DOI: https://doi.org/10.15688/NBIT.jvolsu.2020.4.3

УДК 004.056.5
ББК 32.971.35

РАЗРАБОТКА МЕТОДА ПРОВЕДЕНИЯ АУДИТА СИСТЕМЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Павел Александрович Запороцков

Кандидат физико-математических наук, заместитель начальника
отдела эксплуатации информационных систем, технических средств и каналов связи,
Управление Росреестра по Волгоградской области
34_upr@rosreestr.ru
ул. Калинина, 4, 400001 г. Волгоград, Российская Федерация

Аннотация. В работе рассмотрены существующие стандарты в области проведения аудита информационной безопасности. Разработана инновационная модель проведения аудита системы защиты информации, базирующаяся на сопоставлении требовании мер приказа № 21 ФСТЭК России и способов реализации в подсистемах защиты информации системы защиты персональных данных, даны рекомендации по проверкам конкретных мер защиты и используемым техническим средствам аудита. Разработанный метод апробирован на примере проведения аудита в компании ООО «Лама» выбрано установление соответствия системы защиты персональных данных организации на соответствие требованиям приказа № 21 ФСТЭК России. Разработаны рекомендации по устранению имеющихся недостатков и несоответствий путем переоборудования подсистемы антивирусной защиты и подсистемы межсетевого экранирования и защиты каналов связи.

Ключевые слова: информационная безопасность, аудит системы защиты информации, технические средства аудита, защита каналов связи, антивирусная защита.

Введение

Как известно, принятие решений во всех сферах жизнедеятельности предприятий и организаций базируется на информационных процессах. Анализ таких процессов реализуется на основе информационных моделей, построенных на современных информационно-коммуникационных технологиях.

Информационный ресурс, как часть информационного процесса, является одним из важнейших источников эффективности предприятия вне зависимости от ее сферы деятельности.

Информационные процессы, как и информационные ресурсы управляют информацией различной степени важности для предприятия. В связи с этим защита такой информации представляет одну из важнейших процедур в области обеспечения безопасности государства, значение которой растет с каждым годом.

Проблема защиты информации – надежное обеспечение ее сохранности и установленного статуса использования – является одной из важнейших проблем современности.

В процессе построения систем защиты информации важно понимать, насколько адекватно существующая система защиты информации способна противостоять угрозам информационной безопасности существующим и еще не найденным уязвимостям, а также по-

стоянному процессу изменения в структуре информационного обмена.

Одним из наиболее эффективных способов проверки состояния информационной безопасности на предприятии является аудит.

В соответствии с ГОСТ Р 53114-2008 «Обеспечение информационной безопасности в организации» под аудитом информационной безопасности понимается систематический, независимый и документируемый процесс получения свидетельств деятельности организации по обеспечению информационной безопасности и установлению степени выполнения в организации критериев информационной безопасности, а также допускающий возможность формирования профессионального аудиторского суждения о состоянии информационной безопасности организации [1].

В представленной работе предложен инновационный метод проведения аудита системы технической защиты информации на примере оценки соответствия системы защиты персональных данных ООО «ЛАМА» на соответствие требованиям установленного уровня защищенности.

Предметная область аудита информационной системы технической защиты информации

Аудит проводится на соответствие критериям аудита, которыми являются совокупность принципов, положений, требований и показателей действующих нормативных документов, относящихся к деятельности организации в области информационной безопасности. Критериями аудита могут быть:

– законодательные нормы и стандарты;

– лучшие практики по обеспечению информационной безопасности;

– внутренние политики информационной безопасности.

Критерии аудита информационной безопасности используются для сопоставления с ними свидетельств аудита информационной безопасности.

По своему типу проведения аудиты подразделяются на внутренние аудиты и внешние аудиты.

