УДК 004. 056

ЗАЩИТА ИНФОРМАЦИИ В ОБЛАКАХ ПО РЕЗУЛЬТАТАМ МОНИТОРИНГА ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Прузан А.Н., Николаенко В.Л.

DOI: 10.12737/15395

Аннотация. Для уменьшения расходов на защиту информации в облачных вычислениях предлагается по результатам автоматизированного мониторинга небезопасных событий (инцидентов информационной безопасности) в облаках выделить наиболее часто встречающиеся инциденты, и разработку собственных программных средств защиты информации или внедрение необходимых организационных мероприятий вести только для парирования угроз, вызывающих наиболее часто встречающиеся инциденты.

Ключевые слова: информационная безопасность, мониторинг, инцидент, облачные вычисления.

Концепция облачных вычислений позволяет заказчику заменить собственные вычислительные ресурсы потребляемыми из облака. Главным преимуществом данной концепции является отсутствие у заказчика затрат на установку и поддержку собственных вычислительных ресурсов. Однако информация в облаках нуждается в защите [1-5]. Для неё обычно приобретаются или разрабатываются собственные программные средства защиты информации (ПС ЗИ) в облаках или разрабатываются и внедряются необходимые организационные мероприятия. Однако стоимость приобретения, разработки или внедрения может быть неподъёмной для предприятия.

Для уменьшения этой стоимости в докладе предлагается по результатам автоматизированного мониторинга небезопасных событий (инцидентов информационной безопасности, ИБ) в облаках выделить наиболее часто встречающиеся инциденты, и разработку собственных ПС ЗИ или внедрение необходимых организационных мероприятий вести только для парирования угроз, вызывающих наиболее часто встречающиеся инциденты.

Пример сделанного предложения. На предприятии, использующем облачные вычисления, результаты проведенного с помощью продукта SkyHigh компании Salesforce.com (рис. 1) мониторинга инцидентов ИБ в модели SaaS

