САМОРЕГУЛИРУЕМАЯ ОРГАНИЗАЦИЯ АУДИТОРОВ
АССОЦИАЦИЯ «СОДРУЖЕСТВО»
член Международной Федерации Бухгалтеров (IFAC)
(ОГРН 1097799010870, ИНН 7729440813, КПП 772901001)
119192, г. Москва, Мичуринский проспект, дом 21, корпус 4.
т: +7 (495) 734-22-22, ф: +7 (495) 734-04-22, www.auditor-sro.org, info@auditor-sro.org

ПРОТОКОЛ № 7
заседания Комитета по ИТ и кибербезопасности Саморегулируемой организации аудиторов Ассоциации «Содружество»

г. Москва **28 июня 2024 года**

Форма заседания: Очная

Члены Комитета, принявшие участие в заседании: Стрий Л.В., Богров Е.Г., Орлов А.В., Бареев Т.Ф., Комиссарова О.В., Брюханов М.Ю., Кушнарев А.С, Зубков А.С., Винокуров Д.М., Полавская Н.В.

Итого в заседании Комитета по ИТ и кибербезопасности (далее - Комитет) участвует 9 из 10 человек, что составляет 90% голосов.
Кворум для принятия решений имеется.
Председатель заседания – Стрий Л.В.

Повестка дня:

1. Утвердить дополнения к Обзору информационных технологий для решения вопросов автоматизации при выполнении аудита финансовой отчетности и документировании его результатов в соответствии с МСА и применимыми законодательными и нормативными требованиями в ответ на решение Правления (протокол № 641 от 22.09.2023) по вопросу 18.3.
2. Утвердить проект Методические рекомендации по обеспечению защиты информации при оказании услуг общественно-значимым организациям на финансовых рынках.
3. Председателю Комитета предложить кандидатуру Заместителя председателя Комитета – Орлова А.В.

Решение, поставленное на голосование:
1. Утвердить Дополнения с учетом поступивших предложений.
2. Утвердить проект с учетом поступивших предложений.
3. Избрать Заместителем председателя Комитета по ИТ и кибербезопасности – Орлова А.В.

Результаты голосования по первому вопросу:
ЗА – 9 чел.
ПРОТИВ – 0 чел.

ВОЗДЕРЖАЛСЯ – 1 чел.
Решение принято

Результаты голосования по второму вопросу:
ЗА – 9 чел.
ПРОТИВ – 0 чел.
ВОЗДЕРЖАЛСЯ – 1 чел.
Решение принято

Результаты голосования по третьему вопросу:
ЗА – 9 чел.
ПРОТИВ – 0 чел.
ВОЗДЕРЖАЛСЯ – 1 чел.
Решение принято

Подсчет голосов производила Председатель Комитета Л.В. Стрий.

К настоящему протоколу прилагаются:
1. Дополнения (Приложение 1)
2. Проект (Приложение 2)

Председатель Комитета **Л.В. Стрий**

Приложение 1

САМОРЕГУЛИРУЕМАЯ ОРГАНИЗАЦИЯ АУДИТОРОВ
АССОЦИАЦИЯ «СОДРУЖЕСТВО»
член Международной Федерации Бухгалтеров (IFAC)
(ОГРН 1097799010870, ИНН 7729440813, КПП 772901001)
119192, г. Москва, Мичуринский проспект, дом 21, корпус 4.
т: +7 (495) 734-22-22, ф: +7 (495) 734-04-22, www. sroaas.ru, info@sroaas.ru

Исх. №
От 14 июня 2024 года

Генеральному директору СРО ААС
Носовой О.А.

Уважаемая Ольга Александровна!

В связи с решением Правления (протокол № 641 от 22.09.2023) по вопросу 18.3 подготовлены разъяснения к «Обзору информационных технологий для решения вопросов автоматизации при выполнении аудита финансовой отчетности и документировании его результатов в соответствии с МСА и применимыми законодательными и нормативными требованиями» (февраль 2023 г.) Комитета СРО ААС по ИТ и кибербезопасности (далее - Обзор) (ПРОТОКОЛ к данному Письму).

Приложение: 2 листа.

