РОЛЬ АУДИТА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Клочкова Т.В.

Клочкова Тамара Владимировна – магистрант,
кафедра информационных систем и телекоммуникаций,
факультет информатики и систем управления,
Московский государственный технический университет им. Н.Э. Баумана,
г. Москва

Аннотация: *в статье рассматривается уровень защищенности конфиденциальной информации на предприятиях и средства борьбы с утечками данных. Помимо этого поднимается вопрос о необходимости аудита информационных технологий на предприятиях, а именно – аудита систем информационной безопасности, обосновывается важность проведения процесса проверки.*
Ключевые слова: *информационные технологии, ИТ-аудит, аудит информационных систем, аудит информационной безопасности, информационная безопасность.*

В XXI веке информационные технологии проникают во все сферы человеческой жизни. Они являются немаловажным ресурсом во многих современных компаниях, осуществляющих свою деятельность в различных профессиональных областях. Однако с доступностью информационных технологий, их активным развитием и использованием в бизнесе пришли и негативные последствия в виде утечки конфиденциальной информации, корпоративных сведений, данных клиентов, которые используются предприятиями. Продукты информационной безопасности стали как никогда актуальны. Многие разработанные ИТ-решения, направленные на сокращение рисков бизнеса и предотвращение утечек конфиденциальной информации, помогли предотвратить часть угроз.

Программные продукты для информационной безопасности предприятия, различные информационные системы, до сих пор продолжают совершенствоваться и издаваться, однако изменяется и противоборствующая сторона: возникают новые типы угроз, появляются другие возможности для утечек корпоративной информации в сеть и др. Одновременно со всеми этими происшествиями претерпевает изменения и бизнес-среда. В современных реалиях многие компании пользуются услугами аутсорсинга, облачными решениями, сторонними платформами, вследствие чего ставят под угрозу свою корпоративную информацию.

Несмотря на развитие информационных технологий, постоянно растет количество сообщений об инцидентах, связанных с нарушением

обязательств и прав сотрудниками различных организаций. Ущерб от злонамеренных действий исчисляется десятками тысячи рублей, и это только в России. Недавние исследования InfoWatch, проведенные в 2019 году, продемонстрировали, что за последние 12 лет зарегистрировано около 14 тысяч утечек конфиденциальной информации из коммерческих компаний и государственных организаций. Несмотря на все действия, которые предпринимаются бизнесом, общественными организациями и государством, полностью остановить утечки пока не удается. Всего с 2007 года на январь 2019 года утекло более 30 млрд записей персональных данных, в том числе более 20 млрд за последние два года [1, 2, 3].

Распространение конфиденциальной информации – это серьёзная проблема, влияющая на деятельность организации, поэтому вопрос о выборе информационных систем, способных сократить подобные риски, по сей день актуален. Рынок ИТ-продуктов изобилует решениями для разных областей, отсутствует дефицит товара, однако количество и разнообразие не гарантируют отличной защищенности. Как для бизнеса, так и для ИТ-компаний, разрабатывающих продукты в сфере информационной безопасности, важно то, насколько качественно система информационной безопасности будет выполнять свои задачи в бизнес-процессах организации, которая её использует.

Повлиять на процент утечек информации, уменьшить его может не только совершенствование систем информационной безопасности, но и процесс проверки информационных систем, то есть их аудит. Под аудитом информационных технологий понимается процесс получения систематизированных и объективных данных о текущем состоянии информационных технологий [4]. Техническим аудитом является сбор и анализ информации с последующим формированием рекомендаций по оптимизации работы конкретного элемента ИТ-инфраструктуры [4]. Благодаря аудиту выявляются уязвимые места, недостатки. Процесс аудита играет важную роль в повышении качества создаваемых ИТ-решений, а также в снижении количества инцидентов, связанных с утечкой конфиденциальных данных. Важно понимать, что процесс аудита занимает продолжительное время, поэтому он должен видоизмениться в соответствии с требованиями современного мира.

