ПРОБЛЕМЫ НЕЙТРАЛИЗАЦИИ НЕГАТИВНЫХ ИНФОРМАЦИОННЫХ ВОЗДЕЙСТВИЙ НА БИЗНЕС-ПРОЦЕСС КРЕДИТНОЙ ОРГАНИЗАЦИИ

Макеев С.А.[1]

В статье рассматривается информационная безопасность бизнес–процессов организаций кредитно–финансовой сферы. Качество применяемых информационных технологий определяет среду функционирования современной кредитной организации. Кредитные организации как особые информационные объекты становятся объектами реализации негативного информационного воздействия на протекающие в них бизнес–процессы. Источником негативных информационных воздействий является заинтересованная конфликтная сторона, а формой реализации – целенаправленные компьютерные атаки с использованием специального вредоносного программного обеспечения. Целью данной статьи является определение общих проблем, связанных с нейтрализацией негативных информационных воздействий на бизнес–процессы организаций. Стратегия проведения активного противодействия угрозам бизнес–процессам кредитной организации осуществляется в форме нейтрализации негативных информационных воздействий. Автором проведен анализ предметной области в части практики противодействия угрозам бизнес–процессам кредитной организации. В результате были выделены основные проблемы нейтрализации негативных информационных воздействий на бизнес–процесс кредитной организации, среди которых рассмотрены проблемы превентивной защиты бизнес–процесса, непосредственной нейтрализации источника негативных информационных воздействий на бизнес–процесс, восстановления состояния бизнес–процесса, защиты от осуществления информационно–психологического воздействия на участников бизнес–процесса, развития отечественного информационного права в направлении определения корпоративных норм поведения в информационной сфере. Решение выделенных проблем позволит повысить информационную безопасность организаций различных форм собственности. Полученные результаты следует использовать для разработки новых моделей и алгоритмов противодействия угрозам и нейтрализации негативных информационных воздействий, а также для формирования научно–технических рекомендаций руководителям служб информационной безопасности для совершенствования систем обеспечения информационной безопасности кредитных организаций в интересах бизнес–процессов.

***Ключевые слова**: негативное информационное воздействие, управление безопасностью, противодействие угрозам*

Введение

В настоящее время экономическая безопасность хозяйствующих субъектов существенно зависит от качества применяемых организациями в своей деятельности информационных технологий и, как следствие, данная проблема стала междисциплинарной, в том числе затрагивающей вопросы обеспечения информационной безопасности организаций различных форм собственности и нейтрализации негативных информационных воздействий на бизнес-процессы организаций [1].

Кроме того, проведенный анализ современных угроз бизнесу показывает появление классов новых целевых вредоносных программ и обеспечивающих их преступных структур, отличающихся сложной организацией и серьезным финансированием [2, 3].

Целью данной статьи является определение общих проблем, связанных с нейтрализацией негативных информационных воздействий на бизнес-процессы организаций, решение которых позволить повысить информационную безопасность организаций различных форм собственности.

Бизнес-процесс как объект защиты

Организации различных форм собственности следует рассматривать как особые информационные объекты, как правило, конкурентно взаимодействующие друг с другом в информационной сфере. Применив определение информационной сферы к данным объектам, получаем совокупность следующих элементов:

– информации, т.е. активов организаций;

– информационной инфраструктуры, т.е. ин-

1 Макеев Сергей Александрович, ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, s.makeev@npo-echelon.ru.

фраструктуры организации (технологической, производственной, др.);

– субъектов, осуществляющих сбор, формирование, распространение и использование информации, т.е. организаций различных форм собственности и взаимодействующих с ними субъектов общественной жизни;

– системы регулирования возникающих при этом общественных отношений, т.е. национального законодательства в различных областях деятельности и уполномоченных органов государственной власти, выполняющих надзорные и регулятивные функции.

Целью обеспечения информационной безопасности организации является создание и поддержание условий эффективного управления активами организации с помощью бизнес-процессов. Одной из важнейших задач обеспечения информационной безопасности организации является активное противодействие угрозам информационным объектам (бизнес-процессам) организации [4].

