

РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО ПОВЫШЕНИЮ УРОВНЯ ИНФОРМАЦИОННОЙ СОСТАВЛЯЮЩЕЙ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ (НА ПРИМЕРЕ ПАО «РОСБАНК»)

© 2022 А.А. Касьянова², О.В. Кравченко^{1,2}

¹Самарский университет государственного управления
«Международный институт рынка», г. Самара, Россия

²Самарский государственный технический университет, г. Самара, Россия

В статье рассмотрена проблема обеспечения информационной безопасности, так как рост масштабов киберпреступности, недостаточный уровень кадрового обеспечения в данном направлении создают реальные угрозы для экономической безопасности. Авторами предложены направления и механизмы по обеспечению, информационной безопасности коммерческого банка.

Ключевые слова: экономическая безопасность, информационная безопасность, кибербезопасность, ПАО «Росбанк».

Актуальность темы исследования обусловлена тем, что в современных условиях любая организация в процессе своей хозяйственной деятельности сталкивается с различными угрозами, которые оказывают дестабилизирующее воздействие на экономическую безопасность хозяйствующего субъекта. В результате для поддержания высокой конкурентоспособности и устойчивого положения на рынке организация должна постоянно актуализировать способы обеспечения всех составляющих ее экономической безопасности.

Особое место в системе экономической безопасности организации занимает информационная безопасность, которая обусловлена желанием предпринимателей обладать уникальными информационными ресурсами в условиях ужесточения конкурентной борьбы и использовать их как бесспорное конкурентное преимущество.

Целью исследования является анализ информационной безопасности ПАО «Росбанк» и разработка рекомендаций по ее повышению.

Экономическая безопасность хозяйствующего субъекта выступает комплексным понятием, охватывающим, с одной стороны, непосредственное финансовое состояние организации с учетом микроклимата, а с другой – особенности взаимодействия экономических субъектов на всех фазах воспроизводственного процесса [1]. В процессе тако-

го взаимодействия происходит более эффективное использование всех имеющихся в распоряжении организации ресурсов, позволяющих ему удерживать стабильное экономическое состояние в перспективе. В целом обеспечение экономической безопасности организации предполагает учет составляющих ее элементов: финансовой, правовой, экологической, силовой, технико-технологической, интеллектуальной, информационной безопасности. Каждый из элементов охватывает определенный участок работы предприятия, контроль за которым позволяет свести к минимуму все внутренние и внешние угрозы.

Понятие экономической безопасности предприятия раскрывают в своих трудах многие ученые. Например, А.Ю. Золотарева [2] трактует экономическую безопасность как набор условий и факторов, позволяющих хозяйствующему субъекту стабильно развиваться и самосовершенствоваться.

С.Н. Малофеев полагает, что экономическая безопасность представляет собой способность предприятия эффективно удовлетворять личные и общественные потребности при оптимальном соотношении внешних и внутренних условий экономического развития [3].

В свою очередь, И.А. Сергеева рассматривает экономическую безопасность хозяйствующего субъекта как совокупность условий и факторов, позволяющих стимулировать

положительные тенденции экономического развития предприятия и нивелировать негативные явления, минимизируя угрозы внешней среды [6].

При этом все авторы сходятся во мнении, что основной характеристикой экономической безопасности предприятия является ее должное обеспечение (благодаря которому решается большинство проблем организаций) с учетом внутренних и внешних угроз.

В современном мире доступность к информации является основным фактором разрешения спорных ситуаций в деловой среде.

В связи с этим информационная безопасность как часть экономической безопасности организации предполагает не только разработку комплексной программы по защите информационных баз данных, но и создание высокотехнологичной системы защиты, позволяющей найти оптимальное соотношение между надежностью и экономичностью. Как правило, для решения этой задачи в организациях создаются соответствующие структурные подразделения, выполняющие функции защиты информационных массивов (рис. 1) [5].

