Электронный научный журнал "Математическое моделирование, компьютерный и натурный эксперимент в естественных науках" http://mathmod.esrae.ru/
URL статьи: **mathmod.esrae.ru/41-165**
Ссылка для цитирования этой статьи:
Ковалев А.Д. Обзор исследований моделирования защиты информации от утечки по техническим каналам на объектах информатизации предприятий // Математическое моделирование, компьютерный и натурный эксперимент в естественных науках. 2023. № 1.

УДК 004.056.5 DOI: 10.24412/2541-9269-2023-1-40-44

ОБЗОР ИССЛЕДОВАНИЙ МОДЕЛИРОВАНИЯ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ ПРЕДПРИЯТИЙ

Ковалев А.Д.[1]
[1]Саратовский государственный технический университет имени Гагарина Ю.А., Россия, Саратов, kovalev.ad13@gmail.com

REVIEW OF STUDIES ON MODELING PROTECTION OF INFORMATION AGAINST LEAKAGE THROUGH TECHNICAL CHANNELS AT INFORMATION OBJECTS OF ENTERPRISES

Kovalev A.D.[1]
[1]Yuri Gagarin State Technical University of Saratov, Russia, Saratov, kovalev.ad13@gmail.com

Аннотация. В статье приводится обзор исследований моделирования защиты информации от утечки по техническим каналам на объектах информатизации предприятий. Определены основные направления современных исследований. Показана необходимость продолжения исследований в области оценки рисков возникновения угроз информационной безопасности с точки зрения технических каналов утечки.

Ключевые слова: математическое моделирование, риски информационной безопасности, утечка по техническим каналам, риски возникновения угроз.

Abstract. The article provides an overview of research on modeling the protection of information from leakage through technical channels at the objects of informatization of enterprises. The main directions of modern research are determined. The need to continue research in the field of assessing the risks of information security threats from the point of view of technical leak channels is shown.

Keywords: mathematical modeling, information security risks, leakage through technical channels, risks of threats.

В настоящее время большое количество информации обрабатывается в различного рода информационных системах. Это связано с возросшим

количеством самой информации, методов ее обработки, специфики хранения, видов использования и т.д. Большинство организаций под универсальным способом защиты огромного массива данных, обрабатываемых в автоматизированных системах и обсуждаемых в процессе коммерческой деятельности, подразумевают ограничение доступа к рабочим местам, установке специализированного программного обеспечения (антивирусная защита, средства защиты информации от несанкционированного доступа и т.д.) и звукоизоляции стен зала для проведения совещаний, не понимая или не принимая во внимание такой аспект комплексной защиты информации как защиты информации от утечки по техническим каналам. Добывание информации таким способом никак не отслеживается службой безопасности и отделами по защите информации предприятия, в то время как вредоносное программное обеспечение и несанкционированный доступ в большинстве случаев можно расследовать во время и после инцидента, совершенного злоумышленником. Исходя из вышеуказанного можно сделать вывод о важности и обязательности выполнения комплексного технического контроля и возможного моделирования рисков возникновения технических каналов утечки информации на объектах информатизации предприятий.

Исследованиями в области моделирования управления рисками возникновения угроз информационной безопасности на распределенных объектах управления и объектах информатизации предприятий занимались многие специалисты, в том числе Карпов А.В.[1], Супрун А.Ф.[2], Казарин О.В.[3], Макеев А.С [4], Исаев А.Н.[5], Дорофеев А.В. [6], Рахметов Р.А. [7-8], Бердюгин А.А. [9], Шиляев С.А.[10], Адрианов В.В. [11], Киселева И.А. [12], Козьминых С.И.[13], Жидко Е.А. [14-15], Михайлова А.П.[16].

Анализ работ [1-16] специалистов по информационной безопасности показал, что задача моделирования рисков возникновения угроз информационной безопасности проработана и освещена очень широко, однако, касаемо рисков возникновения ТКУИ на объектах информатизации исследований очень мало, и они не решают проблему оценки рисков возникновения угрозы.

К примеру, в работе [1] приведена модель количественной оценки рисков образования канала утечки информации, что в свою очередь, используется для проектной оценки защищенности при построении типовых вариантов системы защиты информации (СЗИ) либо эксплуатационной оценки безопасности информации при функционировании данного объекта [17]. К достоинствам данного метода можно отнести его простоту и возможность добавления или удаления из логической функции риска утечки информации параметров, необходимых для более качественного решения поставленной задачи.

Проблема комплексного моделирования системы защиты и угроз остро отражена в работе [2]. Описание различных видов моделирования и необходимость мониторинга специалистами в сфере информационной безопасности, безусловно, повышают качество комплекса защиты информации

и создают для руководства предприятия экономическое обоснование для ассигнований в поддержание и развитие уровня безопасности. Касаемо ТКУИ, исследователем приведена математическая модель защиты информации, графическое представление канала утечки информации и построение модели защиты информации по определенным критериям.

