УДК 004.056

В.С. Оладько

ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ АКТИВНОГО МОНИТОРИНГА И АУДИТА БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ СЕТИ ОРГАНИЗАЦИИ

ФГАОУ ВПО «Волгоградский государственный университет»

В статье выявлены основные причины нарушения безопасности информации на предприятии. Предложен подход к проведению активного мониторинга и аудита безопасности корпоративной сети и ее ресурсов, с учетом причин нарушения безопасности. Реализован программный комплекс, позволяющий диагностировать инциденты безопасности, оценивать их критичность и вырабатывать рекомендации направленные на противодействие и устранение последствий.

Ключевые слова: обработка информации, атака, контроль, защита информации, надежность, угрозы

Введение. Любая организация является сложной, развивающейся и управляемой системой. Основными функциями управления организацией являются планирование, учет, анализ, контроль и регулирование. В процессе управления нужная информация фиксируется, представляется, сохраняется, накопляется и обрабатывается. Комплекс этих процедур составляет информационный процесс управления. Для организации и осуществления информационного процесса необходим персонал, способный осуществлять его процедуры, а также надлежащие средства и методы обрабатывания информации. Все это в совокупности составляет корпоративную сеть (КС) организации от качества и безопасности функционирования которой будет напрямую зависеть успешность и работоспособность всей организации в целом.

Следовательно, актуальным направлением в обеспечении защиты информации является не только создание адекватной системы защиты наиболее полно соответствующей требованиям и рекомендациям регуляторов[1], но проведение своевременного и регулярного контроля над состоянием безопасности обрабатываемой и хранимой в корпоративной сети информации.

Причины нарушения безопасности информации в корпоративной сети. В КС объектами защиты являются информация, средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической, видео - и речевой информации, общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты

информации. При этом основными причинами нарушения доступности, целостности и конфиденциальности являются угрозы нарушения информационной безопасности. Причинами реализации угроз являются ошибки пользователей, действия злоумышленников как внешних, так и внутренних, сбои и отказы технических и программных средств. По данным исследований, проводимых «Лабораторией Касперского» и материалам опубликованных в [2,3] можно сделать вывод о том, что большинство угроз безопасности информации в 2014 годы было связано с действием вредоносного ПО, фишинговыми и спам-атаками, а также отказами и сбоями, происходящими в корпоративной сети (см. рисунок 1).

Рисунок 1 – Статистика угроз информационной безопасности за 2014 год

Следовательно, для того чтобы своевременно выявить попытку или факт реализации угрозы, а также устранить ее последствия с минимальными потерями для предприятия необходимо осуществлять активный мониторинг и аудит безопасности КС и ее ресурсов, с учетом наиболее распространённых причин нарушения безопасности. В подобной системе должны решаться следующие задачи: диагностика и идентификацию угрозы и места ее воздействия, оценка ее критичности и риска для организации, выработка рекомендаций направленных на противодействие и устранение последствий диагностированной угрозы.

Задача и функции активного мониторинга и аудита безопасности корпоративной сети. Для решения обозначенных задач, автором предлагается программный комплекс для проведения активного мониторинга и аудита безопасности КС. В отличие от существующих средств оценки защищенности, обнаружения атак и аудита безопасности, программный комплекс позволяет не только выявить аномалию в работе сети и провести оценку рисков, но и позволяет оценить надежность подсистем КС, влияющую на доступность информации и сервисов, а также спрогнозировать возможные отказы. Это позволяет получить комплексную оценку безопасности КС и дать наиболее рациональные рекомендации, направленные на поддержание необходимого уровня безопасности или его повышение.