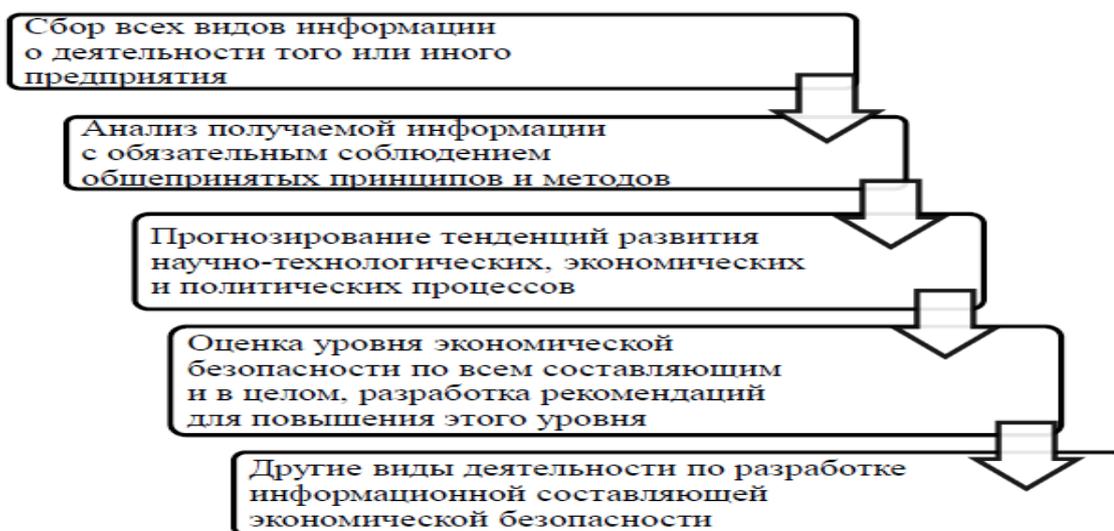


Рисунок 1 - Функции службы защиты информационной составляющей экономической безопасности организации

Обеспечение защиты информации является стратегическим направлением деятельности любой кредитно-финансовой организации. Так, на рынке банковских услуг широко известен такой банк, как ПАО «Росбанк», входящий в состав международной финансовой группы Societe Generale.

Обеспечение информационной безопасности в ПАО «Росбанк» реализуется через активное использование разнообразных информационных технологий при гарантированной защите информационных данных. К сожалению, в настоящее время в банковском секторе наблюдается рост нарушений информационной безопасности. Исключением не является и Росбанк. Так, для клиентов банка, особенно физических лиц угрозой представляет распространение приемов социальной инженерии, в первую очередь деятельность телефонных мошенников. По

оценкам банка, только в 2020 году по сравнению с 2019 годом доля розничных клиентов, подвергнувшихся мошенническим действиям, выросла на 30%: с 35 до 65% [4]. Именно благодаря наличию достаточно надежной системы информационной безопасности ПАО «Росбанк» удалось не допустить реализацию большей части мошеннических схем. Разумеется, утечка конфиденциальных корпоративных данных, например, информации о клиентах, приведет к снижению репутации банка и, как следствие, к оттоку клиентов, что недопустимо в условиях жесткой конкурентной борьбы на рынке банковских услуг. В связи с этим для ПАО «Росбанк» особенно актуально совершенствование комплекса мер в области защиты информации, предполагающих минимизацию возможных внешних и внутренних рисков и угроз.

Реализация мероприятий по обеспечению информационной безопасности ПАО «Росбанк» предполагает последовательное выполнение комплекса работ (рис. 2).



Рисунок 2 - Меры охраны информационной безопасности ПАО «Росбанк»

Как показала практика, можно выделить четыре группы угроз информационным ресурсам ПАО «Росбанк»: программные, технические, физические и режимные (рис. 3).

