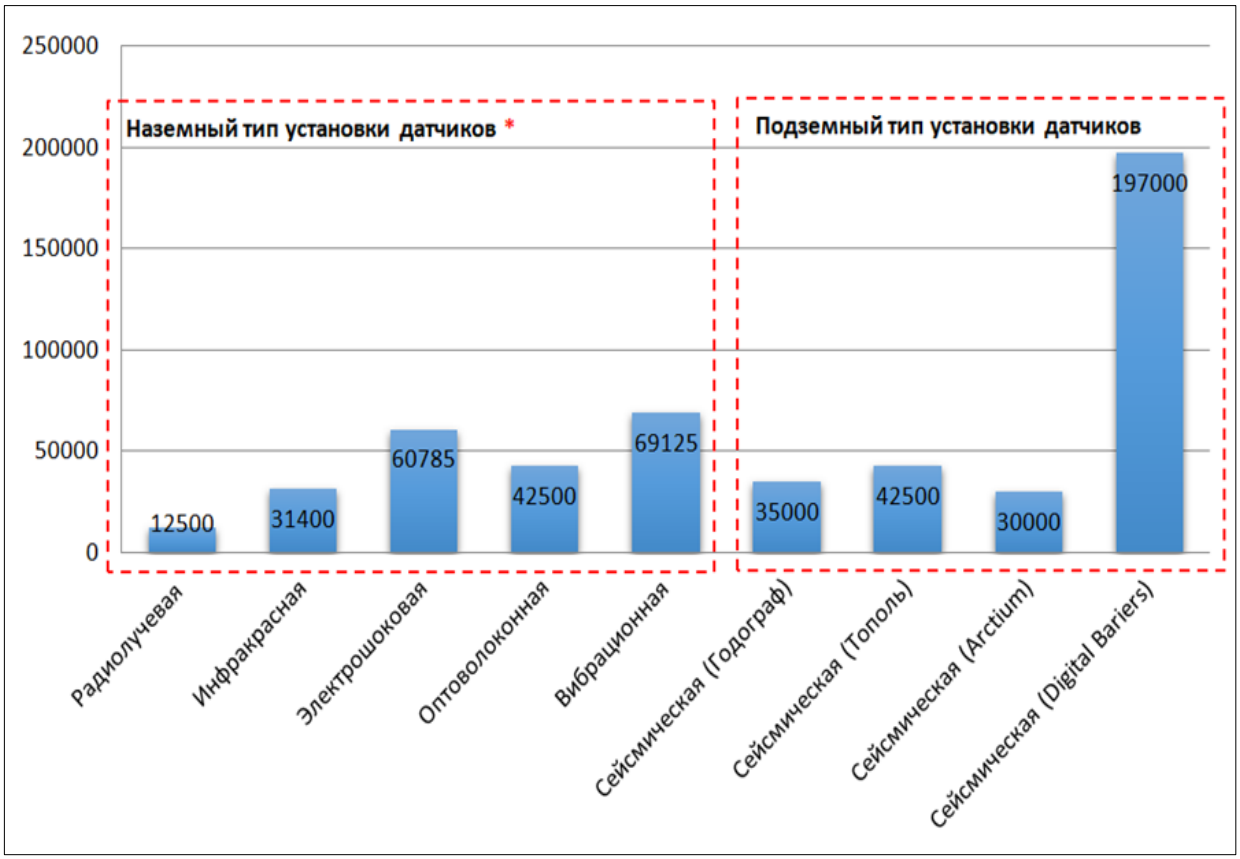

Рис. 1. Сравнение стоимости СОП для периметра протяженностью в 1000 метров

Список использованных источников:

1. Стайкуца С. В. Аналіз загроз безпеки телекомунікаційних компаній з розробкою методології захисту / С. В. Стайкуца, О. О. Семенов. // Науково-практична конференція «Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS'2016). – 2016. – С. 63–67.

2. Нацполіція повідомила про 16 000 крадіжок майна мобільних операторів з початку року в Україні [Електронний ресурс] // Mind. – 2018. – Режим доступу до ресурсу: https://mind.ua/news/20191294-nacpoliciya-povidomila-pro-16-000-kradizhok-majna-mobilnih-operatoriv-z-pochatku-roku-v-ukrayini.

3. Вергун Д. Диверсии конкурентов: за порезанные интернет-провода заплатят абоненты [Електронний ресурс] / Денис Вергун // Finance.ua. – 2017. – Режим доступу до ресурсу:

https://news.finance.ua/ru/news/-/412080/diversii-konkurentov-za-porezannye-internet-provoda-zaplatyat-abonenty

4. Стайкуца С. В. Применение технических средств охраны для повышения уровня защищенности объектов телекоммуникационных сетей / С. В. Стайкуца, И. А. Киреев, Д. В. Великий. // Теорія і практика сучасної науки. – 2017. – С. 33–37.

5. Стайкуца С. В. Анализ и обоснование выбора периметральных систем охраны / С. В. Стайкуца, С. А. Дигол, К. С. Седов. // Сборник тезисов третьей всеукраинская научно-практическая конференция «Перспективные направления защиты информации», ОНАС им. А.С. Попова. – 2017. – С. 72–76.

6. Система охраны раннего обнаружения Arctium [Електронний ресурс] // Корпоративный сайт компании «Гофер». – 2018. – Режим доступу до ресурсу: http://www.arctium.gofer.ua.