УДК 004.492
DOI: 10.33764/2618-981X-2021-6-268-275

ВОПРОСЫ АВТОМАТИЗАЦИИ ПРОВЕДЕНИЯ АУДИТА В СООТВЕТСТВИИ С ГОСТ Р 57580.2-2018

Анастасия Вадимовна Ситская
Новосибирский государственный технический университет, 630073, Россия, г. Новосибирск, пр. Карла Маркса, 20, магистрант, тел. (999)450-93-11, e-mail: AnSits@yandex.ru

Валерия Александровна Табакаева
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант кафедры фотоники и приборостроения, тел. (962)831-22-52, e-mail: tabakaeva1997@mail.ru

Валентин Валерьевич Селифанов
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, доцент кафедры информационной безопасности, тел. (923)247-25-81, e-mail: sfo1@mail.ru

Современный мир можно охарактеризовать огромным объемом информации и компьютеризацией всех сфер деятельности человека. Информация, касающаяся финансовой сферы, становится одной из наиболее важных. Именно инциденты информационной безопасности в финансовых организациях могут привести не только к нарушению интересов отдельного клиента, но и к кризису финансового рынка всей страны. Аудит информационной безопасности позволяет своевременно обнаружить нарушения в информационной системе организации, что значительно повышает безопасность информации. Зачастую своевременное и быстрое получение качественной и количественной оценки уровня безопасности позволяет избежать инцидента.

Для повышения точности оценок и сокращения времени их получения необходима автоматизация процесса проведения аудита, для чего было разработано приложение «Аудит57580», актуальность которого рассмотрена в статье.

Ключевые слова: информационная безопасность, ГОСТ Р 57580.1-2017, ГОСТ Р 57580.1-2018, информационная безопасность финансовых организаций, аудит информационной безопасности, аудит финансовых организаций, актуальность разработанного приложения

ISSUES OF AUTOMATION OF THE AUDIT IN ACCORDANCE WITH GOST R 57580.2-2018

Anastasia V. Sitskaya
Novosibirsk State Technical University, 20, K. Marks Prospekt, Novosibirsk, 630073, Russia, Graduate, phone: (999)450-93-11, e-mail: AnSits@yandex.ru

Valeria A. Tabakaeva
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, Department of Photonics and Device Engineering, phone: (962)831-22-52, e-mail: tabakaeva1997@mail.ru

Valentin V. Selifanov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Associate Professor of the Department of Information Security, phone: (923)247-25-81, e-mail: sfo1@mail.ru

The modern world can be characterized by a huge amount of information and computerization of all spheres of human activity. But one of the most valuable information can be considered the information that concerns financial organizations. There are incidents of information security in financial organizations that can lead not only to the violation of the interests of an individual client, but also to the crisis of the financial market of the entire country. Information security audit allows you to detect violations in the organization's information system in a timely manner, which significantly increases the security of information. Often, timely and rapid receipt of a qualitative and quantitative assessment of the level of security allows you to avoid an incident.

To improve the accuracy of estimates and reduce the time of their receipt, the application "Audit57580" was developed, the relevance of which is discussed in detail in the article.

Keywords: information security, GOST R 57580.1-2017, GOST R 57580.1-2018, information security of financial organizations, information security audit, audit of financial organizations

Введение

На данный момент быстрый темп развития информационных технологий ведет наш мир к компьютеризации всех сфер деятельности человека, что говорит об информации как о наивысшей ценности. Информация может быть ценна для отдельного человека или же для всей страны, именно такую информацию необходимо защищать. Одна из областей информации, представляющая ценность как для отдельного человека, так и для всей страны в целом - это область информации, касающаяся финансовой сферы, а именно деятельности финансовых организаций. Можно сказать, что именно от функционирования финансовых организаций зависит благосостояние каждого человека и страны в целом.

Наступление инцидента информационной безопасности может привести как к нарушению интересов отдельного клиента финансовых организаций, так и к возникновению кризиса финансового рынка целой страны. Именно поэтому наибольшую опасность несут в себе угрозы по отношению к информационной безопасности, и именно безопасность информации для финансовых организаций стала приоритетной.

Инциденты информационной безопасности могут быть преднамеренными или случайными, вызванные как техническими, так и не техническими средствами. Последствиями инцидента могут быть несанкционированное раскрытие информации или ее изменение, нанесение ущерба активам организации или их хищение.

