DOI: 10.17117/na.2015.07.560

Поступило в редакцию: 15.07.2015

<http://ucom.ru/doc/na.2015.07.560.pdf>

Алексанян А.П., Пестов И.Е.

Система мониторинга состояния информационной безопасности в ключевых системах информационной инфраструктуры

Aleksanyan A.P., Pestov I.E.

The system of monitoring the state of the information security systems in key information infrastructure

Статья посвящена анализу мониторинга информационных систем. Показана примерная разработка методики выбора программно-технических средств мониторинга состояния информационной безопасности в ключевых системах информационной инфраструктуры. Также, даны рекомендации по организации и проведению мониторинга состояния информационной безопасности в ключевых системах информационной инфраструктуры

This article analyzes the monitoring information systems. It shows an exemplary development of procedures for the selection of software and hardware monitoring of the state of information security systems in key information infrastructure. Also, the recommendations on the organization and monitoring of the state of information security systems in key information infrastructure

Ключевые слова: информационная безопасность, мониторинг, ключевые системы информационной структуры

Key words: information security, monitoring, key system information structure

Алексанян Андрей Павлович

Бакалавр

Государственный университет морского и речного флота им. С.О. Макарова

г. Санкт-Петербург, ул. Двинская, 7

Aleksanyan Andrey Pavlovich

Bachelor

State university of marine and river fleet named S.O. Makarov

St. Petersburg, Dvina st., 7

Пестов Игорь Евгеньевич

Магистр, ассистент кафедры

Санкт-Петербургский государственный университет телекоммуникаций им. Бонч-Бруевича

г. Санкт-Петербург, пр. Большевиков, 22/1

Pestov Igor Evgenievich

Master, Assistant

St. Petersburg state university of telecommunications named Bonch-Bruevicha

St. Petersburg, pr. Bolsheviks, 22/1

В настоящее время информационные технологии (ИТ) активно развиваются и широко распространяются во всем мире и во всех сферах деятельности человечества.

С развитием ИТ растет и количество угроз, способных нанести непоправимый ущерб той или иной информационной системе (ИС).

Наиболее важными ИС в РФ принято считать ключевые системы информационной инфраструктуры (КСИИ), так как последствия деструктивного воздействия на нее могут нанести непоправимый ущерб населению и государству в целом. Следовательно, чтобы избежать подобных последствий, информацию, хранящуюся или обрабатываемую в КСИИ нужно защищать.

Чтобы понять, насколько правильно и эффективно построена и проводится защита информации в КСИИ, нужно проводить мониторинг состояния информационной безопасности (ИБ). Это позволит представить полную картину состояния защищенности КСИИ.

Основным признаком КСИИ является наличие в системе критически важного объекта (КВО). На территории РФ находится более 4,5 тысячи КВО. Большинство из них размещено в густонаселенных районах, в пределах крупных городов и населенных пунктов. На европейской части России (в Северо-Западном, Центральном, Южном, Северо-Кавказском и Приволжском федеральных округах) сосредоточено 75% всех КВО. Более четверти из них (25,57%) размещено в центральной России.

КСИИ в России признаются системы, формируемые КВО, нарушение штатного режима функционирования которых способно нарушить функции управления важными для РФ процессами.

Особенности КСИИ представлены на рисунке 1.

Рис. 1. Особенности КСИИ

К основным особенностям КСИИ относят следующие:

1) критически важная информация, обрабатываемая в КСИИ, как правило, не относится к информации ограниченного доступа, защита которой регламентируется действующими нормативными документами;

Защита КВО, связана, в основном, с обеспечением ее целостности и доступности.

2) в КСИИ может применяться как типовое системное программное обеспечение (ПО), так и специальное ПО, выполняющее специфическую обработку технологической информации;

К типовым системным ПО относятся:

- операционные системы (ОС) общего применения;
- системы управления базами данных (БД);
- текстовые и графические редакторы и другие.

К специальным ПО относят такие системы, как:

- ОС реального времени;
- специальные программы управления различными приборами и системами.

3) КСИИ могут быть связаны в единую сеть с другими системами и объектами информационной инфраструктуры страны, в том числе относящимися к различным министерствам и ведомствам;

4) в КСИИ в большинстве случаев используется аппаратное обеспечение, разработанное только для данной КСИИ и не используемое в других системах;

В частности, это могут быть измерительные датчики и системы.

5) многие функционирующие КСИИ обеспечивают управление непрерывными технологическими процессами и не могут быть отключены на период проведения контрольных мероприятий;

6) характер последствий:

- нарушение государственного или военного управления;
- катастрофы с гибелью населения;
- экологический ущерб;
- экономический ущерб в национальном масштабе;
- ущерб престижу страны;
- финансовый, социальный кризис.

Сделаем под итог, информация, входящая в состав КСИИ не зависимо от степени ее конфиденциальности является важной и ее нужно защищать. Для того, чтобы эта информация была всегда под защитой, методы этой защиты нужно постоянно совершенствовать, так как многие зарубежные государства, а также террористические и криминальные структуры интенсивно совершенствуют методы и способы использования информационных технологий (ИТ) и средств для деструктивных информационных воздействий на информационные ресурсы информационных систем (ИС) и сетей государственных и негосударственных организаций. Применение ИТ для деструктивных воздействий придает им свойства, так называемого информационного оружия. Для нанесения значительного ущерба интересам государства и общества информационное оружие может быть применено и в мирное время, особенно террористическими организациями.

