Тип работы: Дипломная работа

Предмет: Информационные системе в Бухучёте

Обеспечение информационной безопасности – это, в первую очередь, вопрос эффективности затраченных средств, поэтому расходы на защиту не должны превышать суммы возможного ущерба.
Поскольку любые расходы на предотвращение рисков должны быть обоснованы, необходимо обязательно рассчитывать их экономическую эффективность. Расчетом эффективности и обоснованием расходов на заседании бюджетного комитета занимается менеджер направления, которое заинтересовано в снижении риска.
Для обеспечения необходимой защиты от IT-рисков и контроля безопасности можно провести следующие мероприятия:
• определить круг лиц, отвечающих за информационную безопасность, создать нормативные документы, в которых будут описаны действия персонала компании, направленные на предотвращение IT-рисков, а также обеспечить резервные мощности для работы в критической ситуации;
• разработать единые стандарты информационных систем в рамках организации, то есть перейти к единым отчетным формам, а также единым правилам расчета показателей, которые будут применяться во всех программных продуктах компании, используемых для этой цели;
• классифицировать данные по степени конфиденциальности и разграничить права доступа к ним;

• следить за тем, чтобы любые документы, обращающиеся внутри организации, создавались с помощью систем, централизованно установленных на компьютерах. Установка любых других программ должна быть санкционирована, иначе риск сбоев и вирусных атак резко возрастет;
• внедрить средства контроля, позволяющие отслеживать состояние всех корпоративных систем: в случае несанкционированного доступа система должна или автоматически запрещать вход, или сигнализировать об опасности, чтобы персонал мог принять меры.

Помимо перечисленных мер, необходимо подготовиться к последствиям возможных кризисных ситуаций и описать действия компании по выходу из кризиса. Для этого следует:
• проанализировать сценарии проникновения посторонних лиц или не имеющих соответствующих полномочий сотрудников компании во внутреннюю информационную сеть, а также провести учебные мероприятия с целью отработки модели поведения сотрудников, ответственных за информационную безопасность, в кризисных ситуациях;
• разработать варианты решения проблем, связанных с кадрами, включая уход из компании ключевых сотрудников; например, составить и ознакомить персонал с планом преемственности управления на предприятии;
• подготовить запасные информационные мощности (серверы, компьютеры), а также резервные линии связи.

Так как ПАО КБ «РусьБанк» зависит от состояния ее информационных сетей, необходимо назначить ответственного за разработку, внедрение и контроль исполнения корпоративных правил, направленных на снижение IT-рисков. Желательно, чтобы такой координатор не имел отношения к IT-структуре компании (например, исполнительный директор).

Считается, что сотрудник, который не связан напрямую с информационными технологиями, будет наиболее объективен при организации мероприятий по риск-менеджменту. Его работа должна оцениваться с помощью измеряемых показателей, скажем, время устранения сбоев в работе сервера не должно превышать 30 минут или же частота таких сбоев должна быть не выше, чем два раза в год.

Обязательным условием успешного риск-менеджмента в области информационных технологий является его непрерывность. Поэтому оценка IT-рисков, а также разработка и обновление планов по их минимизации должны производиться с определенной периодичностью, например раз в квартал. Периодический аудит системы работы с информацией (информационный аудит), проводимый независимыми экспертами, будет дополнительно способствовать минимизации рисков.

Разработка и реализация политики по минимизации IT-рисков не принесет пользы, если рекомендуемые стандарты и правила неверно используются. Например, если сотрудники не обучены их применению и не понимают их важности. Поэтому работа по обеспечению IT-безопасности должна быть комплексной и продуманной.

1. Бабаш, А. В. Информационная безопасность / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2018. - 136 с.
2. Банковские информационные системы и технологии. Часть 1. Технология банковского учета. - М.: Финансы и статистика, 2019. - 384 с.
3. Беленькая, М. Н. Администрирование в информационных системах / М.Н. Беленькая, С.Т. Малиновский, Н.В. Яковенко. - М.: Горячая линия - Телеком, 2017. - 400 с.
4. Бионические информационные системы и их практические применения / Коллектив авторов. - Москва: ИЛ, 2019. - 796 с.
5. Васильков, А. В. Безопасность и управление доступом в информационных системах / А.В. Васильков, И.А. Васильков. - М.: Форум, 2020. - 368 с.
6. Гафнер, В. В. Информационная безопасность / В.В. Гафнер. - М.: Феникс, 2020. - 336 с.
7. Девянин, П.Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах / П.Н. Девянин. - М.: Радио и связь, 2006. - 176 с.
8. Ивлев, В. А. ABIS. Информационные системы на основе действий / В.А. Ивлев, Т.В. Попова. - М.: 1С-Паблишинг, 2020. - 248 с.
9. Избачков, Ю. Информационные системы / Ю. Избачков, В. Петров. - Москва: СИНТЕГ, 2016. - 656 с.
10. Информационные системы - миф и действительность. - М.: Знание, 2021. - 433 с.
11. Информационные системы в экономике. - М.: ИНФРА-М, 2019. - 240 с.
12. Информационные системы в экономике. - М.: Юнити-Дана, 2018. - 464 с.
13. Исаев, Г. Н. Информационные системы в экономике / Г.Н. Исаев. - М.: Омега-Л, 2020. - 464 с.

