УДК 336.719.2

СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В БАНКОВСКОЙ СФЕРЕ

А. В. Перепелица[1)], В. А. Заянчковский[2)]

[1)] *студент экономического факультета, Белорусский государственный университет, г. Минск, Республика Беларусь, e-mail: perepelisa_alexey@mail.ru*
[2)] *студент экономического факультета, Белорусский государственный университет, г. Минск, Республика Беларусь, e-mail: slavazaja@gmail.com*

Научный руководитель: **Н. И. Шандора**

старший преподаватель, Белорусский государственный университет, г. Минск, Республика Беларусь, e-mail: Shandoranatasha@tut.by

В данной статье представлен анализ применения систем защиты информации в банковском деле, а также выявлены угрозы защиты информации и оценена их степень опасности. На основании анализа и оценки степени опасности угроз сформулировано положение Республики Беларусь в этой отрасли на данный момент, предложены рекомендации по улучшению этого положения.

Ключевые слова: система защиты информации; физическая защита; техническая защита; логический периметр; физический периметр; документация.

INFORMATION SECURITY SYSTEMS IN THE BANKING SECTOR

A. V. Perepelitsa[1)], V. A. Zayanchkouski[2)]

[1)] *student of the faculty of economics, Belarusian State University, Minsk, Republic of Belarus, e-mail: perepelisa_alexey@mail.ru*
[2)] *student of the faculty of economics, Belarusian State University, Minsk, Republic of Belarus, e-mail: slavazaja@gmail.com*

Academic supervisor: **N. I. Shandora**

senior lecturer, Belarusian State University, Minsk, Republic of Belarus, e-mail: Shandoranatasha@tut.by

This article presents an analysis of the use of information security systems in banking, as well as identified threats to information security and assessed their degree of danger. Based on the analysis and assessment of the degree of danger of threats, the position of the Republic of Belarus in this industry at the moment is formulated, recommendations are made to improve this situation.

Keywords: information security system; physical protection; technical protection; logical perimeter; physical perimeter; documentation.

Система защиты информации (далее СЗИ) – совокупность органов и исполнителей, оборудование для защиты информации, объекты защиты, работающие по установленным правовым и нормативным документам о защите информации.

Все виды защиты можно поделить на две категории: физическую и техническую. Также стоит отметить, что важнейшим общим «элементом» этих двух категорий, является документация.

Физическая защита обеспечивает безопасность физического периметра банка, то есть, его территории, зданий офисов, технологических помещений. Физическая защита строится на следующих принципах: необходимой достаточности, иерархии доступа, персональной ответственности, безопасности элементов инфраструктуры.

Физическая защита может быть представлена в виде контролируемых пропускных пунктов, системы пропусков, охраны технологических помещений, металлодетекторов и т. д.

Техническая защита обеспечивает безопасность логического периметра банка. Логический периметр – это персональные компьютеры в офисах банка и связь между ними, поэтому. Сложность этой задачи заключается в том, что, из-за большого расстояния между офисами и современных технологий, границ логического периметра нет.

Сегодня техническая защита достигается путем использования SIEM, WAF, PAM, EDR, APT, это все разного рода программы и системы, позволяющие контролировать происходящее в банке и за его пределами, отражать серьезные кибератаки.

PAM – Pluggable Authentication Modules (подключаемые модули аутентификации). EDR (Endpoint Detection and Response) и система обнаружения сложных атак APT используются вместе для обнаружения и предотвращения кибератак. WAF (Web Application Firewall) – межсетевой экран для веб-приложений. Данная программа используется для анализа трафика в веб-приложении, защиты приложений от DDOS-атак. SIEM – security information and event management (управление событиями и информацией о безопасности).

То есть SIEM не задействуется непосредственно в защите информации, эта система лишь контролирует все происходящее, получая данные от WAF, PAM, EDR, APT. Именно решением неполадок занимается специальное подразделение людей SOC или CERT, которые следят за поступающими на SIEM сигналами и реагируют на появление проблем.

SOC (Security Operations Center) – оперативный центр безопасности. CERT (Computer Emergency Response Team) – компьютерная команда (центр) по реагированию на инциденты кибербезопасности. Главное различие CERT и SOC – квалификация людей, из которых набрана команда. Если SOC может только мониторить сигналы от SIEM и передавать сведения дальше, чтобы неполадки были устранены уполномоченными людьми, то команда CERT достаточно компетентна для устранения инцидентов самостоятельно.

Таким образом, все сигналы от WAF, PAM, EDR, APT контролирует и выводить на монитор SIEM, за которой, в свою очередь, следит SOC или CERT и потом, в зависимости от классификации, либо сообщают о неполадках инженерам, либо сами пытаются их устранить.