Методы и материалы

Существует неограниченное количество инцидентов в области информационной безопасности банковской сферы, но их можно разделить на три основные категории:

– отказ в обслуживании;

– сбор информации;

– несанкционированный доступ.

Далее рассмотрим каждую категорию инцидентов подробно.

Отказ в обслуживании. Инциденты данной категории приводят к неспособности систем, сервисов или сетей продолжать функционирование в полном объеме или же приводит к полному отказу в доступе авторизованным пользователям. На настоящий момент подразделяют два типа инцидентов данной категории, связанных с отказом в обслуживании техническими средствами: уничтожение ресурсов и истощение ресурсов (то есть замедление работы технических средств, блокирование или разрушение).

Технические инциденты могут быть случайными и неслучайными. Случайные могут возникать в следствии ошибки конфигурации, допущенной оператором, или же несовместимости программного обеспечения. Преднамеренные инциденты могут инициировать разрушение системы, сервиса или снижать производительность сети (например, зондирование сети, передача данных в непредусмотренном формате и др.). Но также бывает, что инциденты могут быть последствиями иной вредоносной деятельности по отношению к информационной системе организации.

К нетехническим нарушениям данной категории можно отнести нарушения, которые могут быть вызваны такими факторами как нарушение систем физической защиты, что может привести к хищению или преднамеренному нанесению ущерба оборудованию; нанесение ущерба оборудованию под воздействием окружающей среды (высокая температура воздуха, непосредственная близость огня или воды); перегрузка системы и др.

Сбор информации. Данная категория инцидентов подразумевает действия, связанные с получение необходимой информации об организации (определение потенциальных уязвимостей сетевой среды, информация о сетевой топологии и т.п.). Инциденты могут быть вызваны нарушениями физической защиты безопасности или неправильно конфигурированными операционными системами по причине неконтролируемых изменений в системе или неправильным функционированием программного или аппаратного обеспечения, что приводит к хищению и раскрытию информации, содержащей значимые данные. Примерами таких инцидентов могут быть сбрасывания записей DNS (англ. Domain Name System), отправка текстовых запросов по случайным сетевым адресам для нахождения работающей системы, зондирование системы для идентификации операционной системы хоста, сканирование доступных сетевых портов на протокол передачи файлов системе с целью идентификации соответствующих сервисов (например, электронная почта, протокол FTP, сеть и т.д.) и версий программного обеспечения этих сервисов) и др.

Инциденты данной категории, создаваемые нетехническими средствами, приводят к таким последствиям как прямое или косвенное раскрытие информации, мо-

дификации информации, нарушение учетности (например, при регистрации учетных записей), неправильному использованию информационных систем и др.

Несанкционированный доступ. Данная категория инцидентов содержит в себе инциденты, не вошедшие в предыдущие две категории, и заключается в несанкционированных попытках получения доступа в информационную систему организации. К техническим нарушениям относятся попытки извлечения файлов с паролями, попытки расширения привилегий доступа к ресурсам или информации и др.

К нетехническим инцидентам данной категории относятся нарушения, вызванные такими факторами как разрушение устройств физической защиты или неправильной конфигурацией операционной системы вследствие неконтролируемых изменений в системе или неправильного функционирования программного или аппаратного обеспечения.

Для обеспечения информационной безопасности финансовых организаций и предотвращения инцидентов Банком России был разработан ГОСТ Р 57580.1-2017. Данный документ определяет уровни защиты информации и соответствующие им необходимый перечень организационных и технических мер, обеспечивающих защиту информации финансовой организации.

Для работы с документом необходимо знать тип лицензии финансовой организации. На сегодняшний день существует два типа лицензии, которые сопровождаются соответствующим уровнем обеспечения безопасности:

– базовая. 1 уровень защиты информации;

– универсальная. 2 и 3 уровни безопасности.

Каждая из лицензий несет в себе те или иные ограничения и условия для деятельности банков. Например, базовая лицензия несет в себе по большей части ограничения в работе с некоторыми типами клиентов и ценных бумаг. Банки с универсальной лицензии имеют меньше ограничений, но больше требований к уровню организации информационной безопасности. Третий уровень безопасности необходим для системно значимых банков. Системно значимые банки – банки, от деятельности которых зависит устойчивость всей банковской системы страны. Банки, которые практически не имеют ограничений по работе и не являются системно значимыми, организуют второй уровень обеспечения безопасности информации.