Основными функциями программного комплекса активного мониторинга и аудита решений безопасности КС организации являются:

1. сбор, обработка и отображение информации в реальном масштабе времени об обстановке;
2. выборочное представление информации с систем контроля в записи и в реальном масштабе времени с учетом секторов обзора и пространственного расположения;
3. структурированное хранение и представление информации для принятия решения при возникновении угрозы;
4. осуществление доведения управленческой информации до объекта, органов управления, сил и средств и вывода необходимых информационных сообщений;
5. обеспечение мониторинга и управления в режиме реального времени мероприятиями по экстренному реагированию и ликвидации последствий обнаруженной угрозы;
6. определение наличия и актуальности средств и механизмов обеспечения защищенности корпоративной сети;
7. вычисление времени функционирования аппаратных компонентов корпоративной сети и компонентов рабочих станций;
8. вычисление вероятности выхода из строя того или иного компонента корпоративной сети или компонента рабочих станций;
9. выявление противоправных или неверных действий пользователей;
10. выявление атак на систему;
11. выявление изменений файловой системы;
12. контроль над созданием резервных копий по расписанию.

На рисунке 2 ней изображено как программный комплекс взаимодействует с элементами КС организации и какие элементы входят в его состав.

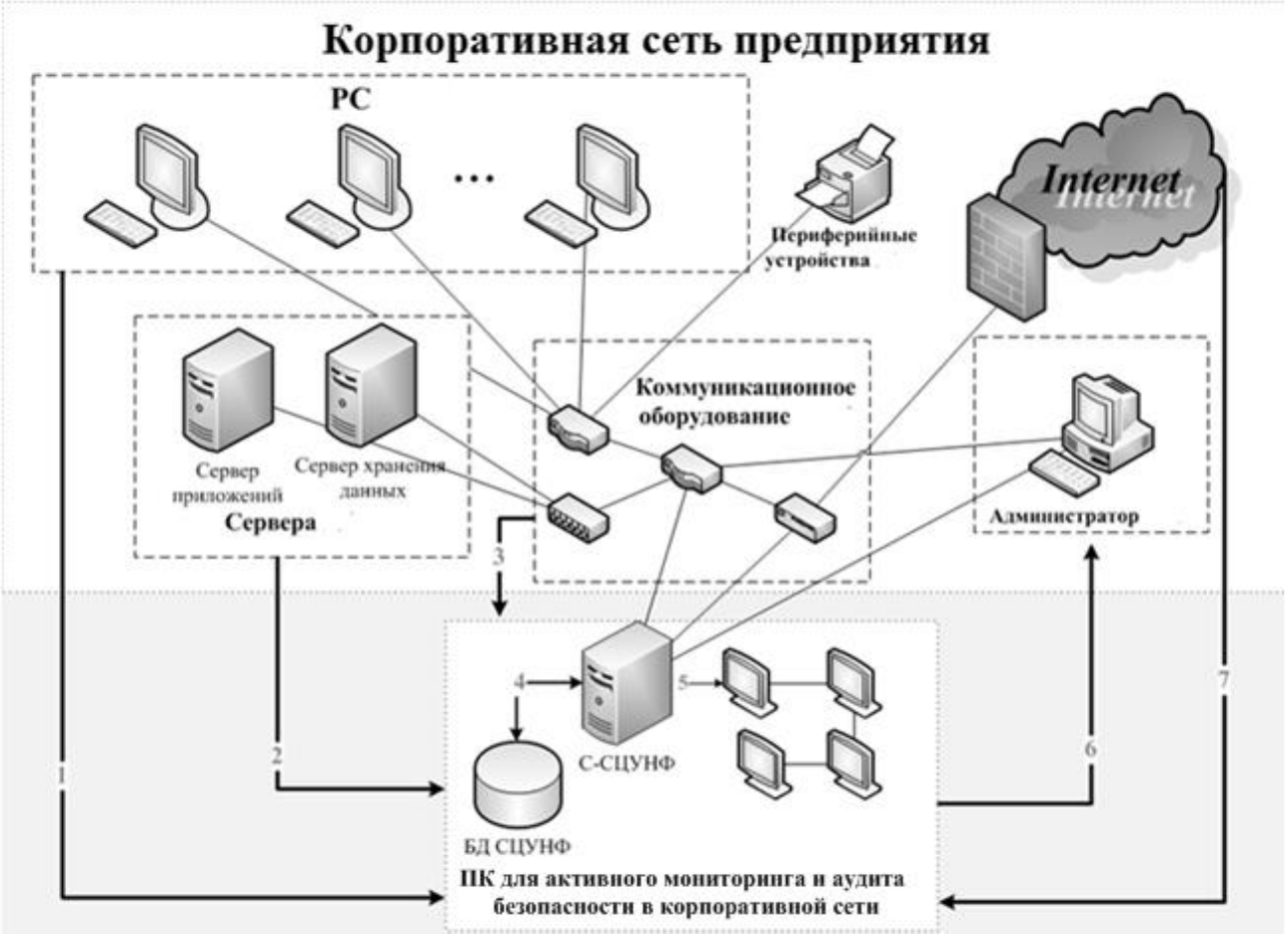

Рисунок 2 – Схема взаимодействия программного комплекса с элементами КС организации

Программный комплекс активного мониторинга и аудита состоит из:

- сервера получения, хранения, отображения и обработки данных о корпоративной сети (С-ЦУНФ);
- базы данных, в которой хранятся сведения о сроках эксплуатации элементов корпоративной сети (БД СЦУНФ).

Данные необходимые для контроля за состоянием безопасности поступают в программный комплекс с персональных компьютеров (PC, стрелка 1), от серверов (стрелка 2) и от коммуникационного оборудования (стрелка 3). Также в возможности программного комплекса входит получения данных и сети Internet (стрелка 7), для получения дополнительной информации. Все полученные данные обрабатываются, структурируются и отображаются на экран (стрелка 5). Для выявления возможного выхода из строя какого-либо элемента КС программный