Основным источником угроз информационному объекту в рамках данного исследования будет являться заинтересованная конфликтная сторона, проводящая информационно-технические и информационно-психологические воздействия (атаки) на составляющие информационного объекта, в результате которых владельцам активов организации, возможно, будет нанесен вред.

Положения Стандарта Банка России СТО БР ИББС-1.0-2014 определяют главной целью злоумышленника получение контроля над информационным ресурсом на самом высшем уровне представления кредитной организации – уровне бизнес-процессов организации.

В стратегии противодействия угрозам информационным объектам организации процесс нейтрализации рассматривается как процесс активного противодействия, включающий в себя комплекс взаимоувязанных мер, направленных на выявление и исключение негативного информационного воздействия на бизнес-процесс в целях предупреждения воздействий, восстановление состояния бизнес-процесса (устранение последствий атаки), а также возможное устранение источника негативного информационного воздействия.

Проблемные вопросы нейтрализации

Проблемными вопросами нейтрализации негативных информационных воздействий на бизнес-процесс организации являются следующие:

1. Проблема превентивной защиты бизнес-процесса.

Учитывая специфику конкуренции организаций в различных видах деятельности, в общем случае выявление и нейтрализация факторов, которые в дальнейшем могут к противоречиям и конфронтации между организациями, является сложной задачей и требует от конкурирующих сторон определенных организационных мероприятий, например, заключения долгосрочных договоров о сотрудничестве.

Для оценки состояния бизнес-процесса может применяться SWOT-анализ с условной количественной оценкой полученных результатов. Техническое решение может заключаться в разработке и внедрении систем сбора и корреляции событий информационной безопасности (SIEM-систем), модули которой выполняют функции непрерывного мониторинга информационной обстановки как в рамках внутренней информационной инфраструктуры организации, так и за её пределами [5].

2. Проблема нейтрализации источника негативных информационных воздействий на бизнес-процессы.

Сложность однозначного определения источника воздействий складывается из специфики информационной сферы и применяемых в ней технологий. Полностью совершить такое действие достаточно сложно, так как источников воздействий может быть много, источник может входить в состав бизнес-процесса, и полностью убрать связи (изолировать) с источниками не всегда представляется возможными [6].

3. Проблема восстановления состояния бизнес-процесса.

Источник угрозы, проводя негативное информационное воздействие на бизнес-процесс, прежде всего, добивается нарушения управления данным бизнес-процессом путем либо его деструкции, либо дисфункции или истощения ресурсов организации на проведение бизнес-процесса. Внедряемые меры и регламенты в рамках системы защиты организации должны фиксировать исходное состояние каждого бизнес-процесса и располагать возможностями по оперативному восстановлению его показателей [7, 8, 11].

4. Проблема возможного осуществления информационно-психологического воздействия на участников бизнес-процесса.

Эффективная защита от информационно-психологического воздействия, например, методов социальной инженерии, в отношении лиц, принимающих решения (ЛПР), по вопросам функционирования бизнес-процессов складывается по-

средством проведения обучающих мероприятий и специальной подготовки ЛПР для работы в нештатных условиях [9].

5. Проблема недостаточного развития нормативно-правовой базы, регулирующей взаимодействия хозяйствующих субъектов в информационной сфере.

Несмотря на развитие отечественного информационного права, стоит отметить, что единого свода правил (кодекса), определяющего общую этику поведения кредитных организаций, не существует. Основой таких правил может служить, например, общая корпоративная цель у организаций в различных отраслях, запрет на манипуляцию с бизнес-целями организаций-конкурентов [10].

Выводы

В результате проведенного анализа практики активного противодействия угрозам бизнес-процессам кредитной организации выделены основные проблемы нейтрализации негативных информационных воздействий на бизнес-процессы организации, а также возможные пути их решения.