Внутренние аудиты (аудиты первой стороны) проводит для внутренних целей сама организация или от ее имени другая организация. Результаты внутреннего аудита могут служить основанием для декларации о соответствии. Во многих случаях, особенно на малых предприятиях, аудит должен проводиться специалистами (людьми, не несущими ответственности за проверяемую деятельность).

Внешние аудиты включают в себя аудиты, называемые аудитами второй стороны и аудитами третьей стороны. Аудиты второй стороны проводят стороны, заинтересованные в деятельности предприятия, например, потребители или другие лица от их имени. Аудиты третьей стороны проводят внешние независимые организации. Эти организации проводят сертификацию или регистрацию на соответствие требованиям, например, требованиям на соответствие законодательным нормам и федеральным законам, требованиям международных стандартов и т. д.

Национальный стандарт РФ, идентичный международному стандарту,ГОСТ Р ИСО 19011-2012 «Руководящие указания по аудиту систем менеджмента» приводит следующую концепцию проведения аудита [2]:

– организация и проведение аудита;

– подготовка к проведению аудита на месте;

– проведение аудита на месте;

– подготовка и рассылка отчета по аудиту;

– завершение аудита;

– действия по результатам аудита.

Команда аудиторов, обычно состоящая из ведущего аудитора, аудитора, аудитора-стажера, технический эксперт и т. д. перед началом аудита, разрабатывает цели и программу проведения аудита.

Цели могут зависеть от:

1) идентифицированных требований информационной безопасности;

2) требований нормативных документов;

3) уровня качества функционирования проверяемой организации, который отражает случаи возникновения сбоев и инцидентов информационной безопасности и эффективность измерений;

4) рисков информационной безопасности организации, подвергающейся аудиту.

Цели аудита можно подразделить на:

– превентивные – направленные на превентивное выявление угроз и уязвимостей и

предотвращение инцидентов информационной безопасности;

– детектирующие – направленные на обнаружение новых или уточнение особенностей уже имеющихся угроз и уязвимостей системы защиты вовремя или после инцидентов информационной безопасности;

– корректирующие – направленные на формирование комплекса мер повышения эффективности существующей системы защиты после инцидентов информационной безопасности с учетом вновь выявленных угроз и уязвимостей.

Объем программы аудита может меняться в зависимости от следующих факторов:

1) от масштаба системы информационной безопасности, включающей общее количество сотрудников предприятия и взаимоотношения со сторонними организациями, регулярно работающими на проверяемом предприятии;

2) количество информационных систем предприятия;

3) количество объектов, охваченных системой информационной безопасности:

– сложность системы информационной безопасности (включая количество и критичность процессов и видов деятельности),

– значимость рисков информационной безопасности,

– важность информации и связанных с ней активов,

– сложность информационных систем, сложности использованных информационных технологий;

4) изменение сложности объектов, находящихся в области действия системы информационной безопасности.

По своей форме аудит может быть:

– организационно-нормативным – когда анализируется организационные мероприятия обеспечения информационной безопасности и нормативные акты в данной сфере;

– техническим – когда анализируется технические средства и способы обеспечения информационной безопасности.

Проведение аудита предусматривает следование определенной формальной процедуре проверки объекта. Данная процедура проводится в соответствии с предварительно сформированными формальными описаниями объекта и процесса аудита, а также актуальных угроз:

– моделью аудита;

– моделью нарушителя / противника;

– моделью угроз;

– общим практическим подходом к проведению аудита;

– общим теоретическим подходом к проведению аудита.

При проведении такой формализации обязательно прописываются следующие аспекты исследования:

– источники угроз;

– защищаемые подсистемы, ресурсы, процессы или другие элементы системы;

– связи между источниками угроз и защищаемыми элементы системы;

– структура и процессы функционирования подсистемы защиты.

Модель аудита включает в себя формализованное описание:

– объекта аудита;

– цели аудита;

– предъявляемых требований;

– используемых практических и теоретических подходов;

– масштаба и глубины;

– исполнителей;

– порядка проведения аудита.