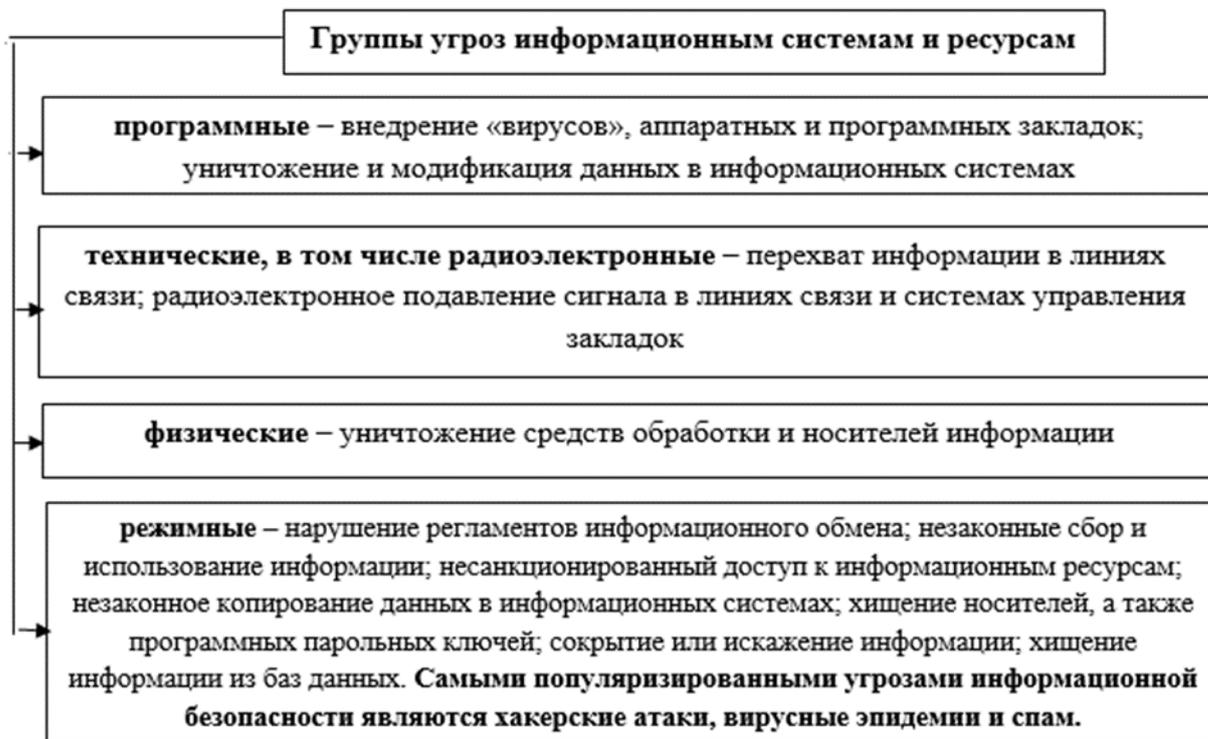


Рисунок 3 - Угрозы информационным ресурсам в ПАО «Росбанк»

В современных условиях Росбанк является стратегическим партнером в области кибербезопасности международной компании Group-IB, специализирующейся на предотвращении кибератак.

ПАО «Росбанк» совместно использует технологии Anti-Malware-on-client и систему поведенческого анализа Secure Bank, что позволяет банку оперативно реагировать на мошеннические действия с применением

приемов социальной инженерии, а также блокировать операции на основе использования украденных учетных данных. Более того, внедрение в практику банка технологий машинного обучения, кросс-канальной аналитики способствует обеспечению комплексной защиты не только цифровой личности клиента, но и его онлайн-сессий с банком.

Кроме того, использование ПАО «Росбанк» сервиса Group IB Brand Protection позволяет предотвращать до 85% кибератак на бренд банка и выявлять фишинговые сайты и мобильные приложения, направленные на совершение атак на банковских клиентов. Только за 2020 г. было обнаружено и ликвидировано около 150 групп в социальных се-

тях, которые свою нелегальную деятельность прикрывали под брендом Росбанка [4].

В настоящее время ПАО «Росбанк» для повышения информационной безопасности внедрило sGRC-платформу класса GRC, которая позволяет банку объединять информацию из различных процессов в едином интерфейсе, обеспечивая ее визуализацию и прозрачность для оперативного получения сведений о состоянии информационной безопасности [1]. В перспективе планируется расширение масштаба охвата платформы на все бизнес-процессы.

Комплекс мероприятий по обеспечению информационной безопасности в ПАО «Росбанк» разрабатывается на основе подходов к обеспечению информационной безопасности и включает ряд мер (рис. 4).