В состав информационно-измерительной, информационно-исполнительной подсистем, а также подсистемы внешнего управления входит подсистема передачи данных, отвечающая за транспортировку технологической информации. Через сетевые интерфейсы этой подсистемы различные компоненты КСИИ взаимодействуют с каналами передачи данных, которые

представляют собой совокупность различных сред распространения сигнала (электропроводящие, оптоволоконные кабели, радиоэфир), а также транзитных сетевых устройств (узлов), решающих задачи ретрансляции, коммутации, маршрутизации при передаче данных.

КСИИ очень сложная и разветвленная система, в которой все элементы взаимосвязаны. КСИИ функционирует как большой механизм, в котором каждая деталь важна и непременно взаимосвязана с остальным, например, вместе с ростом количества средств защиты существенно увеличивается и объём информации, которую должен обработать администратор безопасности. Это в свою очередь приводит к увеличению времени, которое должен тратить оператор для анализа всей информации, поступающей от различных средств защиты для принятия адекватных решений по реагированию на выявленные атаки.

Для повышения эффективности принятия решений по реагированию на события, связанные с нарушением безопасности рекомендуется использовать специализированные системы мониторинга, которые могут автоматизировать процесс сбора и анализа информации, поступающей от различных средств защиты. В данный момент, можно утверждать, что мониторинг ИБ – один из основных процессов ИБ в КСИИ. Правильно спроектированный, настроенный и отлаженный мониторинг является основным источником информации о реальной уровне ИБ в КСИИ. В настоящее время средства мониторинга состояния ИБ объединяют в группу систем мониторинга управления информацией и событиями безопасности – SIEM (Security Information and Event Management) системы.

SIEM – это система сбора и корреляции событий. Важно понимать, что SIEM-системы в качестве самостоятельного решения не предназначены и не способны предотвращать инциденты нарушения ИБ. Их суть заложена в их названии: анализ информации, поступающей из различных источников, и дальнейшее выявление отклонений от норм по заданным критериям.

Рис. 2. Типовая структура системы мониторинга ИБ

Для общего представления работы системы мониторинга, рассмотрим типовую структуру системы мониторинга ИБ, которая показана на рисунке 2.

Нужно учитывать, что контроль работоспособности и защищенности только аппаратных средств недостаточен для представления полной картины состояния защищенности всей КСИИ. Для этого мониторинг состояния защищенности должен проводиться в комплексе, в частности, немаловажным является проведение мониторинга парольной защиты.

Правильная организация и проведение мониторинга парольной защиты позволит предупредить и максимально исключить возможность доступа в систему несанкционированного пользователя или злоумышленника. Полноценный мониторинг парольной защиты в большей своей части зависит от правильной работы с персоналом, информирование его об ответственности за разглашение или утраты пароля.

Мониторинг состояния парольной защиты является важным, но зачастую не достаточным для контроля состояния защищенности всей КСИИ. Одной из важнейших составляющих системы мониторинга состояния ИБ в КСИИ является мониторинг попыток НСД к защищаемой информации.

Оперативность выявления попытки НСД является главной задачей мониторинга состояния ИБ в КСИИ.

Важно учитывать все обстоятельства, связанные с попыткой НСД к защищаемой информации, чтобы можно было определить источник и причины подобных угроз. Это делается для того, чтобы в дальнейшем избежать подобных инцидентов.

Таким образом, с развитием ИТ совершенствуются и угрозы, которые могут оказать негативное воздействие на КСИИ. Для того чтобы избежать негативных последствий вследствие деструктивных воздействий на информацию, которая подлежит защите, нужно развивать и совершенствовать средства защиты информации от этих угроз.

Была разработана методика выбора минимально-необходимого состава средств мониторинга состояния ИБ в КСИИ. В ходе выбора наиболее подходящей для типовой КСИИ была признана система мониторинга ИБ IBM Qradar SIEM.

В работе были разработаны основные рекомендации по организации и проведению мониторинга аппаратных средств, парольной защиты и попыток НСД к информации.

Использование предложенной системы мониторинга ИБ типовой КСИИ и рекомендации по ее организации и проведению позволяет контролировать состояние защищенности ИБ в КСИИ, обеспечивая конфиденциальность, целостность и доступность защищаемой информации, тем самым позволяет минимизировать возможный ущерб КСИИ.

Список литературы:

1. Федеральный закон РФ от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Указ Президента РФ от 30 ноября 2006 г. № 1321 «О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004 г. № 1085».

3. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом РФ от 9 сентября 2000 г. № Пр-1895.
4. Постановление Правительства РФ от 15 сентября 1993 г. № 912-51 «Об утверждении Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам».
5. Постановление Правительства РФ от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».
6. Нормативно-методический документ ФСТЭК России от 18 ноября 2008 г. «Методические рекомендации по организации контроля состояния обеспечения безопасности информации в ключевых системах информационной инфраструктуры Российской Федерации».
7. Нормативно-методический документ утвержден указом президента РФ от 3 февраля 2012 г. № 803 «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации».
8. Нормативно-методический документ утвержден ФСТЭК России от 14 марта 2014 г. «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».
9. Безбородов В.Г., Романов А.А., Урличич Ю.М. Концепция Федеральной системы мониторинга критически важных и (или) опасных объектов и грузов РФ на период по 2010 года и дальнейшую перспективу. Москва: Российский научно-исследовательский институт космического приборостроения, 2003. 19 с.

© 2015, Алексанян А.П., Пестов И.Е.
Система мониторинга состояния
информационной безопасности в ключевых
системах информационной инфраструктуры

© 2015, Aleksanyan A.P., Pestov I.E.
The system of monitoring the state of the
information security systems in key information
infrastructure