С уважением,

Председатель Комитета
СРО ААС по ИТ и кибербезопасности Л.В. Стрий

П Р О Т О К О Л

Совещания Комитета СРО ААС по ИТ и кибербезопасности

От 14 июня 2024 г.

Присутствовали:

Председатель Комитета СРО ААС по ИТ и кибербезопасности	- Л.В. Стрий
Заместитель Председателя Комитета СРО ААС по ИТ и кибербезопасности	- А.В. Орлов
Члены Комитета СРО ААС по ИТ и кибербезопасности	- Н.В. Полавская, А.С. Кушнарев, Д.М. Винокуров, О.В. Комиссарова, Т.Ф. Бареев, М.Ю. Брюханов, А.С. Зубков, Е.Г. Богров

По итогам состоявшегося обсуждения сформированы следующие тезисы:

1. Почему в Обзор включены только программы: AuditXP, IT Audit и Case Ware?

В ходе подготовки Обзора Комитетом было принято решение сосредоточится исключительно на тиражном ПО, представленном на российском рынке.
При этом, был выработан ряд критериев для их отбора:

- ПО должно соответствовать определению «**Тиражное программное обеспечение (ПО)**» — это любой законченный программный продукт, доступный всем на рынке.
  В идеале процессы загрузки, установки, регистрации, покупки лицензии и настройки программы должны быть максимально автоматизированы и происходить без участия вендора (разработчика).
  Альтернативой тиражным решениям является индивидуальная разработка. Она позволяет получить уникальный с точки зрения дизайна и функционала продукт.
- Разработчик ПО должен **прямо** позиционировать свой продукт как **решение для автоматизации аудиторской деятельности**.
  Т.е. ПО должно обладать какими-то характеристиками для автоматизации именно аудита, а не просто иметь возможность адаптации его функциональности для этих целей.
  В противном случае нам пришлось бы рассматривать огромное количество ПО, которое можно применять или кем-то уже применяется при аудите. Например, MS Office (Excel, Word…), ПО для управления проектами и т.д.
- Несколько не связанных между собой членов СРО ААС **уже должны использовать данное ПО** в своей деятельности на постоянной основе.
  Это было необходимо для получения обратной связи по опыту использования ПО в аудиторской деятельности, более полного и всестороннего изучения продуктов.

В результате в финальную версию Обзора вошли две программы от российских разработчиков (AuditXP, IT Audit) и одна канадского (Case Ware).

2. Почему Case Ware не исключена из Обзора?

Следует учитывать, что подготовка к Обзору началась до 2022 года и Комитетом уже был собран и проанализирован большой объем информации. В том числе и по данной программе.
Несмотря на то, что программа Case Ware в начале 2022 года фактически ушла с российского рынка, а продолжение ее использования несло дополнительно и инфраструктурные риски в сложившихся условиях, было принято решение оставить ее в Обзоре по следующим соображениям:

- Программу Case Ware уже использовали в своей деятельности многие члены СРО ААС, и им нужно было принимать решение о смене ПО;
- Прямое сравнение с иностранным ПО дает более полную картину по конкурентоспособности российских программ.

3. Почему нет оценки долей рынка того или иного ПО, вошедшего в Обзор?

Комитетом еще на этапе отбора ПО для Обзора была проведена экспресс-оценка долей рынка. Оценка проводилась на основании данных:

- о количестве пользователей, полученных от разработчиков данного ПО и результатам опроса членов СРО ААС об используемом в своей работе ПО;
  45% аудиторских организаций используют AuditXP Professional, 15% - IT Audit, 5% - используют Case Ware и собственное ПО.

В результате обсуждения Комитетом было принято решение не включать информацию о доле рынка в Обзор по следующим основаниям:

- Невозможно без глубокого исследования точно определить долю рынка того или иного ПО;
- Есть аудиторские организации, которые одновременно используют несколько программ;
- Слишком большой перевес в сторону одного из продуктов может сформировать предвзятое мнение о его функциональном превосходстве.

4. Почему в Обзоре нет разработки ООО "Аудит-НТ"?