14. Информационная безопасность открытых систем. В 2 томах. Том 1. Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников и др. - М.: Горячая линия - Телеком, 2016. - 536 с.
15. Красникова Т, Невежин В. МОДЕЛИРОВАНИЕ ОЦЕНКИ ПРИ АУДИТЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ, Финансовый университет при Правительстве Российской Федерации, 2017
16. Криницкий, Н.А. Автоматизированные информационные системы / Н.А. Криницкий, Г.А. Миронов, Г.Д. Фролов. - М.: Наука, 2018. - 382 с.
17. Максименко В.Н. ОСНОВНЫЕ ПОДХОДЫ К АНАЛИЗУ И ОЦЕНКЕ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, «ЭКОНОМИКА И КАЧЕСТВО СИСТЕМ СВЯЗИ» 2/2017
18. Мельников, В. П. Информационная безопасность / В.П. Мельников, С.А. Клейменов, А.М. Петраков. - М.: Academia, 2019 - 336 с.
19. Мельников, В. П. Информационная безопасность / В.П. Мельников, С.А. Клейменов, А.М. Петраков. - М.: Академия, 2018. - 336 с.
20. Мельников, В. П. Информационная безопасность и защита информации / В.П. Мельников, С.А. Клейменов, А.М. Петраков. - М.: Academia, 2011. - 336 с.
21. Любарский, Ю.Я. Интеллектуальные информационные системы / Ю.Я.
22. Лобанова Д.Г. «МОДЕЛЬ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРЕДИТНО-ФИНАНСОВЫХ ОРГАНИЗАЦИЙ», ФГОБУ ВПО «Финансовый университет при Правительстве РФ»
23. Любарский. - М.: Наука, 2017. - 228 с.
24. Любарский, Ю.Я. Интеллектуальные информационные системы / Ю.Я. Любарский. - М.: Наука, 2016. - 232 с.
25. Маглинец, Ю.А. Анализ требований к автоматизированным информационным системам / Ю.А. Маглинец. - М.: Бином. Лаборатория знаний, 2014. - 384 с.
26. Мезенцев, К. Н. Автоматизированные информационные системы / К.Н. Мезенцев. - М.: Академия, 2016. - 176 с.
27. Мезенцев, К. Н. Автоматизированные информационные системы / К.Н. Мезенцев. - Москва: Мир, 2019. - 176 с.
28. Моримото, Т. Большая банковская война: (Система финансирования в Японии трещит по швам) / Т. Моримото. - М.: Мысль, 2017. - 270 с.
29. Персианов, Вячеслав Венедиктович; Логвинова Екатерина Ивановна Информационные Системы (Специальность Доу).Учебно-Методическое Пособие / Ивановна Персианов Вячеслав Венедиктович; Логвинова Екатерина. - Москва: Машиностроение, 2017. - 197 с.
30. Партыка, Т. Л. Информационная безопасность / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2018. - 432 с.
31. Петров, Сергей Викторович; Кисляков Павел Александрович Информационная Безопасность / Александрович Петров Сергей Викторович; Кисляков Павел. - Москва: Огни, 2019. - 329 с.
32. Путькина, Л. В. Интеллектуальные информационные системы / Л.В. Путькина, Т.Г. Пискунова. - М.: СПбГУП, 2020. - 228 с.
33. Рассел, Джесси Honeypot (информационная безопасность) / Джесси Рассел. - М.: Книга по Требованию, 2019. - 106 с.
34. Редько, В.Н. Базы данных и информационные системы / В.Н. Редько, И.А. Басараб. - М.: Знание, 2016. - 192 с.
35. Рогожин, М. Ю. Делопроизводство и документооборот в бухгалтерии / М.Ю. Рогожин. - М.: ГроссМедиа, РОСБУХ, 2019. - 248 с.
36. Чипига, А. Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. - М.: Гелиос АРВ, 2019. - 336 с.
37. Шаньгин, В. Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. - М.: ДМК Пресс, 2018. - 702 с.
38. Ярочкин, В.И. Информационная безопасность / В.И. Ярочкин. - М.: Академический проект, 2018. - 544 с.
39. Хубаев, Георгий Николаевич Информатика. Информационные системы. Информационные технологии. Тестирование. Подготовка к интернет-экзамену / Хубаев Георгий Николаевич. - М.: Феникс, 2011. - 831 с.
40. Цапенко, М.П. Измерительные информационные системы / М.П. Цапенко. - М.: Энергоатомиздат, 2016. - 440 с.

Интернет-источники

1. Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 05.12.2016 N 646. Режим доступа

https://www.garant.ru/products/ipo/prime/doc/71456224/ Дата обращения: 31.10.2021
2. МЕТОДИКА ОЦЕНКИ СООТВЕТСТВИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ ТРЕБОВАНИЯМ СТО БР ИББС-1.0-2014 Режим доступа: consultantplus://offline/ref=705628071329A062D6AD6168E2A396B9805D37B2E9D020D5AE04553CA2m1b0U Дата обращения: 31.10.2021
3. Основные направления развития финансового рынка Российской Федерации на период 2019-2021 годов Режим доступа https://cbr.ru/analytics/develop/main_direction_2019_2021/ Дата обращения: 31.10.2021
4. ОТЧЕТ ЦЕНТРА МОНИТОРИНГА И РЕАГИРОВАНИЯ НА КОМПЬЮТЕРНЫЕ АТАКИ В КРЕДИТНО-ФИНАНСОВОЙ СФЕРЕ ДЕПАРТАМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКА РОССИИ 1.09.2018 – 31.08.2019 Режим доступа: https://d-russia.ru/wp-content/uploads/2019/10/FINCERT_report_20191010.pdf Дата обращения: 31.10.2021
5. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы, утвержденная Указом Президента Российской Федерации от 09.05.2017 N 203 Режим доступа http://publication.pravo.gov.ru/Document/View/0001201705100002 Дата обращения: 31.10.2021
6. Стратегия экономической безопасности Российской Федерации на период до 2030 года, утвержденная Указом Президента Российской Федерации от 13.05.2017 N 208 Режим доступа http://www.kremlin.ru/acts/bank/41921 Дата обращения: 31.10.2021