Модель нарушителя / противника включает в себя формализованное описание:

– формализованное понятие нарушителя / противника;

– критерии нарушения информационной безопасности;

– категорирование нарушителей / противников;

– предположения о квалификации, возможностях, располагаемых средствах и способах информационного воздействия для каждой категории нарушителей / злоумышленников;

– предположения о сценариях действий каждой категории нарушителей / злоумышленников;

– уровень полномочий и способы получения доступа к системе для каждой категории нарушителей / злоумышленников.

Описание объекта исследования

В качестве объекта исследования рассматривается ООО «Лама», являющаяся

крупной розничной сетью магазинов по реализации продуктов продовольствия, состоящая из 54 магазинов формата универсам, супермаркет, гипермаркет и центрального офиса.Оперативное управление ООО «Лама» осуществляется генеральным директором в соответствии с уставом.Функции обеспечения защиты информации возложены на специалиста по информационной безопасности, входящего в отдел АСУ. Виды обрабатываемой информации: – персональные данные (далее – ПДн) сотрудников и физических лиц, не являющихся сотрудниками и коммерческая тайна. Примерный объем обрабатываемых персональных данных – более 100 000. Обработка персональных данных происходит как с использованием средств автоматизации (в информационных системах персональных данных), так и без использования средств автоматизации (на документальных носителях).

В ООО «Лама» персональные данные обрабатываются в следующих информационных системах персональных данных (далее – ИСПДн):

– 1С: Бухгалтерия;

– 1С: Бухгалтерия;

– 1С: Управление продажами.

Предоставление сервисов информационных систем персональных данных пользователям реализуется посредством локальной вычислительной сети. Сетевая архитектура локальной вычислительной сети построена на базе оборудования Dlink (см. рис. 1).

Ядром сети выступает маршрутизатор DSR-1000. За коммутацию серверного оборудования отвечает коммутатор типа DGS-1008MP. За коммутацию рабочих станций отвечают коммутаторы серии DES-1050G.

В соответствии с Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 [3] определяются 4 уровня защищенности, в соответствии с которыми обеспечивается защита персональных данных. Уровень защищенности определяется категорией обрабатываемой информации, типом актуальных угроз и числом субъектов ПДн.

Для всех ИСПДнООО «Лама» характерны угрозы 3-го типа, не связанные с наличием недекларированных возможностей,так как все применяемоепрограммное обеспечение лицензировано и имеет разрешение к применению на территории Российской Федерации.Так как ООО «Лама» не обрабатывают специальные, биометрические и общедоступные ПДн, можно установить, что ИСПДн ООО «Лама» обрабатывают иные категории ПДн.

На основании вышеизложенной информации и Постановления Правительства РФ от 1 ноября 2012 г. № 1119, уровень защищенности устанавливается как УЗ-4 [3].

На основании сведений о уровне защищенности можно установить содержание мер по обеспечении безопасности ПДн в соответствии с Приказом ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [4]:

– идентификация и аутентификация: ИАФ.1, ИАФ.2, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.6;

– управление доступом: УПД.1, УПД.2, УПД.3, УПД.4, УПД.5, УПД.6, УПД.13, УПД.14, УПД.15, УПД.16;

– регистрация событий безопасности: РСБ.1, РСБ.2, РСБ.3, РСБ.7;

– антивирусная защита: АВ3.1, АВ3.2;

– анализ защищенности: АН3.2;

– защита технических средств: ЗТС.3, ЗТС.4;

– защита информационных систем: ЗИС.3.

Сведения о необходимости соответствия техническим мерам по защите персональных данных в этом случае будут являться критериями аудита.

3. Разработка методики аудита

В качестве системы технической защиты информации ООО «Лама» рассматривается система защиты персональных данных ООО «Лама» (далее – СЗПДн). СЗПДн предназначена для соблюдения требований Федерального закона № 152-ФЗ «О персональных данных» [5], требований нормативных документов и позволяет минимизировать правовые и репутационные риски, связанные с потенциальными утечками персональных данных и несоблюдением законодательства Российской Федерации.