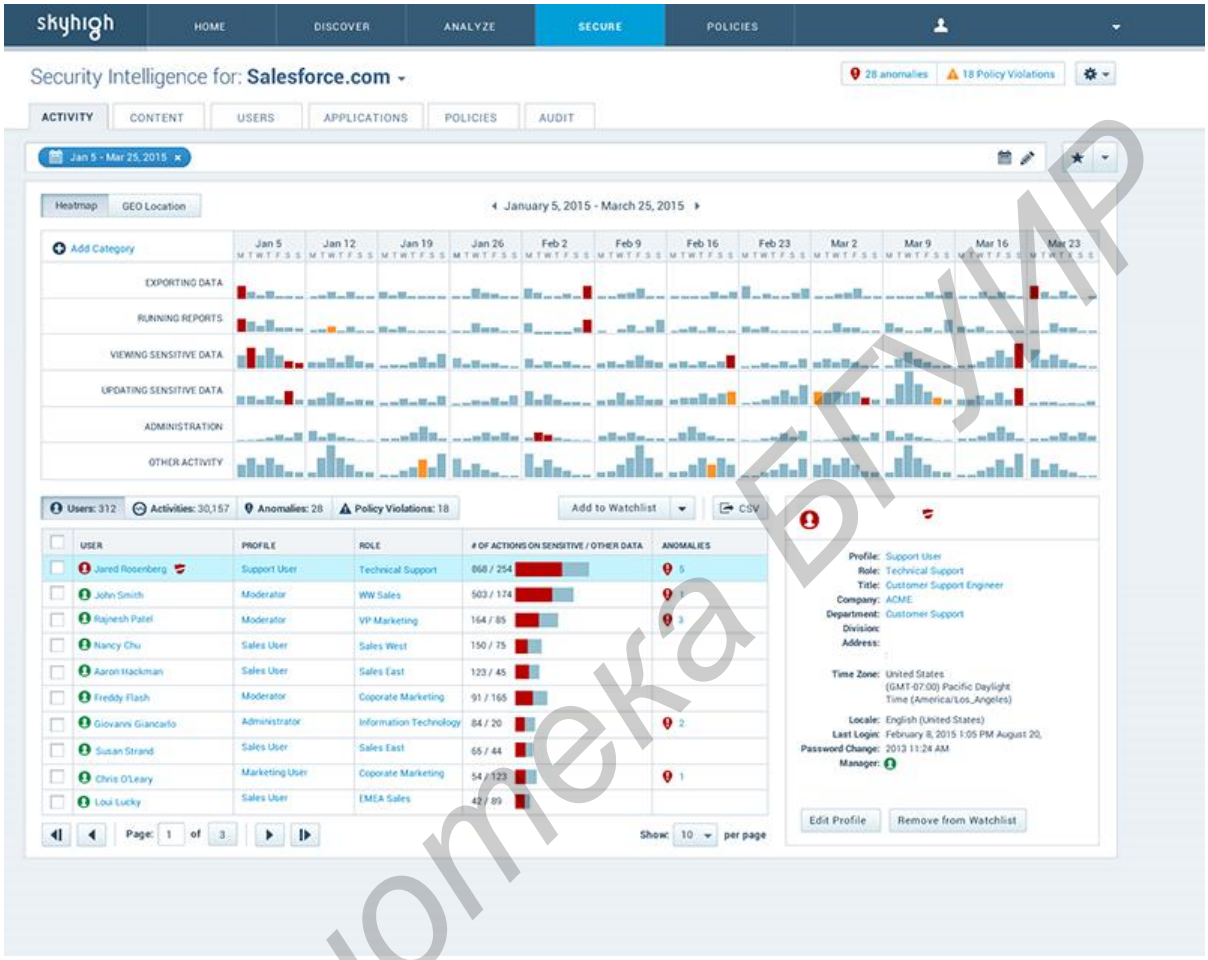

Рисунок 1 – Окно программного продукта SkyHigh

показали, что наиболее значимой причиной возникновения инцидентов в течение 2014 года стала угроза от уволившихся сотрудников: часть сотрудников, покинувших или потерявших свои рабочие места, долго могут держать у себя конфиденциальные корпоративные данные и использовать их на своих новых рабочих местах.

Для парирования этой угрозы в политику безопасности предприятия в 2015 году следует внести изменения, которые позволят предприятию сократить инцидентов ИБ, вызванных вышеуказанной угрозой.

Список литературы

1. Николаенко В.Л., Прузан А.Н., Сечко Г.В., Таболич Т.Г. Опыт мониторинга инцидентов информационной безопасности в облачных вычислениях // Сб. статей III межд. заоч. НПК «Информационные системы и технологии: управление и безопасность» (декабрь 2014). – Тольятти-Русе: Поволжский гос. университет сервиса в партнёрстве с Русенским университетом «Ангел Кънчев» (Болгария), 2014. – 345 с. – С. 209-215.

2. Прузан А.Н., Николаенко В.В. Парирование угроз информационной безопасности в облаках // Современные средства связи: материалы XVIII Междунар. науч.-техн. конф., 15–16 окт. 2013 года, Минск, Респ. Беларусь / редкол.: А. О. Зеневич [и др.]. – Минск: УО ВГКС, 2013. – 322 с. – С. 176-177.

3. Прузан А.Н., Николаенко Е.В., Таболич Т.Г. Программное средство для защиты информации в облаках // Материалы XX МНТК «Информационные системы и технологии» (ИСТ–2014), Нижний Новгород (18 апреля 2014 г.). – Нижний Новгород: Нижегородский государственный технический университет им. Р.Е. Алексеева, 2014. – С. 268.

4. Прузан А.Н., Николаенко Е.В., Таболич Т.Г. Угрозы и атаки на облачные сервисы компании ANP // Материалы XXI МНТК «Информационные системы и технологии» (ИСТ–2015), Нижний Новгород (17 апреля 2015 г.). – Нижний Новгород: Нижегородский государственный технический университет им. Р.Е. Алексеева, 2015. – С. 309.

5. Прузан А.Н., Николаенко Е.В., Тихонов А.В. Приоритизация инцидентов информационной безопасности в облаках // Технические средства защиты информации: Тезисы докладов XIII Белор.-российск. НТК (Минск, 4–5 июня 2015 г.). – Мн.: БГУИР, 2015. – 100 с.– С. 39-40.

Прузан Андрей Николаевич, аспирант 1 года обучения кафедры защиты информации Белорусского государственного университета информатики и радиоэлектроники, г. Минск, Беларусь

Научный руководитель - Николаенко Владимир Лаврентьевич, кандидат технических наук, доцент, заместитель директора по учебной работе Института информационных технологий Белорусского государственного университета информатики и радиоэлектроники, г. Минск, Беларусь