РОСТ КОЛИЧЕСТВА УТЕЧЕК КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ КАК ПРОБЛЕМА СОВРЕМЕННОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Клочкова Т.В. Email: Klochkova1157@scientifictext.ru

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 анализируются данные за период 2015, 2016, и 2017 годов, рассматривается ситуация в сфере информационной безопасности на момент 2018 года, выявляются актуальные проблемы, сравнивается рост количества утечек конфиденциальной информации за последние годы, а также указываются основные каналы, по которым происходят утечки. Аудит систем информационной безопасности представлен как один из способов контроля программных средств защиты, которые используются при построении системы информационной безопасности на предприятии.*
Ключевые слова: *информационные технологии, ИТ-аудит, аудит информационных систем, аудит информационной безопасности, информационная безопасность.*

GROWTH OF LEAKAGE CONFIDENTIAL INFORMATION AS A PROBLEM OF MODERN INFORMATION SECURITY

Klochkova T.V.

Klochkova Tamara Vladimirovna – Undergraduate,
DEPARTMENT OF INFORMATION SYSTEMS AND TELECOMMUNICATIONS, FACULTY OF INFORMATICS AND CONTROL SYSTEMS,
BAUMAN MOSCOW STATE TECHNICAL UNIVERSITY, MOSCOW

Abstract: *the article analyzes data for 2015, 2016, and 2017, reviews the situation in the field of information security at the time of 2018, identifies current problems, compares the growth of leaks of confidential information in recent years and also indicates the main channels through which leaks occur. The audit of information security systems is presented as one of the ways to control software protection tools that are used when building an information security system in an enterprise.*
Keywords: *information technology, IT audit, audit of information systems, audit of information security, information security.*

УДК 001.8

С развитием информационных технологий (ИТ) произошла трансформация различных сфер жизни общества. Современные предприятия используют в своей деятельности передовые технологии, в том числе соответствующие программные средства защиты конфиденциальной информации, однако, несмотря на бурное развитие рынка программного обеспечения в области информационной безопасности, риск утечки конфиденциальных корпоративных сведений существует и, что удивительно, по данным последних исследований, растет. В совокупности прирост количества утечек был незначительным до 2017 года, в который произошёл скачок, показанный на рисунке 1. Под утечками подразумеваются случайные или же намеренные действия внешних и внутренних нарушителей, в результате которых нарушена конфиденциальность данных [1]. По последним данным аналитического центра Infowatch, в 2018 в мире зарегистрировано более 1000 случаев утечки конфиденциальной информации, что на 12% превышает данные 2017 года [1].

Рис. 1. Количество утечек, произошедших в период с 2015 по 2017 годы

Большая часть атак произошла с участием внутреннего нарушителя, поэтому при построении грамотной системы информационной безопасности для минимизации рисков следует обращать внимание не только на внешние угрозы, но и на внутреннюю среду.

Несмотря на наличие программных средств защиты, повсеместно в мире происходят утечки конфиденциальной информации, в том числе информации, содержащей государственную тайну. По данным за 2018 год утечки информации по электронной почте сократились на 4,8%: в 2017 году утечка по данному каналу составляла 13,3%, в 2018 же всего 8,5%, однако электронная почта всё ещё остаётся одним из популярных каналов, по которым утекают данные [2]. Незначительно уменьшились утечки по каналу браузер сети Интернет и облака, но всё ещё остаются в зоне риска. Возрос процент утечек через съёмные носители на 1,9%, то есть при проведении аудита следует проверить, каким образом происходит запись информации на съёмные носители и как программные средства, установленные на предприятии, предотвращают кражу потенциально важной конфиденциальной информации. По данным Смарт Лайн Инк, более 40% отечественных компаний не применяют никакие программные средства защиты для контроля съёмных носителей [6].

Аудит информационных технологий является одним из инструментов, с помощью которого можно повлиять на складывающуюся под влиянием современных тенденций ситуацию в сфере информационной безопасности. Под современными тенденциями понимается, например, переход многих компаний к облачным вычислениям, работа с которыми влечёт за собой определенные последствия. По данным исследования аналитического центра Infowatch за 2018 год, утечки ликвидного типа данных по сетевому каналу, то есть через браузер или облачный сервис, превалируют над другими каналами. Помимо умышленных утечек данных, есть и случайные, которые должны предотвращаться как программными, так и аппаратными средствами защиты. Программным средствам защиты следует уделять повышенное внимание при аудите, потому что они являются популярным, но достаточно уязвимым инструментом информационной безопасности. Программные средства защиты обеспечивают безопасность информации на предприятии и решают такие задачи по обеспечению безопасности информации, как идентификация и аутентификация пользователя, защита данных пользователя, распределение прав доступа пользователя к ресурсам, криптографическая поддержка, аутентификация сторон, которые участвуют в обмене данными. При аудите программного средства защиты следует уделять особое внимание мониторингу активности пользователя в сети.

ИТ аудит может способствовать улучшению ситуации, его основное влияние направлено на выявление недочётов в системе безопасности предприятия. Уверенность в ИС можно получить после того, как все её компоненты изучены и проанализированы. Для борьбы с внешними и внутренними злоумышленниками особенно важно исследовать программные средства защиты корпоративной информации – информационные системы безопасности, используемые предприятием для предотвращения возможных утечек. Беря во внимание международные, а также российские стандарты информационной безопасности, а также учитывая необходимость в узком специализированном вспомогательном продукте, следует рассмотреть возможность создания программного обеспечения, упрощающего и ускоряющего процесс ИТ аудита. Однако учитывая разнообразие информационных систем безопасности, которыми пользуются предприятия, нужно создать универсальный продукт или же такой, который можно изменять под нужды процесса проверки.

Процесс ИТ аудита преследует практически те же цели, что и обычный аудит, но с некоторыми отличиями. Если мы говорим о процессе аудита ИС безопасности, то, диагностируя программные средства защиты, аудитору в конечном итоге необходимо получить свидетельства того, что компоненты информационной системы безопасности поддерживают целостность данных, предоставляют надежные способы хранения информации и предотвращают её утечку посредством соответствующего функционала, обеспечивают безопасность конфиденциальной информации, шифрование, защиту персональных данных, мониторинг, контроль технических каналов утечки информации за пределы корпоративной сети с помощью технологий предотвращения утечек конфиденциальной информации, мониторинг активности пользователя и прочее. В свою очередь, оценив средства программной защиты на предприятии, аудитор способен выявить узкие места до возникновения опасности утечки данных и дать рекомендации для предупреждения потенциального риска потери конфиденциальной информации.

Список литературы / References

1. За 12 лет утекло более 30 млрд записей персональных данных. [Электронный ресурс]. Режим доступа: https://www.infowatch.ru/analytics/digest/15281/ (дата обращения: 21.05.2019).
2. Глобальное исследование утечек конфиденциальной информации в 2017 году // [Электронный ресурс]. Режим доступа: https://www.infowatch.ru/presscenter/news/20726 (дата обращения: 20.05.19).
3. Глобальное исследование утечек конфиденциальной информации в 2018 году // [Электронный ресурс]. Режим доступа: https://www.infowatch.ru/report2018/ (дата обращения: 20.05.19).
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).
6. Исследование: утечки информации через рабочие станции. // [Электронный ресурс]. Режим доступа: https://www.devicelock.com/ru/dl/dl_survey_leakage2008_ru.pdf/ (дата обращения: 20.05.19).