Результаты

Для достижения банками эффективной защиты информации необходимо не только соблюдение мер, описанных в ГОСТ Р 57580.1-2017 и соответствующих установленному уровню защиты финансовой организации, но и объективная оценка защиты информации сторонней организацией, а именно аудит.

На настоящий момент устоявшегося определения «аудит информационной безопасности» нет. Однако наиболее стремительно развивающимся направлением в области безопасности информационных систем является именное аудит информационной безопасности. Основной задачей аудита является объективная

оценка уровня защиты информации информационной системы организации. В процессе аудита происходит сбор и анализ информации о безопасности информационной системы организации, на основе которой осуществляется качественная и количественная оценка уровня обеспечения информационной безопасности организации. Сам процесс аудиторской проверки можно разделить на следующие этапы:

– определение задачи аудита и границ работы. На данном этапе происходит формирование целей и задач проведения аудита, а также методов проведения проверки в заданных организацией рамках, также формируется состав проверяющей группы;

– сбор и анализ информации. Данный этап характеризуется сбором информации о состоянии информационной безопасности организации и последующий ее анализ с целью оценки результатов проверки, и составление рекомендация по устранению нарушений. Формируется отчет о результатах проверки, включающий в себя качественную и количественную оценки уровня защиты информационной системы организации;

– формирование отчета. На данном этапе аудита формируется итоговый отчет, включающий в себя не только оценки уровня защиты, но и разработка плана по устранению выявленных в ходе проверки уязвимостей в обеспечении информационной безопасности организации.

Опираясь на вышесказанное можно дать определение понятию аудита информационной безопасности: аудит информационной безопасности – это процесс получения качественной и количественной оценок уровня защиты информации, основанных на полученной информации об информационной системе организации и последующим ее анализе, а также разработка плана устранения выявленных уязвимостей информационной системы.

На настоящий момент большинство отраслей любого вида деятельности достигли высоко уровня автоматизации, в то время как аудиторы, по данным исследований, проводимых Институтом профессиональных бухгалтеров и аудиторов России, практически не используют специализированные программы, предпочитая использовать программы общего назначения, такие как продукты Microsoft office или подобные им. Такой подход существенно замедляет работу аудиторов, в то время как автоматизация некоторых этапов работы позволит увеличить качество работы и уменьшить затрачиваемое время на ее выполнение. Можно выделить некоторые причины неприменения в аудиторской деятельности специального программного обеспечения:

– необходимость в освоении сложного программного обеспечения, что ведет за собой нежелание использования сложных программ, которые требуют времени для их освоения;

– разный уровень компьютерной грамотность аудиторов;

– выездной характер работы, что является помехой, если программное обеспечение нельзя использовать на посторонних ПК;

– отсутствие единого подхода к проведению аудита;

– и др.

Перечисленные проблемы не являются единственными, но многие из них устранимы, при использовании разработанного приложения «Аудит57580». Данное приложение может использовать аудитор с любым уровнем компьютерной грамотности, т.к. оно просто в использовании и сравнимо с простым заполнением таблицы. Приложение не требует специального обучения работы с ним, интерфейс и этапы работы с приложением понятны на интуитивном уровне. Аудитор последовательно заполняет таблицы, построенные по образцам ГОСТа Р 57580.2-2018, который был разработан Банком России для проведения аудита финансовых организаций. Данный документ устанавливает единые требования к методике проведения аудита и оформлению результатов оценок, полученных в процессе проверки, соответствия уровню защиты, установленного финансовой организацией. При этом от аудитора требуется заполнение только пунктов, касающихся оценок и реализации мер, все остальные данные уже заполнены программой.

Проведения аудита без автоматизации весьма трудоемкий и длительный процесс, при этом есть случаи, требующие быстрого результата. Финансовые организации требуют наиболее качественной защиты информации, и при проведении аудита именно время получения объективной оценки может повлиять на скорость устранения нарушений, а также при необходимости принятия решения для организации дополнительных организационных и технических мер безопасности для повышения уровня защиты информационной системы организации, что может предотвратить инциденты защиты информации.

Приложение «Аудит57580» разработано именно для сокращения времени получения точного значения количественной оценки, и в соответствии с ее значением позволяет быстро получить качественную оценку уровня защиты информации финансовой организации. Разработанное приложение целесообразно использовать на последнем этапе аудита, т.к. оно создано именно для частичного формирования отчета.