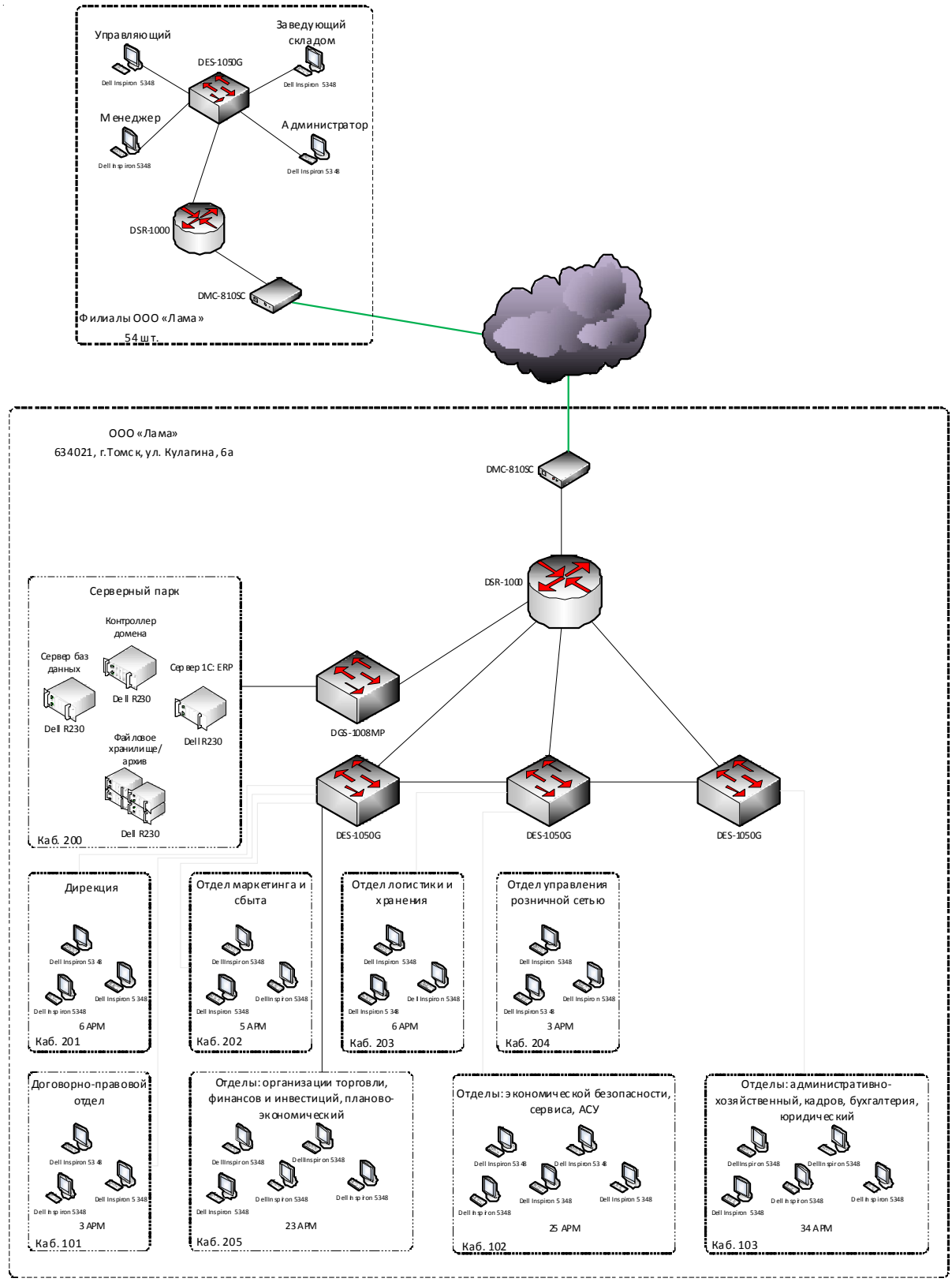

Рис. 1. Структура локальной вычислительной сети ООО «Лама»

В соответствии с минимально необходимым комплексом мер в состав типовой СЗПДн входят следующие подсистемы:

– подсистема управления доступом;

– подсистема регистрации и учета;

– подсистема обеспечения целостности;

– подсистема антивирусной защиты;

– подсистема межсетевого экранирования и защиты каналов связи;

– подсистема управления системой защиты персональных данных.