На момент подготовки Обзора (февраль 2023) мы не смогли найти информацию подтверждающую, что есть еще какое-то ПО на рынке. Сайт программы не работал уже больше года. На сайте ООО "Аудит-НТ"(https://audit-nt.ru/) какой-либо информации о ПО для аудита на дату подготовки Обзора уже не было. С пользователями их ПО "не сталкиваемся" в ходе опроса аудиторов. О других сайтах информация у Комитета отсутствовала.
В июне 2024 после получения информации от Романовой Светланы Игоревны, что ПО все-таки еще существует Заместитель председателя Комитета Орлов Александр Владимирович нашел информацию о данном ПО (АИС «АУДИТ») на сайте https://ant-konsalt.ru/it-produkt/AIS-audit.php.

На данный момент попытки получить информацию о продукте не увенчались успехом. При звонке по городскому номеру с сайта сотрудник не с первого раза понял вообще о какой программе идет речь. После дал мобильный номер сотрудника с кем можно поговорить об этой программе. Связаться с ним не удалось, т.к. номер не обслуживается.

На момент формирования Обзора, по нашему мнению, данное ПО не являлось тиражным решением и не подходило под критерии Обзора.

На 2024 год Комитетом планируется актуализировать информацию об аудиторском ПО и

подготовить в начале 2025 года новый актуальный Обзор, в который в случае получения информации от других разработчиков, в том числе и АИС «АУДИТ», будет включено и другое ПО.

Приложение 2

РЕКОМЕНДОВАНО

СРО ААС

Методические рекомендации
по обеспечению защиты информации
при оказании услуг общественно-значимым организациям на финансовых рынках.

Настоящие Методические рекомендации на основании пункта 3.2 Устава СРО ААС, части 2 статьи 1 Федерального закона от 30.12.2008 N 307-ФЗ "Об аудиторской деятельности», статьи 76.9-6 Федерального закона от 10 июля 2002 года N 86-ФЗ "О Центральном банке Российской Федерации (Банке России)», определяют:

обязательные для аудиторских организаций, являющихся членами СРО ААС (далее – АО), оказывающих профессиональные услуги общественно-значимым организациям на финансовых рынках (ОЗОФР), подходы и требования к обеспечению защиты информации.

Глава 1. Общие положения

1.1. АО в целях реализации требований к обеспечению защиты информации при оказании профессиональных услуг клиенту, относящемуся к ОЗОФР (далее – Клиент, требования к обеспечению защиты информации), применяемых в отношении автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация и использование которых обеспечивается при оказании профессиональных услуг ОЗОФР (далее - объекты информационной инфраструктуры), должны применять меры защиты информации, основанные на выполнении требований, изложенных в данном документе.

Глава 2. Требования к обеспечению защиты информации

2.1. АО должны обеспечить защиту информации, получаемой, подготавливаемой, обрабатываемой, передаваемой, хранимой и уничтожаемой (при прекращении хранения и обработки) АО с использованием автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования (далее при совместном упоминании – объекты информационной инфраструктуры) в рамках:

a) обеспечения защиты информации при управлении доступом;

b) обеспечения защиты вычислительных сетей;

c) контроля целостности и защищенности объектов информационной инфраструктуры;

d) защиты от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (далее – вредоносные коды);

e) предотвращения утечек информации;

f) управления инцидентами защиты информации;

g) защиты среды виртуализации;

h) защиты информации при осуществлении удаленного логического доступа с

использованием мобильных (переносных) устройств.

2.2. АО должны определить во внутренних документах состав и порядок применения организационных и технических мер в рамках процессов (направлений) защиты информации, указанных в пункте 2.1 настоящих Методических рекомендаций.

2.3. В зависимости от типов обрабатываемой информации (аудиторская документация, персональные данные и т.д.) АО могут сформировать один или несколько контуров безопасности, задействованных в процессе оказания аудиторских услуг ОЗОФР, для которых может быть установлен разный уровень защиты информации.

2.4. АО должна обеспечить уровень защиты не ниже 3 (минимальный) информации и соответствующие им требования к содержанию базового состава мер защиты информации.

2.5. При выборе средств защиты рекомендуется использовать сертифицированные российские программные продукты и технические средства.

Глава 3. Требования к системе защиты информации

3.1. Физическая защита

В помещениях, в которых находится сетевое и коммуникационное оборудование, а также происходит работа с защищаемой информацией, должна быть организована защита от несанкционированного доступа. Данная система включает в себя как физические средства, такие как барьеры, двери, так и технические – охранные системы, системы контроля и наблюдение. Кроме того, необходимо обеспечить бесперебойное питание оборудования и устройств.