На основании вышеизложенного можно сказать, что информационные системы, которые используют компании для обеспечения сохранности собственных данных, важны, и именно поэтому должное внимание следует уделять их проверке и составлению рекомендаций для последующего улучшения.

В век развитых информационных технологий процесс аудита всячески автоматизируется. Представители аудиторских компаний используют в своей работе отдельные продукты для составления конечных заключений и рекомендаций. Иногда аудиторы проводят тест на проникновение

(показательная демонстрация действий нарушителя), помимо этого, их проверка включает в себя анализ параметров конфигурации информационной системы, применение сканера уязвимостей, например, таких программ как «Nessus» от Tenable Network Security, «OpenVAS» от Greenbone Networks GmbH, «Retina Network Security Scanner» от BeyondTrust, и, наконец, составление итогового отчёта, в котором формируются рекомендации на основании выявленных «узких мест». Общее описание продуктов представлено в таблице 1.

Таблица 1. Используемые в процессе ИТ-аудита сканнеры уязвимостей

Название продукта	**Основная направленность**	**Сфера применения продукта**	**Возможности**	**Особенности**
Nessus	Анализ защищённости информационной системы	Аудит конфигураций и содержимого	Выполняет работа по всему жесткому диску систем Windows и Unix с целью поиска неразрешенного содержимого, тестирование на проникновение	Сканер может быть использован для входа на серверы под управлением ОС Unix и Windows, в системы устройств Cisco, системы SCADA, серверы IBM iSeries и базы данных для определения того, настроены ли они в соответствии с локальной политикой безопасности объекта
OpenVAS	Анализ защищённости информационной системы	Активного мониторинг узлов вычислительной сети на предмет наличия проблем, связанных с безопасностью,	Сканирование открытых портов, имитация атаки	Открытый исходный код

		оценка серьезности этих проблем		
Retina Network Security Scanner	Сетевой анализ	Нахождение уязвимостей в сети, в базах данных, тестирование на проникновение	Определение и анализ хостов локальной сети, определение уязвимости ОС и потенциально опасных настроек, тестирование на проникновение	Открытая архитектура, позволяющая разрабатывать тесты безопасности, учитывающие специфику организации

Исходя из представленных в таблице данных, можно сказать, что сканнеры уязвимостей могут положительно влиять на процесс проведения аудита информационных систем безопасности предприятия, упрощать и ускорять его, однако лицензии на указанные программные продукты, кроме «OpenVAS», находящимся в свободном распространении, достаточно дорогие, чтобы использовать их в качестве дополнительного инструмента. Более того сканнеры являются частью проверки, а не полноценным продуктом автоматизации аудита, в результате которого обязательна должна быть оценка, а не только сводный отчёт о найденных уязвимостях. Оценка аудитора должна вычисляться в соответствии с существующими стандартам, и, несмотря на то, что в трёх представленных ИТ-решениях есть возможность вывода информации о проверке, полученная в ходе работы документация – это описание найденных уязвимостей, что является лишь частью итоговой аудиторской оценки.

Существующие на рынке программные продукты для автоматизации аудита и документооборота ориентированы больше на финансовую сферу, бухгалтерскую деятельность. Самое понятие аудита информационных технологий для России новое, поэтому методики его проведения не формализованы, используются зарубежные практики (COBIT), международные ГОСТы (ISO 19011:2011). По этой же причине отсутствует узкоспециализированное программное обеспечение для аудита информационных технологий, есть комплексные ИТ-решения, но их не так много. Выделить можно такие программные продукты как «IT Audit: Аудитор», («Мастер-Софт»), «ЭкспрессАудит: ПРОФ» (Консалтинговая группа «ТЕРМИКА», AuditXP «Комплекс Аудит» («Гольдберг-Софт»), AuditNET. Все четыре решения применимы в аудите финансово-

хозяйственной деятельности, в системах отражены отраслевые особенности бухучета и налогообложения. Однако существуют и иные инструменты, которые используются при аудиторской проверке. Их используют в комплексе с другими программными продуктами, но и сфера их применения не ограничивается аудиторской деятельностью. Скорее, данные ИТ-решения способствуют решению той или иной задачи, которая стоит перед аудитором, в ходе выполнения проверки.