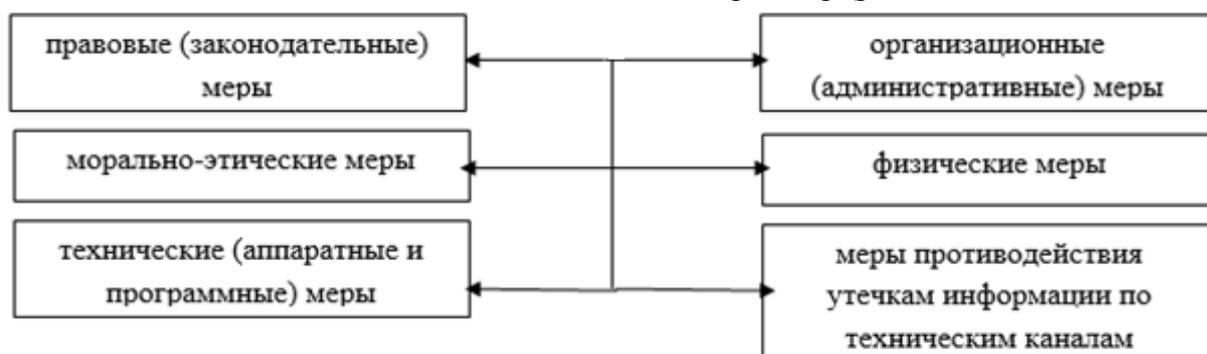


Рисунок 4 – Меры ПАО «Росбанк» по обеспечению информационной безопасности

На наш взгляд, для повышения уровня информационной безопасности банка необходимо учитывать специфические факторы, направленные на увеличение эффективности использования не только информационных ресурсов, но и на улучшение применения трудовых и материальных ресурсов, а именно:

1. Группа факторов, направленная на улучшение использования трудовых ресурсов: управление кадровыми рисками; повышение кадровых технологий; совершенствование интеллектуального потенциала сотрудников; защита здоровья, жизни, репутации специалистов и руководителей предприятия.
2. Группа факторов, связанная с увеличением эффективности использования материальных ресурсов: всестороннее предотвращение хищений материальных ценностей; уход производства в тень

(бессознательное использование электроэнергии, производственных мощностей, материальных ресурсов); обеспечение защиты технологий, в том числе исполнение патентной системы.

3. Группа факторов, связанная с повышением эффективности использования информационных ресурсов: охрана коммерческой тайны; предотвращение утечки информации; накопление информации о деятельности конкурентов с целью возможного вмешательства; обеспечение точности, полноты, непротиворечивости информации для принятия управленческих решений.

Таким образом, обеспечение информационной безопасности как одной из основных составляющих экономической безопасности позволит ПАО «Росбанк» предотвратить возможный ущерб вследствие наступления тех или иных информационных рисков, а также

обеспечить стабильный экономический рост в перспективе. Внимание руководство банка должно уделять не только информационной безопасности, но и другим функциональным составляющим экономической безопасности, важно назначать компетентных, ответственных сотрудников по каждому блоку.

СПИСОК ИСТОЧНИКОВ

1. Бойко А.В. Проблемы экономической безопасности в условиях цифровой экономики // Актуальные исследования. - 2021. - №24 (51). - С. 78-80.
2. Золотарева А.Ю. Информационная безопасность банковской сферы // Материалы XI Международной студенческой научной конференции «Студенческий научный форум». - <https://scienceforum.ru/2019/article/2018015576><https://scienceforum.ru/2019/article/2018015576>.
3. Малофеев С.Н. Проблемы защиты информации в банковской сфере // Инновации и инвестиции. - 2019. - №12. – С. 76-80.
4. Мордвинова Е.А. Информационная безопасность банковских продуктов и услуг в России // Молодой ученый. - 2021. - № 21 (363). - С. 239-241.
5. Осипова В.А. Информационная безопасность как элемент экономической безопасности // Вектор экономики. - 2020. - № 3 (45). - С. 49-55.
6. Сергеева И.А. Комплексная система обеспечения экономической безопасности предприятия. – Пенза: Изд-во ПГУ, 2017. – 124 с.

DEVELOPMENT OF RECOMMENDATIONS FOR IMPROVING THE LEVEL OF THE INFORMATION COMPONENT OF THE ECONOMIC SECURITY OF THE ENTERPRISE (ON THE EXAMPLE OF PJSC ROSBANK)

©2022 A.A. Kasyanova¹, Oksana.V. Kravchenko^{1,2}

¹Samara University of Public Administration
“International Market Institute”, Samara, Russia
²Samara State Technical University, Samara, Russia

The article considers the problem of ensuring information security, since the growth of cybercrime. The insufficient level of staffing in this area creates real threats to economic security. The authors propose directions and mechanisms for ensuring the information security of a commercial bank.

Keywords: economic security, information security, cybersecurity, Rosbank.