комплекс обращается к БД (стрелка 4) для получения информации о сроках эксплуатации элементов и сравнивает их с действующим сроком работы. При выявлении каких-либо причин нарушения, система принятия решений анализирует ситуацию, генерирует отчет с рекомендациями по их устранению и пересылает его администратору сети (стрелка 6), для их последующего устранения.

Формализация активного мониторинга и аудита безопасности. Формализованное описание можно представить с помощью теоретико-множественной модели в виде кортежа.

$$M_{AMA} = (\{I\}, \{OR\}, \{M_{ISE}\}, \{SEC\}, \{N\}, \{O\}, DM),$$

где $\{I\}$ – входные данные; $\{OR\}$ - требования предприятия к параметрам безопасности корпоративной сети; $\{M_{ISE}\}$ – множество, описывающее корпоративную сеть предприятия; $\{SEC\}$ – критерии проверки защищенности персональных компьютеров и серверов; $\{N\}$ – критерии проверки надежности персональных компьютеров и серверов; $\{O\}$ – выходные данные; *DM*–функция принятия решений.

Входные данные – данные поступающие от клиентов в процессе мониторинга состояния элементов КС, содержат информацию о программном обеспечении, аппаратном обеспечении и процессах каждого компьютера.

Требования предприятия к параметрам безопасности КС выражаются в установление эталонного списка программного обеспечения, процессов, технических средств, предельного количества допустимых нарушений, которые могут быть зафиксированы в корпоративной сети предприятия VLN_{max} за установленный период анализа $T_{analyze}$, $Q(t)^{max}$.

Модель КС описывается кортежем

$$M_{ISE} = \{\{PC\}, \{S\}, \{CE\}\},$$

где $\{PC\}$ – это рабочие станции работников организации;
$\{S\}$ – сервера; $\{CE\}$ – коммуникационное оборудование.

Каждая рабочая станция описывается как совокупность множеств

$$PC = \{\{PO_{PC}\}, \{SO_{PC}\}, \{K_{PC}\}\}.$$

Аналогично описываются сервера организации –

$$S = \{\{PO_S\}, \{SO_S\}, \{K_S\}\},$$

где $\{PO\}$ – программное обеспечение; $\{SO\}$ – системное обеспечение; $\{K\}$ – обеспечивающие компоненты PC, т.е. жесткие диски, оперативная память, блоки питания и др.

