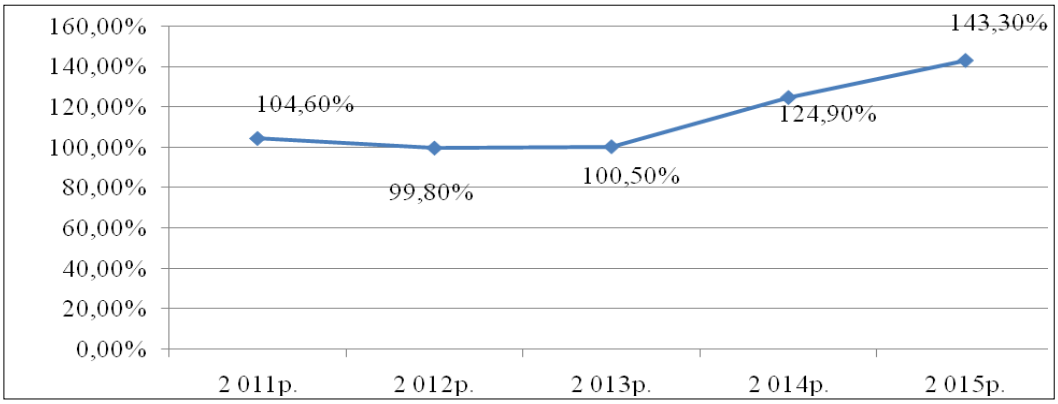

Рис. 6. Індекс інфляції в Україні за 2011–2015 рр.

Список використаних джерел:

1. Мунтіян В.І. Економічна безпека України / В.І. Мунтіян. – К. : КВІЦ, 1999. – 464 с.
2. Пономаренко В.С. Экономическая безопасность региона: анализ, оценка, прогнозирование / В.С. Пономаренко, Т.С. Клебанова, Н.Л. Чернова – Харьков; НД «ИНЖЕК», – 2004. – 144с
3. Ризики і загрози фінансовій безпеці сектору державних фінансів та шляхи їх подолання / О.С. Білоусова, В.І. Гаркавенко, А.І. Даниленко та ін. – К.: ДННУ «Аналіз фінансового управління», 2013. – 308 с.
4. Офіційний сайт державної служби статистики України Електронний ресурс]. – Офіційний сайт Верховної ради України. – Режим доступу: http://www.ukrstat.gov.ua
5. Методичні рекомендації щодо розрахунку рівня економічної безпеки України, затверджені наказом Міністерства економічного розвитку і торгівлі України від 29 жовтня 2013 року № 1277 України [Електронний ресурс]. – Режим доступу: http://search.ligazakon.ua/l_doc2. nsf/link1/ ME131588. html.

Стайкуца С.В.
кандидат философских наук, доцент;
Киреев И.А.
кандидат технических наук, доцент;
Великий Д.В.
студент,
Одесская национальная академия связи имени А.С. Попова

ПРИМЕНЕНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ ОХРАНЫ ДЛЯ ПОВЫШЕНИЯ УРОВНЯ ЗАЩИЩЕННОСТИ ОБЪЕКТОВ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Как отмечается в [1], телекоммуникационная сеть (Telecommunication Network) – это системообразующая совокупность средств телекоммуникаций, предоставляющая территориально разнесенным объектам возможность информационного взаимодействия путем обмена сигналами. Работоспособность всех элементов телекоммуникационной сети и связей между ними – основа бизнес-модели оператора связи/провайдера, его репутация и конкурентоспособность. Поэтому повышение уровня безопасности элементов телекоммуникационной сети является важным звеном при формировании процессов с позиции непрерывности бизнеса.

В рамках телекоммуникационной компании угрозы могут быть направлены на разные структурные элементы сети. Так, согласно [2], к ним относятся непосредственно информационная сеть компании, здания и сооружения (помещения инфраструктуры), инженерная инфраструктура сети, офисные помещения и персонал. Рассматривая более детально помещения инфраструктуры, авторы выделяют центры мониторинга и реагирования на инциденты, помещения ЦАТС и ЦОД, сайты базовых станций, электрических подстанций и генераторных, стационарные посты охраны и т.д. Уровень защищенности каждого здания, сооружения или помещения в целом влияет на непрерывность работы телекоммуникационной сети и на общий уровень безопасности. В зависимости от уровня подготовки злоумышленника и его мотивов деструктивные действия могут быть направлены и на остальные, приведенные выше, группы. Общий перечень угроз в телекоммуникациях более детально представлен в рамках международной рекомендации ITU-T E.408 [3].

