Тип работы: Магистерская работа

Предмет: Информационные системы и процессы

В настоящее время деятельность компаний различного рода деятельности связана с использованием информационных систем. Информация на современном этапе является неотъемлемой составляющей функционала сотрудников, что приводит к зависимости возможностей исполнения служебных функций от качества функционирования объектов ИТ-инфраструктуры. В настоящее время создано большое количество информационных систем, нарушение функционирования которых может приводить к значительным негативным последствиям вплоть до остановки деятельности учреждений, невозможности проведения платежей, невозможности штатного функционирования объектов транспортной и коммуникационной инфраструктуры. Таким образом, объекты автоматизации, от которых зависит жизнедеятельность государства, отнесены к особой категории, регламенты защиты информации в которой определяются отдельными нормативными актами.
Цель этой работы заключается в разработке методов и алгоритмов по обеспечению защиты информации в условиях Совкомбанка
Для достижения поставленной цели необходимо решить следующие задачи:
 анализ основных подходов к обеспечению информационной безопасности в условиях работы с объектами критической информационной инфраструктуры Банка;
 изучение нормативных актов, регламентирующих мероприятия по защите объектов критический информационной инфраструктуры, принципов отнесения объектов к категории указанного класса;
 анализ деятельности исследуемой компании, определение перечня защищаемых информационных ресурсов;
 построение модели угроз;
 выбор механизмов защиты, посредством которых обеспечивается возможность обеспечения защиты объектов критической информационной инфраструктуры;
 анализ правового обеспечения систем защиты информации объектов критической информационной инфраструктуры;
- оценка ожидаемого уровня снижения рисков информационной безопасности посредством риск-ориентированного подхода.
Объект исследования – объекты информационной инфраструктуры Банка.
Предмет исследования: методы и алгоритмы обеспечения безопасности объектов критической информационной инфраструктуры Банка.
Вопросы обеспечения безопасности объекта критической информационной инфраструктуры рассматривались в работах ряда авторов, в частности Клименко И. С., Бондарева В. В., Солодянникова А. В. Методическую основу выпускной квалификационной работы составили работы Язова Ю. К., Соловьева С. В., Маркова А. С., Королева Е. Н.

Теоретическую основу выпускной квалификационной работы Зенкова А. В., Васильевой И. Н., Казарина О. В. Работа состоит из трех глав, введения, заключения, списка использованных источников.

1. Аналитическая часть

1.1. Обзор нормативно-правовых актов в области обеспечения защиты информации в банковской сфере

Специфика деятельности компаний, работающих в финансовом секторе, предполагает необходимость защиты проведения финансовых транзакций в части соблюдения требований к конфиденциальности, защиты каналов передачи данных, по которым осуществляется работа с платежными сервисами, предотвращение инцидентов, в рамках которых возможно предоставление доступа к платежным счетам клиентов со стороны злоумышленников.

Проводя классификацию информационных рисков, выделяют следующие критерии: по источникам (внутренние и внешние), по характеру (преднамеренные и непреднамеренные), по виду (прямые или косвенные), по виду нарушения (информационные, физические, организационно-правовые), по механизму воздействия (стихийного бедствия, техногенные, политические, социальные, развитие информационно-коммуникационных технологий).

Классификация рисков в области информационной безопасности имеет важное значение для правильной оценки информационных рисков, охватывающих все возможные инциденты, угрозы информационной безопасности, которые могут привести к нарушению свойств информации. Инцидент информационной безопасности — событие или группа событий, вследствие которых вероятна реализация угроз, связанных с нарушением защищенности системы информационной безопасности на предприятиях.

Рекомендации по предотвращению инцидентов информационной безопасности и методология реагирования на них определены в стандартах. В документе [1] подробно описаны стадии планирования, эксплуатации, анализа и улучшения системы управления инцидентами безопасности. В документе [2] определена необходимость выполнения организациями банковской системы Российской Федерации деятельности по выявлению инцидентов ИБ и реагированию на инциденты ИБ.

Методические рекомендации ГосСОПКА разработаны для органов государственной власти, принявших решение о создании ведомственных центров ГосСОПКА, государственных корпораций, операторов связи и других организаций, осуществляющих лицензируемую деятельность в области защиты информации и принявших решение о создании корпоративных центров ГосСОПКА.