ГОСТ Р 57580.2-2018 предусматривает в себе множество формул, которые необходимы для получения количественной и качественной оценок безопасности информационной системы организации. В то же время каждая формула имеет большое количество отсылок к различным таблицам, которые заполняет аудитор в процессе сбора информации, что требует от процесса расчета оценки предельного внимания при обращении к заполненным ранее таблицам, а также определенное количество времени. А в случае, когда у организации построено несколько разноуровневых контуров, то процесс заполнения таблиц и работа с формулами требует еще больше времени.

Именно на данном этапе приложение становится актуальным, поскольку позволяет увеличить точность расчетов, а также сократить время на получение количественной оценки соответствия уровню защиты информации, установленного финансовой организации. Увеличение точности расчетов достигается тем, что от аудитора не требуется постоянного обращения к таблицам, достаточно единовременное последовательное их заполнение в программе. В свою очередь

приложение позволяет получить точную оценку уровня защиты информации непосредственно в момент завершения проведения аудита, это возможно благодаря тому, что аудитор, используя приложение может заполнять таблицы ГОСТа во время проведения аудиторской проверки.

Результатом работы программы является документ Excel, в котором содержатся заполненные таблицы, расчётные формулы со значениями, а также количественная и качественная оценки, при этом количественная оценка содержит в себе не только значение, но и комментарии, подробно описывающие полученный результат.

Данное приложение будет наиболее полезно аудиторам, работающим непосредственно с финансовыми организациями, а также с организациями, использующие для построения системы защиты информационных систем ГОСТ Р 57580.1-2017. Данное приложение будет доступно любой организации, занимающейся аудиторской деятельности, его распространение происходить в глобальной сети Интернет посредством специально разработанного сайта (audit.gost57580.ru) на котором содержатся подробная инструкция использования приложения, а также документы ГОСТ Р 57580.1-2017, который доступен для скачивания как в полном объеме, так и для удобства работы разделенный в соответствии с процессами и направлениями, ГОСТ-57580.2-2018.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ Р 57580.1-2017 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер. введ. 2018-01-01. URL: http://docs.cntd.ru/document/1200146534 (Дата обращения: 1.02.2021).

2. ГОСТ Р 57580.2-2018 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия. введ. 2018-09-01. URL: http://docs.cntd.ru/document/1200158801 (Дата обращения: 1.02.2021).

3. ГОСТ Р ИСО 19011-2012 Руководящие указания по аудиту систем менеджмента. введ. 2013-02-01. URL: http://docs.cntd.ru/document/1200095049 (Дата обращения: 5.02.2021).

4. ГОСТ Р ИСО/МЭК ТО 18044-2007 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности (Переиздание). URL: http://docs.cntd.ru/document/1200068822 (Дата обращения: 5.02.2021).

5. Крупко А.Э. Политика информационной безопасности: состав, структура, аудит информационной безопасности // ФЭС: Финансы. Экономика. 2015. №8. С. 27-32. URL: https://www.elibrary.ru/item.asp?id=24315377 (Дата обращения: 10.02.2021).

6. Макаренко С.И. Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий // Системы управления, связи и безопасности. 2018. №1. URL: https://sccs.intelgr.com/20181.html (Дата обращения: 10.02.2021).

7. РС БР ИББС-2.2-2009 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности. 2010. URL: http://docs.cntd.ru/document/902189338 (Дата обращения: 30.03.2021).

8. Палканов И.С., Рачков В.Е. Внутренний аудит информационной безопасности как инструмент объективных оценок состояния информационной безопасности организации // Сту-

денческая наука для развития информационной общества. Сборник материалов X Всероссийской научно-технической конференции с международным участием 2019. 2019. 153-161 С. URL: https://www.elibrary.ru/item.asp?id=43101860(Дата обращения: 1.04.2021).

9. Астахов А. Введение в аудит информационной безопасности // Доклад. 2018. URL: http://globaltrust.ru(Дата обращения: 10.04.2021).

10. Кульба В. В., Шелков А. Б., Гладков Ю. М., Павельев С. В. Мониторинг и аудит информационной безопасности автоматизированных систем. 2009. URL: https://search.rsl.ru/ru/record/01004328988 (Дата обращения: 10.04.2021).