О процедуре анализа рисков и ее экономической обоснованности, с построением алгоритма анализа рисков и системы защиты информации при создании радиоэлектронных систем, идет речь в исследовании [3]. Принадлежность к определенной системе дает понятие выполняемых в процессе жизненного цикла этапов и мероприятий комплекса защиты информации от утечки по техническим каналам. Система оценки рисков возникновения угрозы разработана для определенного вида задач и требует универсальности и точности в подходе.

Оценка рисков также рассматривается в исследовании [4]. Вводятся такие понятия как шкала оценки активов и шкала ценности, что помогает наглядно проследить связь между возможным риском и его последствиями для предприятия. Опять же универсальность данного метода оценки рисков применимо и разрабатывается для каждого конкретного случая, каждой конкретной угрозы, каждого конкретного объекта защиты.

Не смотря на большое количество исследований, проведенных специалистами в области информационной безопасности, в их работах слабо раскрыта тема моделирования рисков возникновения угроз информационной безопасности с точки зрения технических каналов утечки.

Литература

1. Карпов А.В., Лепешкин О.М. «Моделирование технических каналов утечки информации на распределенных объектах управления» // Международный журнал перспективных исследований, Т. 8, №1, 2018, С. 69-83 DOI: 10.12731/2227-930X-2018-1-69-83
2. Супрун А.Ф. Комплексное обеспечение информационной безопасности. Моделирование процессов реализации угроз. Часть 1. СПб: Изд-во СПбГПУ, 2012, 50 с.
3. Казарин О. В., Репин М. М. Особенности анализа рисков утечки конфиденциальной информации по техническим каналам при создании радиоэлектронных средств // Вопросы кибербезопасности. 2015. №4 (12). URL: https://cyberleninka.ru/article/n/osobennosti-analiza-riskov-utechki-konfidentsialnoy-informatsii-po-tehnicheskim-kanalam-pri-sozdanii-radioelektronnyh-sredstv.
4. Макеев А. С. Основные аспекты управления рисками информационной безопасности // Молодой ученый. — 2016. — № 8 (112). — С. 126-134. — URL: https://moluch.ru/archive/112/28532/

5. Исаев А.Н. Противодействие утечке информации по техническим каналам // Молодой ученый. — 2021. — № 2 (344). — С. 17-19. — URL: https://moluch.ru/archive/344/77362/
6. Дорофеев А.В. Менеджмент информационной безопасности: управление рисками // Вопросы кибербезопасности. 2014. №2 (3). URL: https://cyberleninka.ru/article/n/menedzhment-informatsionnoy-bezopasnosti-upravlenie-riskami.
7. Рахметов Р. Анализ международных документов по управлению рисками информационной безопасности. Часть 1. https://habr.com/ru/articles/495236/
8. Рахметов Р. Анализ международных документов по управлению рисками информационной безопасности. Часть 2 https://habr.com/ru/articles/495986/
9. Бердюгин А.А. Управление риском нарушения информационной безопасности в условиях электронного банкинга // Вопросы кибербезопасности. 2018. №1 (25). URL: https://cyberleninka.ru/article/n/upravlenie-riskom-narusheniya-informatsionnoy-bezopasnosti-v-usloviyah-elektronnogo-bankinga
10. Шиляев С. Методика оценки рисков информационной безопасности /// https://kontur.ru/articles/1691
11. Адрианов В.В. Обеспечение информационной безопасности бизнеса // М.: ООО «Центр исследований платежных систем и расчетов», «Альпина», 2011, 450 с.
12. Киселева И.А., Искаджян С.О. Информационные риски: методы оценки и анализа // ИТпортал. 2017. №2 (14). URL: https://cyberleninka.ru/article/n/informatsionnye-riski-metody-otsenki-i-analiza
13. Козьминых С.И. Математическое моделирование обеспечения комплексной безопасности объектов информатизации кредитно-финансовой сферы // Вопросы кибербезопасности. 2018. №1 (25). URL: https://cyberleninka.ru/article/n/matematicheskoe-modelirovanie-obespecheniya-kompleksnoy-bezopasnosti-obektov-informatizatsii-kreditno-finansovoy-sfery
14. Жидко Е.А. Методология системного математического моделирования информационной безопасности // Вестник евразийской науки. 2014. №3 (22). URL: https://cyberleninka.ru/article/n/metodologiya-sistemnogo-matematicheskogo-modelirovaniya-informatsionnoy-bezopasnosti.
15. Жидко Е.А. Попова Л.Г. Принципы системного математического моделирования информационной безопасности // Интернет-журнал "Науковедение". 2014. №2 (21). URL: https://znanium.com/catalog/product/487844
16. Михайлов А. П., Маревцева Н. А. Модели информационной борьбы // Матем. моделирование, 23:10 (2011), С. 19–32

17. Корсунский А.С., Масленникова Т.Н., Лепешкин О.В., Чукариков А.Г., Карпов А.В. Направления развития подсистемы контроля состояния защиты информации объекта // Актуальные проблемы и перспективы развития радиотехнических и инфокоммуникационных систем. Сборник научных трудов III Международной научно-практической конференции. Том Часть 1. Московский технологический университет (МИРЭА). 2017, С. 187-192