Множество программного обеспечения описывается как

$$PO = \{\{NAME\}, \{DATE\}, \{VER\}\},$$

где $\{NAME\}$ – это имя продукта; $\{DATE\}$ – дата установки; $\{VER\}$ – версия.

Множество PO_{PC} и множество PO_S строго определенно, так как на каждой РС или сервере КС стоит определенный перечень программного обеспечения.

Множеством входящие в системное обеспечение $\{SO\}$ являются процессы системы $\{PR\}$ воздействие, на которых или запуск посторонних может привести к сбою системного обеспечения, т.е. $SO = \{PR_1, \dots, PR_n\}$.

К компонентам персональных компьютеров и серверов наиболее серьезно оказывающие влияние на непрерывность функционирования корпоративной сети и доступность ее подсистем можно отнести следующее аппаратное обеспечение: блоки питания $\{PSU\}$; жесткие диски $\{HDD\}$;оперативная память $\{RAM\}$.

Таким образом, обеспечивающие компоненты включают в себя следующие множество:

$$K_{PC} = \{\{PSU_{PC}\}, \{HDD_{PC}\}, \{RAM_{PC}\}\}.$$
$$K_S = \{\{PSU_S\}, \{HDD_S\}, \{RAM_S\}\}.$$

Каждый из этих компонентов имеет два параметра:t – время эксплуатации; T – срок эксплуатации. Критерии поверки защищенности КС организации $\{SEC\}$ складывается из следующих действий:

- проверки программного обеспечения $\{SEC_{PO}\}$;
- проверки запущенных процессов $\{SEC_{PR}\}$;
- проверки актуальности и работоспособности антивирусных (АВ) средств защиты $\{SEC_{AV}\}$;
- обнаружения попыток несанкционированного входа в систему$\{SEC_{NSD}\}$;
- обнаружения несанкционированных действий пользователя в системе$\{SEC_{NSM}\}$;
- обнаружение изменений файловой системы (ФС) $\{SEC_{MFS}\}$.

Тем самым множество критерием проверки защищенности имеет следующий вид:

$$\{SEC\} = \{\{SEC_{PO}\}, \{SEC_{PR}\}, \{SEC_{AV}\}, \{SEC_{NSD}\}, \{SEC_{NSM}\}, \{SEC_{MFS}\}.\}$$

Множество $\{SEC_{PO}\} = \{\{PO_{PC}\}, \{PO_{PC}^T\}, \{PO_S\}, \{PO_S^T\}\}$,

где $\{PO_{PC}\}$ и $\{PO_S\}$ – это текущее ПО установленное на РС и серверах, а $\{PO_{PC}^T\}$ и $\{PO_S^T\}$ – это перечень требуемого ПО. При условии

если $PO_{PC} \equiv PO_{PC}^{T}$, то имеет место что в перечне установленного ПО имеются в наличии продукты не соответствующие требуемому перечню ПО. Выявленные элементы не соответствующие «эталонному» списку $\{PO_S^T\}$ заносятся во множество нарушений $\{VLN\}$, которые используются в функции принятия решений *DM* и в векторе выходных данных $\{O\}$.

Аналогичная проверка проводится и с другими элементами множества критериев безопасности.

При проверке надежности корпоративной сети используются следующие критерии: проверка персональных компьютеров; проверка серверов; проверка коммуникационного оборудования.

При осуществлении проверки надежности персональных компьютеров и серверов существуют множества с параметрами $N_{PC} = \{\{PSU_{PC}^t\},\{HDD_{PC}^t\},\{RAM_{PC}^t\}\}$ и $N_S = \{\{PSU_S^t\},\{HDD_S^t\},\{RAM_S^t\}\}$ они определяют время и интенсивность работы основных комплектующих PC и серверов. При вычислении надежности коммуникационного оборудования передается параметр $\{CE^t\}$, который определяет время работы оборудования. При получении этих данных от клиентов системы система поддержки принятия решений вычисляет вероятность отказа компонентов отношением:

$$t \to T \Rightarrow Q(t) \to 1,$$

где $Q(t) -$ вероятность отказа. Если вероятность отказа элемента $Q(t) > Q(t)^{max}$, больше установленного предельно допустимого значения, то данное оборудование также заносится в список потенциальных нарушений $\{VLN\}$. Выходные данные это информация о выявленных угрозах, несоответствиях и рекомендациях, направленных на их устранение.