Для проверки корректности применяемых мер по защите информации ООО «Лама» прибегает к внутреннему аудиту СЗПДн.

Аудит СЗПДн проводится силами отдела АСУ ООО «Лама» и включает в себя следующие этапы:

– планирование аудита;

– подготовка аудита;

– проведение аудита;

– составление отчетной документации по результатам аудита.

Целью планирования аудита является обеспечение проведения проверки наилучшим (оптимальным) образом. Результаты процесса планирования оформляются в двух документах: плане аудита и программе аудита.

В плане аудита отмечается объект аудита, организационная единица, место проведения аудита, критерии аудита, сведения об аудиторах и периодах проведения аудита.

Аудит начинается с вводного совещания, которое проводит руководитель аудита в срок, указанный в программе аудита или в другое согласованное сторонами время.

Во время аудита информация, относящаяся к целям аудита, области и критериям аудита, включая информацию, касающуюся взаимодействия между подразделениями, деятельности и процессов, должна быть, собрана путем необходимых выборок и обработана. Свидетельством аудита может быть только информация, которая может быть обработана. Свидетельства аудита должны быть зарегистрированы.

Источниками исходной информации для аудиторов в ходе проверки являются: документы, регламентирующие деятельность подразделения и процессы, процедуры, методики, приказы, планы, регистрационные журналы, протоколы совещаний.

При сборе свидетельств аудита необходимо использовать следующие методы:

– опросы;

– наблюдение за деятельностью;

– техническая проверка;

– оценивание.

Программа проведения аудита является частным случаем общего алгоритма проведения аудита и детализирует перечень аудиторских процедур подлежащих проведению. Программа служит подробной инструкцией для аудиторской команды и одновременно средством контроля для руководства компании.

Программа проведения аудита реализуется путем постадийной проверки соответствующих подсистем СЗПДн и мер, предназначенных для реализации требований по защите информации, предъявляемых к этим подсистемам. На рисунке 2 представлена методика проведения аудита СЗПДн.

Для каждой из подсистем СЗПДн (УПД.1, УПД.3…ИАФ.1 и т. д.) используется своя методика проверки реализации мер информационной безопасности.

Технические средства аудита

Для аудита информационной безопасности СЗПДн могут применяться различные технические средства.

Для аудита подсистем управления доступом, регистрации и учета, обеспечения целостности может применяться система анализа защищенности Сканер-ВС.

Сканер-ВС – система комплексного анализа защищенности, позволяющая обеспечить своевременное выявление уязвимостей в ИТ-инфраструктуре организаций любого масштаба. С помощью Сканер-ВС можно проводить тестирование на проникновение, сканирование уязвимостей, а также анализ конфигурации, организовать непрерывный контроль защищенности. В качестве средства аудита СЗПДн Сканер-ВС дает широкий функционал по реализации мер сетевого и локального аудита-контроль появления новых сетевых узлов и сервисов, идентификация ОС и приложений, трассировка маршрутов передачи данных, построение топологии сети организации.