3.2. Управление доступом

Управление доступом включает в себя меры по идентификации и аутентификации субъектов доступа и объектов доступа. Они должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности). В тоже время меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил. Периодически должен проводиться аудит прав доступа призванный выявить как отдельные несоответствия, так и принципиальные недочёты в самой системе назначения прав.

3.3. Регистрация и учет

Должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова.

3.4. Обеспечение целостности

Должна быть обеспечена возможность регистрации событий безопасности в том числе сбор, запись, хранение и защита информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

3.5. Антивирусная защита

Должны быть установлены антивирусное и антишпионское программное обеспечение обеспечивающее обнаружение в информационной системе компьютерных программ либо иной

компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации. Данное программное обеспечение должно быть централизовано для решения задач реагирования на инциденты и регулярного обновления.

3.6. Межсетевой экран

Для контроля трафика в сети и предотвращения несанкционированного доступа должны быть установлены межсетевые экраны (файрволлы, брэндмауэры). Эти системы обеспечивают фильтрацию входящего и исходящего трафика на основе заранее установленных правил безопасности, позволяя предотвратить неавторизованный доступ к ресурсам сети и защитить данные от вредоносных атак.

3.7. Патч-менеджмент

Необходимо проводить регулярное обновление программного обеспечения и операционных систем для закрытия уязвимостей.

3.8. Резервное копирование

Регулярное создание резервных копий данных позволит быстро восстановить работоспособность системы в случае ее повреждения в результате вредоносного воздействия.

3.9. Защита среды виртуализации

Меры по защите среды виртуализации должны исключать несанкционированный доступ к данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

3.10. Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств

Двухфакторная аутентификация: Использование не только пароля, но и другого второго фактора для подтверждения личности пользователя, например, одноразового пин-кода, биометрических данных или аппаратного токена.

Удаленное управление устройством: В случае утери или кражи устройства должна быть возможность удаленно блокировать или даже удалить все конфиденциальные данные.

Использование виртуальных частных сетей (VPN): VPN создает защищенное соединение между мобильным устройством и корпоративной сетью, обеспечивая защиту данных от несанкционированного доступа.

3.11. Организационные меры защиты

АО должна разработать политику безопасности, которая будет регулировать использование устройств, обмен информацией и доступ к данным. В том числе, политика должна включать раздел по использованию мобильных устройств, включая требования по безопасности и контроль за установкой приложений.

АО должна проводить регулярное обучение сотрудников по вопросам безопасности информации, в том числе инструктажи по безопасности информации при удаленном доступе.

Глава 4. Управление инцидентами

4.1. Управление инцидентами защиты информации – это процесс обнаружения, реагирования и решения инцидентов, которые влияют на информационную безопасность организации. Это включает в себя следующие основные шаги:

a) Обнаружение инцидентов: Важно иметь системы мониторинга и обнаружения, которые могут предупреждать об инцидентах безопасности. Это могут быть системы сбора журналов, системы мониторинга сети, системы обнаружения вторжений и т. д.

b) Реагирование на инциденты: Когда происходит инцидент, необходимо немедленно реагировать, чтобы минимизировать ущерб и восстановить безопасность. Это может включать в себя изоляцию компрометированных систем, блокировку уязвимостей, изменение паролей и прочие меры по восстановлению безопасности.

c) Инцидентный отклик: Когда инцидент произошел, следует провести оценку его масштаба и последствий, определить его природу, классифицировать его по уровню угрозы и принять меры по предотвращению будущих инцидентов.

d) Обучение и улучшение: После завершения инцидента, важно провести анализ произошедшего, чтобы извлечь уроки и улучшить процессы защиты информации. Также важно обучить персонал организации, чтобы они могли более эффективно реагировать на будущие инциденты.

Глава 6. Оценка соответствия

При оценке соответствия необходимо руководствоваться "ГОСТ Р 57580.2-2018. Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия" (утв. и введен в действие Приказом Росстандарта от 28.03.2018 N 156-ст).