Функция принятия решений *DM* представляет собой классификатор, который по набору признаков объекта выносит решение о том, к какому именно классу он принадлежит [4].

$$DM : \Re^n \to Y \qquad (2)$$

Функция *DM* отображает пространство векторов признаков в пространство векторов меток *Y*. В этом случае *Y*=[0,1], где 0 соответствует «безопасному» состоянию системы, а 1 – «опасному». При этом состояние исследуемой корпоративной сети будет считаться безопасным, если все значения текущих показателей защищенности и надежности будут совпадать со значениями показателей «эталонного профиля» и никаких нарушений не будет выявлено, в противном случае состояние будет классифицировано как «опасное».

$$DM = \begin{cases} 0, & \text{если } (\{SEC\} \cong \{SEC^{ET}\}) \text{ и } (\{N\} \cong \{N\}^{ET}) \text{и} (\{VLN\} = \emptyset) \\ 1, & \text{если } (\{SEC\} \neq \{SEC^{ET}\}) \text{ или} (\{N\} \neq \{N\}^{ET}) \text{или} (\{VLN\} \neq \emptyset) \end{cases}$$

В процессе классификации при сопоставлении элементов из текущих и эталонных множеств используется правило подобия основанное на применении Евклидового расстояния, возможность применения которого обосновано в работе [5].

Заключение. Предложенный подход к анализу безопасности корпоративной сети предприятия и автоматизирующая его система поддержки принятия решений могут применяться на практике для проведения периодического мониторинга и контроля над состоянием безопасности корпоративной сети предприятия, а также в учебном процессе в качестве стенда-макета на лабораторных практикумах при обучении студентов направления информационная безопасность.

ЛИТЕРАТУРА

1. Кострова В.Н., Милошенко О.В. Программные решения для анализа информационной безопасности/Моделирование, оптимизация и информационные технологии. 2015.№1(8). С.21 [Электронный ресурс].- Режим доступа: http://moit.vivt.ru/wpcontent/uploads/2015/04/KostrovaMiloshenko_1_15_2.pdf (дата обращения 15.09.2015).
2. Эмм Д., Гарнаева М., Чевышев В. Развитие информационных угроз в третьем квартале 2014 года//SecureList. [Электронный ресурс].- Режим доступа:https://securelist.ru/analysis/malware-quarterly/24365/razvitie-informacionnyx-ugroz-v-tretem-kvartale-2014-goda/ (дата обращения 04.09.2015)
3. Symantec Intelligent report. July 2014//Публикации службы Security Response. Symantec. [Электронный ресурс].- Режим доступа: http://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence_report_07-2014.en-us.pdf (дата обращения 01.09.2015)
4. Аткина В.С. Мониторинг состояний катастрофоустойчивой информационной системы с помощью гибридной иммунной сети. Известия ЮФУ. Технические науки. 2012. №12 (137). С. 90-96
5. Зайцев С.А., Субботин С.А. Обобщенная модель искусственной иммунной сети//Нейроинформатика. 2010. Часть 2. С. 98 – 107.

V.S. Oladko

SOFTWARE FOR MONITORING AND ACTIVE SECURITY AUDIT CORPORATE NETWORK

Volgograd State University

In the paper the author identified the main causes of violations of information security in the enterprise. Proposed approach to active monitoring and security auditing corporate network resources, taking into account the causes of security. Implemented software package that allows you to diagnose security incidents, assess their criticality and make recommendations aimed at combating and eliminating the consequences.

Keywords: corporate network, monitoring, auditing, security, reliability, threat monitoring