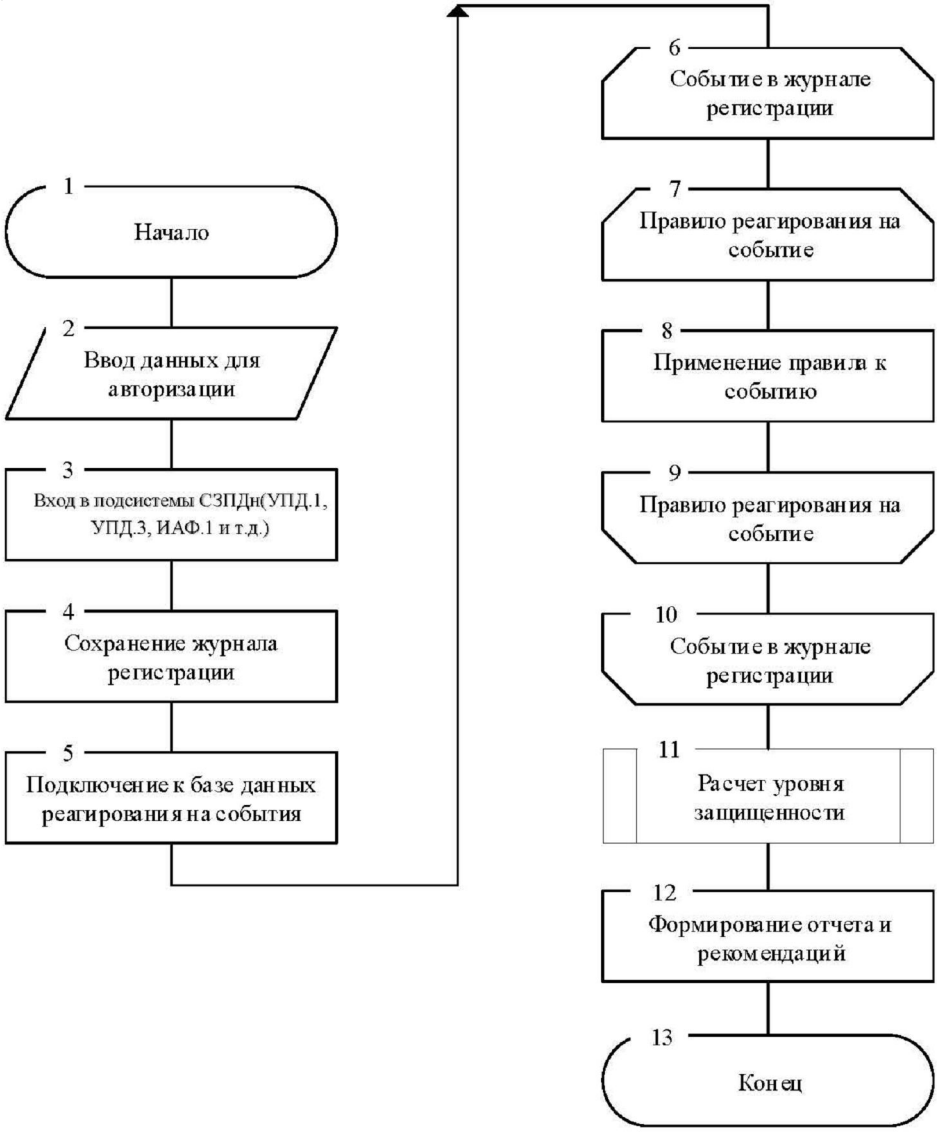

Рис. 2. Методика проведения аудита СЗПДн

Сканер-ВС позволяет проводить аудит установленного аппаратного и программного обеспечения – инвентаризацию программных и аппаратных средств локальной системы, включая параметры установленных операционных систем, программное обеспечение, информацию о пользователях системы, историю подключений к беспроводным сетям, данные системных, коммуникационных и периферийных устройств (центральный процессор, материнская плата, мост, оперативная память и др.), в том числе носителей информации и USB-устройств. Функция сравнения отчетов позволяет отслеживать изменения конфигурации системы. Для аудита мер ИАФ.2, УПД.3, УПД.4, УПД.6 используется средство локального аудита паролейСканер-ВС, предназначенное для поиска и выявления на локальнойрабочей станции неустойчивых к взлому паролей.