Формирование общей концепции безопасности телекоммуникационной сети включает в себя разные подсистемы защиты, к которым относятся организационная составляющая, ТЗИ и криптография, кибербезопасность и технические средства охраны (ТСО) и т.д. Рассмотрим детальнее направление ТСО.

Как отмечается в [4, с. 7], под техническими средствами охраны понимается система раннего обнаружения угроз фирме от стихийных бедствий, несанкционированного проникновения нарушителей и ошибочных либо неправомерных действий обслуживающего персонала или клиентов. Другие источники определяют ТСО как это совокупность аппаратных и программных средств, обеспечивающих контроль, сохранность и противопожарную безопасность территории, помещений, хранилища и др. объектов и субъектов контроля. В базовом составе ТСО включают в себя:

- системы охранно-тревожной сигнализации;
- системы пожарной сигнализации и оповещения о пожаре;
- системы пожаротушения;
- системы охранного телевидения (видеонаблюдения);
- системы контроля и управления доступом;
- системы охраны периметра.

Учитывая тот факт, для эффективного обнаружения нарушителя необходимо учитывать фактор раннего обнаружения, первоочередное задание по выявлению нарушителя полагается на системы охраны периметра (СОП), как на первый рубеж. Такие системы позволяют контролировать периметры территорий, удаленные объекты сети (НРП, базовые станции, места установки антенно-фидерных устройств) и т.д. Классификация СОП обширна и базируется на разных технологиях и методах работы. Выбор типа системы охраны периметра базируется на ряде факторов, предварительно описанных в техническом задании на проектирование. Учитываются такие критерии, как температурный диапазон, вероятность ветров и осадков, требования к маскировке, возможность установки ограждения, растительность и т.д. Помимо указанных выше факторов, необходимо учитывать критерий эффективности СОП. Говоря об эффективности, принимается, что вероятность обнаружения нарушителя системой охраны должна быть максимальной, а вероятность ложных срабатываний – минимальной. Опираясь на результаты, представленные авторами в работе [5] видно, что максимальным потенциалом выявления нарушителя при использовании различных способов преодоления периметра обладают сейсмические СОП. Стоит отметить сейсмическую систему охраны украинского производства «Арктиум». Система имеет целый ряд уникальных возможностей и позиционируется разработчиком как система охраны периметра и территорий [6]. Учитывая количество базовых станций (БС) на сетях операторов мобильной связи, большую территорию их

размещения, недостаток персонала, случаи краж и хищений применение системы «Арктиум» может стать эффективным решением для повышения уровня защиты БС и иных удаленных объектов телекоммуникационных сетей.

Также для защиты оборудования базовых станций на практике применяются системы охранно-тревожной сигнализации, пожарной сигнализации и пожаротушения. Малые габариты помещения сайта БС не требуют большого количества датчиков и модулей пожаротушения. Стоит отметить, что системы пожарной сигнализации и пожаротушения должны быть обязательно сертифицированы, а все направление АСПС и АСПТ в целом находится под контролем действующего законодательства Украины. Такие документы, как ДСТУ-Н CEN / TS 54–14:2009, ДБН В.2.5–56:2014 и др. регламентируют направление противопожарной защиты на всей длине «жизненного цикла», от проектирования до подключения к ПЦН. В случае, когда кроме охранных функций, дополнительно необходимо проводить мониторинг состояния оборудования и инженерных систем БС, возможно применение систем удаленного мониторинга состояния систем БС. Система выполняет более 10-ти функций, к которым относятся контроль и управление ОПС и системой автоматического пожаротушения, контроль напряжения, состояния датчиков дизель-генератора, показатели климат-контроля и т.д.