Рекомендации разработаны Центром защиты информации и специальной связи Федеральной службы безопасности Российской Федерации в соответствии с основными положениями документов [3-5]

Цели расследования инцидентов информационной безопасности включают:

- проведение мероприятий, связанных с устранением последствий возникновения инцидентов информационной безопасности;
- определение специалистов, деятельность которых привела к возникновению инцидентов информационной безопасности;
- проведение анализа причин возникновения инцидентов и принятие мер к недопущению их повторения.

Единая методика проведения расследований инцидентов информационной безопасности в настоящее время не разработана, расследование инцидентов включает этапы:

- сбор данных об обстоятельностях возникновения инцидентов;
- анализ действий пользователей, которые привели к возникновению инцидентов;
- выявление возможных причин, которые сделали возможным возникновение инцидента;
- принятие управленческих решений по итогам расследования инцидента;
- документирование данных по возникновению и расследованию инцидента.

При проведении сбора информации об инцидентах необходимо провести оценку достоверности полученной информации, возможности отнесения полученной информации к причинам возникновения инцидента, оценку полноты полученной информации об инциденте.

При использовании протоколов работы программного обеспечения в процессе возникновения инцидентов необходимо учитывать последовательность действий, состояние работы системы до, во время и после возникновения инцидента.

При анализе действий сотрудников необходимо учитывать наличие умысла на возникновение инцидента, либо пренебрежение требованиями защиты информации вследствие халатности. Также проводится анализ полноты принятых мер технического характера по недопущению возникновения инцидента.

Объекты критической информационной инфраструктуры (КИИ) – это информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, а также коммуникационные системы, используемые для организации их взаимодействия.

Обеспечение защиты информации на объектах КИИ регламентируется специализированными законодательными актами, основным из которых является Федеральный закон РФ №187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации».
Требования указанного закона включают [3]:
- определение порядка отнесения объектов обработки данных к категории КИИ;
- определяет порядок использования законодательства, регламентирующего использование объектов КИИ;
- определяет уровень полномочий органов власти при работе с объектами КИИ;
- определяет порядок оценивания защищённости объектов КИИ.

В соответствии с требованиями Федерального закона РФ №187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации» определены критерии значимости объектов КИИ, включающие [14]:
- социальный уровень, предполагающий обеспечение защиты информационных систем, в которых осуществляется обработка информации, нарушение функциональности которой может приводить к негативным последствиям в жизни общества и невозможности исполнения социальных обязательств (к данной категории относятся информационные базы ПФР, органов социальной защиты, банков, структуры ЖКХ, сервисов предоставления государственных услуг и др.);
- политический уровень, включающий необходимость обеспечения защиты от угроз функционирования систем, обеспечивающих поддержку деятельности органов власти и силовых структур;
- экономический уровень, включающий необходимость обеспечения защиты от угроз функционирования систем, обеспечивающих возможности денежного оборота, проведения расчётов внутри и за пределами страны;
- экологический уровень, необходимость обеспечения защиты от угроз функционирования систем, обеспечивающих поддержку экологических систем;
- уровень безопасности, в рамках которого осуществляются мероприятия по защите объектов, используемых в целях обеспечения обороноспособности.

Порядок категорирования объектов КИИ и определение мероприятий по защите информации в них регламентируются Постановлением Правительства РФ № 127 от 08.02.2018.
Отнесение объекта к той или иной категории объектов КИИ проводится на основании критериев, включающих [3]:
- оценка объемов вероятного ущерба при возникновении инцидентов на объектах КИИ;
- оценка объемов вреда объектам инфраструктуры при возникновении инцидентов на объектах КИИ;
- объемы нарушения доступности транспорта и связи при возникновении инцидентов на объектах КИИ;
- невозможность исполнения своих функций учреждениями при возникновении инцидентов на объектах КИИ;
- уровень сокращения поступлений в бюджеты при возникновении инцидентов на объектах КИИ;
- вероятность возникновения экологической катастрофы при возникновении инцидентов на объектах КИИ;
- сокращение производительности производства на предприятиях при возникновении инцидентов на объектах КИИ.

Нормативная база в области защиты персональных данных включает:
- 152- ФЗ «О Персональных данных» от 27.07.2006;
- 149 – ФЗ «Об информации, информационных технологиях и защите информации» от 27.07.2006;
- Статьи Трудового кодекса, кодекса об административных правонарушениях;
- Локальные нормативные акты.