Для аудита мер УПД.14 применяется средство аудита беспроводных сетей. Средство аудита беспроводных сетей предназначено для обнаружения, сканирования ипроведения пассивных и активных атак на подбор паролей в беспроводных сетях с WEP, WPA иWPA-2 шифрованием.

Модуль сетевого анализа предназначен для перехвата, анализа и фильтрации сетевоготрафика.

Для поиска потенциальных уязвимостей в сети используется модуль «Поиск уязвимос-

тей». Под уязвимостью ПО подразумевается дефект, который может стать причиной нарушенияинформационной безопасности.

В качестве средства аудита мер ИАФ.1, ИАФ.2, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.6, УПД.1, УПД.4, УПД.5, УПД.6 может также использоваться программное средство ChangeAuditor 5.0.

ChangeAuditor 5.0 – является инструментом для оперативного аудита изменений в реальном масштабе времени на серверах служб каталогов, Exchange, а также на файловых серверах под управлением операционной системы Windows. Кроме аудита, в ChangeAuditor 5.0 можно блокировать изменения. Например, запретить добавление в группу AD новых пользователей или запретить изменение файла / папки.

В качестве средства аудита мер РСБ.2, РСБ.3, РСБ.7 может также использоваться менеджмент логов QuestInTrust – интеллектуальный, масштабируемый инструмент управления журналом событий, который позволяет отслеживать все действия пользователей на рабочих станциях и администраторах от входа в систему до выхода из системы и всего того, что было между этими событиями.После сбора вся статистика (события) приводится к состоянию вида: когда произошло, что произошло, где произошло, кто выполнил действие, откуда это действие было выполнено. InTrust может обрабатывать до 60 000 событий в секунду из 10 000 источников. Часто подобные агенты-сборщики устанавливаются на рабочие станции, чтобы отслеживать события WindowseventlogSysmon (отслеживания изменений значений реестра, создания новых процессов с неправильных хэшем и других), логов PowerShell.

В соответствии со сведениями об объекте исследования и методикой проведения аудитабыла проведена аналитическая реализация программы аудита СЗПДн ООО «Лама».

По результатам аудита установлены 19 соответствий и 7 несоответствий. Были выданы рекомендации на разработку 7 корректирующих действий для успешного прохождения аудита, в частности:

– разработать план корректирующих действий, определить ответственных лиц и сроки исполнения;

– произвести замену средства антивирусной защиты на средство, соответствующее требованиям ФСТЭК России по информационной безопасности, произвести его настройку и обновление базы сигнатур до актуальной версии;

– произвести выбор средства, закупку и пуско-наладку средства межсетевого экранирования и шифрования в соответствии с требованиями руководящих документов ФСТЭК и ФСБ России;

– произвести повторный аудит по выявленным несоответствиям и определить корректность их устранений.

Заключение

Были рассмотрены существующие стандарты в области проведения аудита информационной безопасности. Дано описание объекта исследования – компания ООО «Лама». В качестве критериев аудита выбрано установление соответствия системы защиты персональных данных ООО «Лама» на соответствие требованиям приказа № 21 ФСТЭК России.

Разработана модель проведения аудита системы защиты информации, базирующаяся на сопоставлении требовании мер приказа № 21 ФСТЭК России и способов реализации в подсистемах защиты информации системы защиты персональных данных, даны рекомендации по проверкам конкретных мер защиты и используемым техническим средствам аудита.

Проведен аналитический аудит системы защиты персональных данных ООО «Лама», по результатам аудита установлено 19 соответствий и 7 несоответствий, в качестве рекомендаций по повышению уровня защищенности рекомендуется переоборудование подсистемы антивирусной защиты и подсистемы межсетевого экранирования и защиты каналов связи.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 53114-2008. Национальный стандарт Российской Федерации. Защита информации. Обеспечение информационной безопасности в

организации. – Электрон. текстовые дан. – Режим доступа: https://internet-law.ru/gosts/gost/48411. – Загл. с экрана.

