Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

жений, ИТ-специалисты, подготавливающие образы ОС для их запуска в сервисной инфраструктуре. В этой модели могут быть запущены практически любые приложения, установленные на стандартные образы.

Теперь, исходя из выше изложенного, сформулируем некую исходную концептуальную схему, то есть **парадигму безопасности**, которая, в свою очередь, формирует модель злоумышленника и далее политику безопасности, которая должна найти отражение в нормативных документах на рассматриваемую технологию облачных вычислений. Предлагаемую парадигму изложим в виде некоторых постулатов, базирующихся на опыте реализации задач по созданию и обеспечению успешного функционирования конкретных систем информационной безопасности облачных вычислений, на анализе трудностей, о которых сказано ранее, на устранении противоречий, имеющихся в действующем подходе к решению этой весьма сложной проблемы, а главное – в получении эффекта, заметного для провайдера и пользователя и экономически ощутимого.

Далее в докладе рассматриваются постулаты безопасности, которые представляют собой кратко структурированные положения политики безопасности рассматриваемой информационной технологии.

СИСТЕМЫ МОНИТОРИНГА СОСТОЯНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В.А. ДМИТРИЕВ, А.Б. СТЕПАНЯН, А.В. АФАНАСЬЕВ, Е.П. МАКСИМОВИЧ

Объединенный институт проблем информатики НАН Беларуси

В настоящее время все больше внимания уделяется обеспечению безопасности информации как в крупных учреждениях и компаниях, так и в средних и малых организациях. Защищаемые объекты имеют различные уровни доступа, всевозможные варианты развертывания вычислительных сред и разнообразные топологии сетевого взаимодействия.

Актуальной проблемой является проблема обнаружения и локализации вредоносной информации, находящейся внутри корпоративных сетей. Также растут количество и разнообразие информационных атак на ресурсы информационных систем.

Способы проникновения вредоносной информации в корпоративные информационные системы также стремительно модифицируются, что делает процесс нахождения вредоносной информации более трудоемким и требующим применения различных средств защиты информации.

В современных вычислительных сетях и информационных системах обычно используется большое количество разнородных средств защиты информации. Межсетевые экраны, системы обнаружения вторжений, сетевые устройства, операционные системы, антивирусы, базы данных, различные приложения генерируют огромное количество событий безопасности. Журналы событий каждого компонента хранятся отдельно, и вручную найти и сопоставить необходимую информацию для определения инцидентов информационной безопасности крайне сложно. Вместе с сигналами об активности злоумышленников от средств защиты информации поступает огромное количество ложных сигналов, что еще больше снижает эффективность работы сотрудников сетевой безопасности. При этом ответные действия на угрозы безопасности должны быть предприняты немедленно.

Интенсивность информационного обмена, сложность современных алгоритмов обработки информации, разнообразие угроз и средств защиты от них обусловливают необходимость применения разнообразных автоматизированных средств и систем для решения задач обеспечения информационной безопасности.

Одним из современных подходов к решению задач защиты информации информационных систем является внедрение SIEM-технологии. Основной функцией SIEM-систем является анализ информации, поступающей от разных источников. На основе анализа данных из этих источников выявляются отклонения от нормального функционирования, заданного критериями безопасности, и в случае обнаружения происходит оповещение администратора безопасности.

SIEM-система используется для: анализа информации, поступающей от различных источников; предоставления доказательной базы при расследовании инцидентов информационной безопасности; предоставления структурированной информации, необходимой при аудите информационной безопасности; обеспечения непрерывности работы сервисов путем обнаружения сбоев в их работе; структуризации информационно-телекоммуникационной системы.

SIEM-система выявляет следующие события и инциденты информационной безопасности: сетевые атаки во внутреннем и внешнем периметрах; вирусные эпидемии или отдельные вирусные заражения; попытки несанкционированного доступа к информации ограниченного распространения; мошенничества; ошибки и сбои в работе информационных систем; уязвимости; ошибки конфигурации в средствах защиты и информационных системах; целевые атаки.

Основными задачами обеспечения информационной безопасности, которые ставятся перед SIEM-системой, как правило, являются следующие:

централизованное хранение журналов событий;

обработка и корреляция событий;

оповещение об инцидентах; расследование инцидентов; управление инцидентами (инцидент-менеджмент).

Результат применения SIEM-систем:

повышение уровня защищенности информационной инфраструктуры за счет оперативной реакции на инциденты информационной безопаснсоти;

ускорение и автоматизация процесса идентификации и последующего расследования инцидентов;

централизованный подход к задачам обработки и хранения событий информационной безопасности.

Благодаря использованию SIEM-систем значительно снижается время реагирование на атаки, а, следовательно, и экономические затраты на восстановление системы.

ИДЕНТИФИКАЦИЯ УЧАСТНИКОВ СОЦИАЛЬНОЙ СЕТИ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

И.А. ИВАНОВА, А.В. КОБЗАРЬ

ФГБОУ ВО «Московский технологический университет»

Социальные сети – это многофункциональный сетевой ресурс, который привлекает к себе всё больше внимания самых разных структур, поскольку охватывает огромную аудиторию пользователей и имеет большую долю влияния, чем какое-либо другое средство массовой информации. Кроме того, мониторинг социальных сетей позволяет отследить