Для дальнейшего рассмотрения вопросов нейтрализации негативных информационных воздействий на бизнес-процесс необходимо определиться с содержанием критериев предупреждения, нейтрализации последствий, нейтрализации источника негативных информационных воздействий.

Перспективные исследования направлены на уточнение классификации угроз бизнес-процессам с учетом специфики их функционирования в информационной сфере, а также на разработку моделей и алгоритмов нейтрализации негативных информационных воздействий на бизнес-процессы кредитной организации и формирование научно-технических рекомендаций руководителям служб информационной безопасности по нейтрализации негативных информационных воздействий и совершенствования систем обеспечения информационной безопасности кредитной организаций в интересах бизнес-процессов кредитных организаций [4].

Научный руководитель: кандидат технических наук, профессор Малюк Анатолий Александрович, aamalyuk@yandex.ru

Литература:

1. Андрианов В.В., Зефиров С.Л., Голованов В.Б., Голдуев Н.А. Обеспечение информационной безопасности бизнеса. – М.: ЦИПСиР, 2011. 373 с.
2. Марков А.С., Фадин А.А. Организационно-технические проблемы защиты от целевых вредоносных программ типа Stuxnet // Вопросы кибербезопасности. 2013. № 1(1). С. 28-36.
3. Казарин О.В., Сальников А.А., Шаряпов Р.А., Ященко В.В. Новые акторы и безопасность в киберпространстве // Вестник Московского университета. Серия 12. Политические науки. 2010. № 2. С. 71-84.
4. Казарин О.В., Сальников А.А., Шаряпов Р.А., Ященко В.В. Новые акторы и безопасность в киберпространстве (окончание) // Вестник Московского университета. Серия 12. Политические науки. 2010. № 3. С. 90-103.
5. Макеев С.А. Информационная безопасность бизнес-процессов кредитной организации в условиях проведения информационных операций // Труды международного симпозиума Надежность и качество. 2015. Т. 2. С. 244-246.
6. Ефимов Е.Н., Лапицкая Г.М. Информационная безопасность и бизнес-процессы компании // Известия ЮФУ. Технические науки. 2013. № 12 (149). С. 253-260.
7. Скрыль С.В., Белокуров С.В., Бороненков А.И., Краснов П.Е. Способ выявления негативных воздействий на информационные системы защиты информации // Информация и безопасность. 2012. Т. 15. № 3. С. 377-382.
8. Ивлев К.Г., Затевалов А.С. Применение вероятностных моделей для уточнения процесса восстановления и оценки качества моделей бизнес-процессов в условиях ограниченного размера журнала событий // International Journal of Open Information Technologies. 2014. Т. 2. № 1. С. 32-41.
9. Дорофеев А.В., Марков А.С. Планирование обеспечения непрерывности бизнеса и восстановления // Вопросы кибербезопасности. 2015. № 3 (11). С. 68-73.
10. Кабанов А.С., Лось А.Б., Суроев А.В. Методы социальной инженерии в сфере информационной безопасности и противодействие им // Российский следователь. 2015. № 18. С. 32-37.
11. Малюк А.А., Полянская О.Ю., Алексеева И.Ю. Этика в сфере информационных технологий. – М.: Горячая линия – Телеком, 2011. 344 с.
12. Шеремет И.А. Угрозы техносфере России и противодействие им в современных условиях // Вестник академии военных наук. 2014. № 1 (46). С. 27-34.

PROBLEMS OF NEUTRALIZATION OF NEGATIVE INFORMATIONAL INFLUENCE ON CORPORATE BANKING BUSINESS PROCESSES

Makeev S.A.[2]

The issues related to information security of corporate banking business processes. The quality of business–applied information technology determines the operating environment of modern credit institution. Credit organizations as special information objects are targets of negative informational influence on business processes. The source of negative informational influence is concerned the conflict breaker and form of influence is targeted attacks (advanced persistent threats, APT) using special malware. The main goal of this article is to identify the common problems associated with the neutralization of negative informational influence on corporate banking business processes. The strategy of active counteraction to threats on corporate banking business processes takes the form of neutralizing negative informational influence. The author analyzes the domain of the practice in counteraction to threats on corporate banking business processes. As a result, we identified the main problems in the neutralization of negative informational influence, including the problems of preventive protection of the business process, neutralizing the source of negative informational influence on business processes, restoring the state of the business process, protecting against psychological warfare on the participants of the business process, improving of national information law. The solution selected issues will improve organization's information security. The results should be used to develop new models and algorithms counteracting to threats and neutralizing negative informational influence on corporate banking business processes, as well as for the formation of advices to CIOs for improvement of information security management systems.