Нормативной базой технологии систем информационной безопасности являются: федеральное законодательство, нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации, а также руководящие документы Федеральной службы по техническому и экспортному контролю (ФСТЭК России) и ФСБ России, регулирующие вопросы безопасности информации.
В соответствии с нормативными документами в области защиты информации, каждое предприятие и организация, в которой производится обработка персональных данных, обязано принять ряд организационных и технологических мер по обеспечению защиты информации.
Приведем основные положения законодательных актов в области информационной безопасности.
Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным
Согласно Федеральному закону от 27 июля 2006г. № 152-ФЗ, оператор в рамках обработки персональных

данных должен обеспечивать комплекс необходимых правовых, организационных и технических мер по обеспечению конфиденциальности персональных данных, что достигается путем определения угроз безопасности, оценки эффективности мероприятий по обеспечению безопасности, контроля за принимаемыми мерами по защите информации [8].
Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
Постановление № 1119 содержит довольно подробную классификацию информационных систем персональных данных, угроз безопасности таких систем (п. 6), уровней защищенности информационных систем от указанных угроз
Приказ ФСТЭК России № 21 от 18.02.2013 определяет принципы классификации систем персональных данных. Согласно приказу ФСБ от 10.07.2014 № 378 определены четыре уровня защищенности персональных данных.
Каждый из присвоенных уровней защищенности предполагает применение соответствующих мер по обеспечению информационной безопасности.
В зависимости от соотношения типа информационной системы и характерных для нее угроз выделены четыре уровня защищенности персональных данных, необходимых для конкретной информационной системы.
Специфика организации защиты информации в банковской сфере регламентируется стандартами Банка России (Стандарт Банка России СТО БР ИББС-1.0-2014 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации/ Общие положения"). Стандарт регламентирует порядок обеспечения защиты информации при проведении платежных операций в дистанционном режиме, регламентирует требования к работе пользователей в банковских информационных системах, организацию внутриобъектового режима, архитектуру программной защиты информации.
1.2. Анализ структуры обрабатываемой информации в ПАО «Совкомбанк»
В рамках данной работы проведён анализ специфики обеспечения защиты информации в условиях Совкомбанка.
Типовая организационная структура филиалов группы Совкомбанка включает выделение отделов по видам операций: кредитных; расчетных; кассовых; вексельных; фондовых (с ценными бумагами); межбанковских; с иностранной валютой; комиссионных (посреднических) и др.
В настоящее время наблюдается рост оборотов по банковским операциям, внедряются новые технологии, расширяется клиентская база, в связи, с чем возникает вопрос оптимизации технологии работы банка путем внедрения автоматизированной системы удалённого взаимодействия с клиентами.

1. База данных угроз ФСТЭК. [Электронный ресурс]. Режим доступа: https://bdu.fstec.ru/threat (дата доступа: 07.11.2022)
2. Клименко И. С. Информационная безопасность и защита информации: модели и методы управления: монография / И. С. Клименко. - Москва: ИНФРА-М, 2020. – 178с.
3. Бондарев, В. В. Введение в информационную безопасность автоматизированных систем : учебное пособие / В.В. Бондарев. - Москва: Изд-во МГТУ им. Н.Э. Баумана, 2018. - 250 с.
4. Солодянников А. В. Комплексная система защиты объектов информатизации: учебное пособие / А. В. Солодянников. - Санкт-Петербург: Изд-во Санкт-Петербургского государственного экономического университета, 2017. - 91 с.
5. Примакин А. И., Саратов Д. Н., Синещук Ю. И. Техническая защита информации : учебное пособие /Примакин А. И., Саратов Д. Н., Синещук Ю. И. - Санкт-Петербург: Санкт-Петербургский университет МВД России, 2021. - 154 с.
6. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И. С. Клименко. - Москва: ИНФРА-М, 2020. – 178 с.
7. Воеводин В. А., Душкин А. В., Петухов А. Н., Хорев А. А. Программно-аппаратные средства защиты информации: учебное пособие / В. А. Воеводин, А. В. Душкин, А. Н. Петухов, А. А. Хорев. - Москва: МИЭТ, 2021. - 280 с.
8. Чекулаева Е. Н., Кубашева Е. С. Управление информационной безопасностью : учебное пособие / Е. Н. Чекулаева, Е. С. Кубашева. - Йошкар-Ола: Поволжский государственный технологический университет, 2020. - 153 с.
9. Алексеев А. П. Многоуровневая защита информации: монография / А. П. Алексеев. - Самара : ПГУТИ, 2017.