Таблица 2. Комплексные продукты для проведения аудита

Название продукта	Основная направленность	Сфера применения продукта	Возможности	Особенности
IT Audit: Аудитор	Внешний и внутренний аудит	Финансовый аудит и оценка рисков	Планирование и проведение аудиторских проверок, документирование и оценка средств контроля для выполнения требований Международных стандартов аудита	Риск-ориентированный подход. Интегрирована с 1С:Предприятие 7.7, 8.2, 8.3. Возможно доработать методику проведения аудита под свои нужны (нужен отдельный модуль «Методолог»)

ЭкспрессАудит: ПРОФ	Внешний и внутренний аудит	Проверка финансово-хозяйственной деятельности коммерческого малого или среднего предприятия	Разработка общего плана и программы аудита; создание рабочей документации аудита; изучение и оценка систем бухгалтерского учета и внутреннего контроля проверяемых экономических субъектов; получение аудиторских доказательств о достоверности бухгалтерской отчетности;	Два варианта проведения аудиторской проверки сформированных объектов аудита: по полной и по сокращенной программе (экспресс-аудит)
AuditXP «Комплекс Аудит»	Внешний и внутренний аудит	Автоматизация аудиторской деятельности средних и малых аудиторских организаций и индивидуальных аудиторов	Программа включает в себя методику контроля качества аудиторской проверки, блок аналитических процедур и финансового анализа	В программе есть крупный блок автоматической обработки всех разделов аудита, результаты анализа которого сводятся в специальную форму-таблицу. В ней представлены суммы искажений статей форм № 1 и № 2 бухгалтерской отчетности и величина превышения существенности

AuditNET	Внутренний аудит	Автоматизация деятельности аудиторских и аудиторско-консалтинговых организаций, т.е. для внутреннего аудита	Имеется стандартный набор шаблонов рабочих документов, программ проверок, листов-опросников, анкет, текстов и др., которые при необходимости можно самостоятельно изменять	Система исключительно сетевая и требует обязательной установки сервера с минимальным вариантом поставки на 20 рабочих мест

Теоретически данные системы могут применяться и при аудите информационных технологий, но тем не менее качественную комплексную проверку систем информационной безопасности предприятия с ними выполнить будет трудно из-за переизбытка ненужных инструментов и недостатка в тех, которые действительно требуются для проведения ИТ-аудита.

В современных реалиях необходим продукт для конкретной области – в данном случае информационной безопасности, – с помощью которого возможно было бы автоматизировать аудит информационных технологий. Предпочтительно, чтобы в таком продукте использовались в комплексе как зарубежные практики, так и российские стандарты, и, на базе существующих методологий проведения аудита информационных технологий, был выработан новый подход к оценке эффективности систем информационной безопасности предприятия.

Список литературы

1. За 12 лет утекло более 30 млрд записей персональных данных // [Электронный ресурс]. Режим доступа: https://www.infowatch.ru/analytics/digest/15281/ (дата обращения: 27.03.2019).
2. Число утечек из муниципальных организаций выросло на 30% // [Электронный ресурс]. Режим доступа: https://www.infowatch.ru/analytics/digest/15364/ (дата обращения: 27.03.2019).
3. Число утечек из медицинских учреждений выросло на 16% // [Электронный ресурс]. Режим доступа: https://www.infowatch.ru/analytics/digest/15414/ (дата обращения: 27.03.2019).

4. *Аверченков В.И.* Аудит информационной безопасности: учеб. пособие для вузов / В.И. Аверченков. 3-е изд., стереотип. М.: ФЛИНТА, 2016. 269 с.
5. Проверки соответствия Nessus // [Электронный ресурс]. Режим доступа: http://static.tenable.com/documentation/nessus_compliance_checks_RU.pdf/ (дата обращения: 17.04.2019).