Keywords*: negative informational influence, security management, counteraction to threats*

References:

1. Andrianov V.V., Zefirov S.L., Golovanov V.B., Golduev N.A. Obespechenie informatsionnoy bezopasnosti biznesa. – Moscow, TsIPSiR, 2011, 373 p.
2. Markov A.S., Fadin A.A. Organizatsionno-tekhnicheskie problemy zashchity ot tselevykh vredonosnykh programm tipa Stuxnet, Voprosy kiberbezopasnosti. 2013. No 1(1), pp. 28-36.
3. Kazarin O.V., Sal'nikov A.A., Sharyapov R.A., Yashchenko V.V. Novye aktory i bezopasnost' v kiberprostranstve // Vestnik Moskovskogo universiteta. Seriya 12. Politicheskie nauki. 2010. No 2, pp. 71-84.
4. Kazarin O.V., Sal'nikov A.A., Sharyapov R.A., Yashchenko V.V. Novye aktory i bezopasnost' v kiberprostranstve (okonchanie), Vestnik Moskovskogo universiteta. Seriya 12. Politicheskie nauki. 2010. No 3, pp. 90-103.
5. Makeev S.A. Informatsionnaya bezopasnost' biznes-protsessov kreditnoy organizatsii v usloviyakh provedeniya informatsionnykh operatsiy, Trudy mezhdunarodnogo simpoziuma Nadezhnost' i kachestvo. 2015. T. 2, pp. 244-246.
6. Efimov E.N., Lapitskaya G.M. Informatsionnaya bezopasnost' i biznes-protsessy kompanii, Izvestiya YuFU. Tekhnicheskie nauki. 2013. No 12 (149), pp. 253-260.
7. Skryl' S.V., Belokurov S.V., Boronenkov A.I., Krasnov P.E. Sposob vyyavleniya negativnykh vozdeystviy na informatsionnye sistemy zashchity informatsii, Informatsiya i bezopasnost'. 2012. T. 15. No 3, pp. 377-382.
8. Ivlev K.G., Zatevalov A.S. Primenenie veroyatnostnykh modeley dlya utochneniya protsessa vosstanovleniya i otsenki kachestva modeley biznes-protsessov v usloviyakh ogranichennogo razmera zhurnala sobytiy, International Journal of Open Information Technologies. 2014. T. 2. No 1, pp. 32-41.
9. Dorofeev A.V., Markov A.S. Planirovanie obespecheniya nepreryvnosti biznesa i vosstanovleniya, Voprosy kiberbezopasnosti. 2015. No 3 (11), pp. 68-73.
10. Kabanov A.S., Los' A.B., Suroev A.V. Metody sotsial'noy inzhenerii v sfere informatsionnoy bezopasnosti i protivodeystvie im, Rossiyskiy sledovatel'. 2015. No 18, pp. 32-37.
11. Malyuk A.A., Polyanskaya O.Yu., Alekseeva I.Yu. Etika v sfere informatsionnykh tekhnologiy. – M.: Goryachaya liniya – Telekom, 2011, 344 p.
12. Sheremet I.A. Ugrozy tekhnosfere Rossii i protivodeystvie im v sovremennykh usloviyakh, Vestnik akademii voennykh nauk. 2014. No 1 (46), pp. 27-34.

2 Sergey Makeev, Finance University under the Government of the Russian Federation, Moscow, s.makeev@npo-echelon.ru.