- 128 с.
10. Благодаров, А. В. Алгоритмы категорирования персональных данных для систем автоматизированного проектирования баз данных информационных систем / А. В. Благодаров, В.С. Зияутдинов, П.А. Корнев, В.Н. Малыш. - Москва: Горячая линия-Телеком, 2015. - 115 с.
11. Бондарев, В. В. Анализ защищенности и мониторинг компьютерных сетей: методы и средства: учебное пособие / В.В. Бондарев. - Москва: Изд-во МГТУ им. Н.Э. Баумана, 2017. – 225с.
12. Язов Ю. К., Соловьев С. В. Организация защиты информации в информационных системах от несанкционированного доступа : [монография] / Ю. К. Язов, С. В. Соловьев. - Воронеж: Кварта, 2018. - 588 с.
13. Марков А. С. Техническая защита информации: курс лекций: учебное пособие / Марков А.С. - Москва : Изд-во АИСНТ, 2020. – 233с.
14. Королев, Е. Н. Администрирование операционных систем: учебное пособие / Е. Н. Королев. - Воронеж: Воронежский государственный технический университет, 2017. - 85 с.
15. Михайлова, Е. М. Организационная защита информации [Электронный ресурс]/ Михайлова Е. М., Анурьева М. С. - Тамбов: ФГБОУ ВО "Тамбовский государственный университет имени Г. Р. Державина", 2017. – 342 с.
16. Камалова Г. Г. Юридическая ответственность за нарушение конфиденциальности информации: монография / Камалова Гульфия Гафиятовна. - Саратов : Амирит, 2019. - 160 с.
17. Никифоров, С. Н. Защита информации: защита от внешних вторжений : учебное пособие / С.Н. Никифоров. - Санкт-Петербург: Санкт-Петербургский государственный архитектурно-строительный университет, 2017. - 82 с
18. Белов, Е. Б. Организационно-правовое обеспечение информационной безопасности: учебник / Е.Б. Белов, В.Н. Пржегорлинский. - 2-е изд., испр. и доп. - Москва: Академия, 2020. – 332с.
19. Ревнивых, А. В. Информационная безопасность в организациях: учебное пособие / А. В. Ревнивых. - Новосибирск: НГУЭУ, 2018. - 83 с.
20. Щеглов А. Ю. Защита информации: основы теории: учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва: Издательство Юрайт, 2022. — 309 с.
21. Зенков А. В. Информационная безопасность и защита информации: учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с.
22. Бузов Г. А. Защита информации ограниченного доступа от утечки по техническим каналам / Г. А. Бузов. - Москва: Горячая линия - Телеком, 2022. - 585 с.
23. Васильева И. Н. Криптографические методы защиты информации: учебник и практикум для вузов / И. Н. Васильева. — Москва: Издательство Юрайт, 2022. — 349 с.
24. Мазин А. В. Техническая защита информации в информационных системах: учебное пособие / Мазин А. В. - Калуга : Манускрипт, 2019. - 109 с.
25. Казарин О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2022. — 312 с.
26. Хорев П. Б. Программно-аппаратная защита информации : учебное пособие : для студентов высших учебных заведений, / П.Б. Хорев. - 3-е изд., испр. и доп. - Москва : ИНФРА-М, 2020. – 325 с.
27. Еськин Д. Л., Бакулин В. М. Основы защиты информации в компьютерных системах и сетях: учебное пособие / Д. Л. Еськин, В. М. Бакулин. - Волгоград : ВА МВД России, 2019. - 67 с.
28. Гостищева Т. В., Ломазов В. А., Малий Ю. В. Модели и методы проектирования систем защиты информации : монография / Т. В. Гостищева, В. А. Ломазов, Ю. В. Малий. - Белгород: Изд-во Белгородского университета кооперации, экономики и права, 2021. - 175 с.
29. Бабиева Н. А. Информационная безопасность и защита информации: учебное пособие / Н. А. Бабиева. - Казань: Медицина, 2018. – 127с.
30. Тельный А. В., Монахов Ю. М. Техническая защита информации [Электронный ресурс]. Защита информации от утечки по техническим каналам / А.В. Тельный, Ю.М. Монахов. - Владимир : ВлГУ, 2019. – 212с.