2. ГОСТ Р ИСО 19011-2012. Руководящие указания по аудиту систем менеджмента. – Электрон. текстовые дан. – Режим доступа: https://internet-law.ru/gosts/gost/52229. – Загл. с экрана.

3. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». – Доступ из справ.-правовой системы «КонсультантПлюс».

4. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». – Доступ из справ.-правовой системы «КонсультантПлюс».

5. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 21.07.2014) «О персональных данных». – Доступ из справ.-правовой системы «КонсультантПлюс».

REFERENCES

1. *GOST R 53114-2008 Nacional'nyj standart Rossijskoj Federacii. Zashchita informacii. Obespechenie informacionnoj bezopasnosti v organizacii* [The National Standard of the Russian Federation. Information Security. Ensuring Information Security in the Organization]. URL: https://internet-law.ru/gosts/gost/48411.

2. *GOST R ISO 19011-2012. Rukovodyashchie ukazaniya po auditu sistem menedzhmenta* [Guidelines for the Audit of Management Systems]. URL: https://internet-law.ru/gosts/gost/52229.

3. *Postanovlenie Pravitel'stva RF ot 1 noyabrya 2012 g. № 1119 «Ob utverzhdenii trebovanij k zashchite personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh»* [Resolution of the Government of the Russian Federation of 8 November, 2020 no. 647 "On Approval of the Requirements for the Protection of Personal Data During Their Processing in Personal Data Information Systems"]. Access from Reference Legal System "KonsultantPlyus".

4. *Prikaz FSTEK Rossii ot 18 fevralya 2013 g. № 21 «Ob utverzhdenii sostava i soderzhaniya organizacionnyh i tekhnicheskih mer po obespecheniyu bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh»* [Order FSTEK of 18 February 2013 no. 21 "On Approval of the Composition and Content of Organizational and Technical Measures to Ensure the Security of Personal Data During Their Processing in Personal Data Information Systems"]. Access from Reference Legal System "KonsultantPlyus".

5. *Federal'nyj zakon ot 27.07.2006 № 152-FZ (red. ot 21.07.2014) «O personal'nyh dannyh»* [Federal Law of 27 July 2006 no. 152-FZ (as Amended on 21 July 2014) "About Personal Data"]. Access from Reference Legal System "KonsultantPlyus".

DEVELOPMENT OF A METHOD FOR CONDUCTING AN AUDIT OF THE INFORMATION SECURITY SYSTEM

Pavel A. Zaporotskov

Candidate of Sciences (Physics and Mathematics), Deputy Head of the
Department of Operation of Information Systems, Technical Means and Communication Channels,
Department of Rosreestr for Volgograd Region
34_upr@rosreestr.ru
Kalinina St, 4, 400001 Volgograd, Russian Federation

Abstract. Information processes, as well as information resources, manage information of varying degrees of importance for the enterprise. In this regard, the protection of such information is one of the most important procedures in the field of state security, the importance of which is growing every year. The problem of information security – the reliable provision of its safety and the established status of use – is one of the most important problems of our time. The paper considers the existing standards in the field of information security audit. The author has developed an innovative model of audit of the information security system based on the comparison of demand measures of order no. 21 of the FSTEC of Russia and ways of implementation in the subsystem of the information system of personal data protection, the

recommendations for inspections of specific measures of protection and used technology audit technical means. The developed method is tested on the example of conducting an audit in “Lama” LLC company. The choice was made to establish the compliance of the organization’s personal data protection system with the requirements of order no. 21 of the FSTEC of Russia. Recommendations have been developed to eliminate the existing shortcomings and inconsistencies by re-equipping the anti-virus protection subsystem and the subsystem of inter-network shielding and protection of communication channels.

Key words: information security, audit of the information security system, technical means of audit, protection of communication channels, anti-virus protection.