Помимо базовых станций, высокий уровень требований к безопасности предъявляется к помещениям ЦАТС и ЦОД, где расположено основное оборудование управления сетью. В [7] авторами на примере помещений опорного узла связи мобильной связи рассмотрен вариант применения внесистемных средств мониторинга состояния ЦАТС – автоматической системы пожарной сигнализации (АСПС), автоматической системы пожаротушения (АСПТ) и системы контроля доступа (СКУД). Размещение элементов АСПС представлено на рис. 1

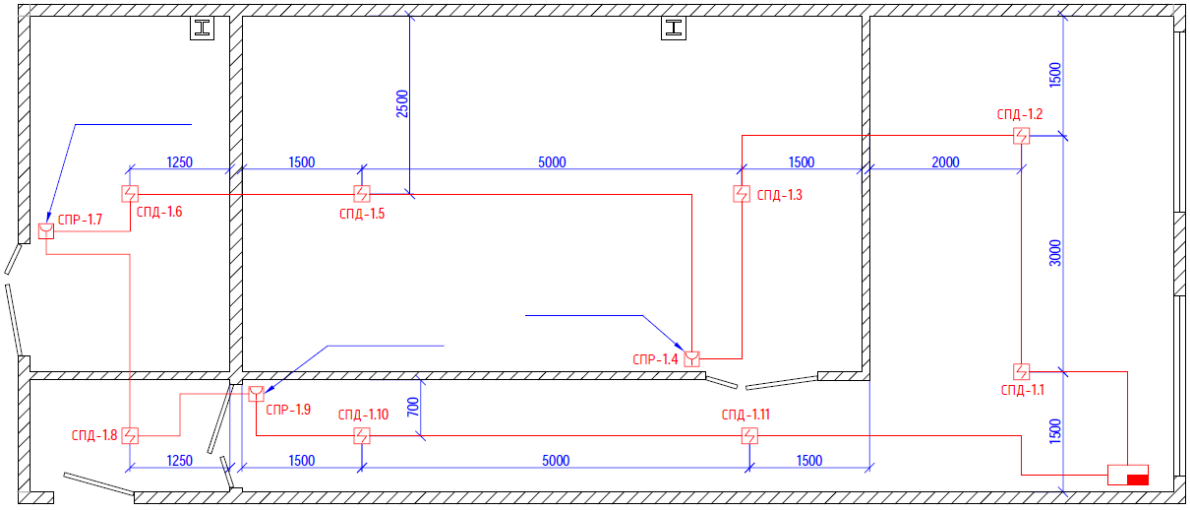

Рис. 1. Размещение элементов автоматической системы пожарной сигнализации на примере помещений опорного узла связи мобильной связи

Также стоит отметить серьезную проблематику защиты кабельных линий от вторжения и воровства. Каждый год рынок коммуникаций сталкивается с ситуациями, основой которых выступают кражи и вандализм. Возникающий ущерб включает в себя расходы на ремонтно-восстановительные работы, недополучение прибыли в связи с невозможностью предоставления услуг, негативную реакцию со стороны общественности, отток клиентской базы и т.д. Так, 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. [8]. От данной проблемы также несут

убытки множество операторов и провайдеров меньшего масштаба. Решением проблемы может стать применение систем сигнализации на люках кабельной канализации, использование сейсмических систем охраны (как отдельно, так и в условиях интеграции со сторонними системами безопасности), а также применение волоконно-оптических систем защиты и контроля (СЗК).

Список використаних джерел:

1 Сучасні телекомунікації: мережі, технології, безпека, економіка, регулювання, Довгий С. О., Воробієнко П. П., Гуляєв К. Д., за загальною редакцією члена-кореспондента НАН України Довгого С. О., Київ «Азимут-Україна», 607 ст., 2013 р.

2 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.

3 Рекомендація ITU-T E.408 Telecommunication networks security requirements.

4 Дворский М. Н. Техническая безопасность объектов предпринимательства / М. Н. Дворский, С. Н. Палатченко. – Киев: А-ДЕПТ, 2006. – 304 с. – (Концепции безопасности).

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 Дігол С. О. Підвищення ефективності захисту державного кордону України на основі СОП «Арктиум» / С. О. Дігол, М. І. Лисий, С. В. Стайкуца. // Збірник тез X Всеукраїнської науково-практичної конференції «Освітньо-наукове забезпечення діяльності складових сектору безпеки і оборони України», Національна академія ДПСУ ім. Б. Хмельницького. – 2017. – С. 564–566.

7 Кононович В. Г., Стайкуца С. В., Лемеха Т. М., Копитін Ю. В.// Інформаційна безпека цифрових програмно-керованих АТС // Навчальний посібник для студентів вищих навчальних закладів ОНАЗ ім. О. С. Попова. – Одеса, 2013. – 242 с.

8 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