Важную роль в защите информации играет документация. Документация должна включать: документально оформленные заявления о политики и целях руководства, процедуры и средства управления СЗИ, документированные процедуры, необходимые для результативного планирования, обеспечения функционирования и управления процессами в области защиты информации;

Все вышеперечисленные пункты помогают не упустить и оперативно найти этап, на котором была допущена ошибка. Анализ документов дает понять, где, кем и на каком этапе была совершена ошибка, а также помогает избежать идентичной или похожей ошибки в будущем.

Угрозы так же можно поделить на две категории, по причине их возникновения: угрозы технологического характера и антропогенного характера.

Угрозы технологического характера – это кибератаки, мошенничество, вредоносные программы, несанкционированный доступ, потеря информации, нарушение целостности информации.

Вызовы антропогенного характера представлены тремя основными проблемами: отток специалистов, нелояльность специалистов, нехватка компетентных специалистов.

Источники угроз имеют разную степень опасности ($К_{оп}$), которую можно измерить количественно, проведя их ранжирование. При этом оценка проводится по следующим критериям: возможность возникновения источника ($К_1$), готовность источника ($К_2$), фатальность ($К_3$).

Возможность возникновения источника – степень доступности к защищаемому объекту. Готовность источника определяет степень квалификации преступника. Фатальность определяет степень неустранимого ущерба в случае реализации угрозы.

Каждый из этих критериев оценивается по пятибалльной шкале, где 1 – минимальная степень влияния данного показателя, 5 – максимальная.

$К_{оп}$ для одного источника вычисляют по следующей формуле:

$$К_{оп} = \frac{К_1 * К_2 * К_3}{125} * 100\%,$$

где $К_1$, $К_2$, $К_3$ – степень влияния показателей от 1 до 5, а 125 – произведение трех показателей с максимальной степенью влияния.

Такую формулу можно применить и для описанных выше угроз и вызовов: кибератак, несанкционированного доступа, потери данных.

При расчете степени опасности вызовов антропологического характера нельзя применить степень квалификации, поэтому формула будет выглядеть следующим образом:

$$К_{оп} = \frac{К_1 * К_3}{25} * 100\%,$$

где $К_1$ и $К_3$ степени масштабности и фатальности соответственно.

Проделав вычисления со всеми угрозами и вызовами, можно увидеть процентное соотношение опасности угроз информации на диаграмме.

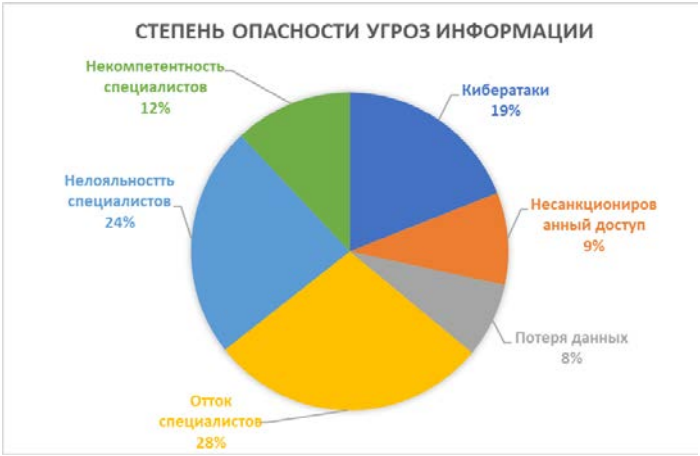

Диаграмма степеней опасности угроз информации

Примечание. Источник: [6].

Для минимизации оттока и нелояльности специалистов можно поднять зарплату и улучшить условия труда, пополнить социальный пакет. Нужно обеспечить приток иностранных специалистов и массовую подготовку высококвалифицированных работников.

Для нейтрализации некомпетентности специалистов нужно оценивать их квалификацию при приеме на работу, проводить периодические проверки квалификации сотрудников.

В связи со сложившейся обстановкой на сегодняшний день, в Беларусь не поставляются импортные программные обеспечения (далее ПО), разработанные для защиты информации, не поставляется само оборудование, также, нельзя обновить поставленные ранее ПО, потому что это вызовет отказ всей системы защиты. На данный момент кибератаки на Беларусь не расследуются всерьез, из-за политической обстановки, что значительно повышает из частоту. Существует вероятность возникновения технического перекоса, если нынешняя ситуация не исправится.

На данный момент задача состоит в том, чтобы за период отсутствия импортного ОС, ПО и оборудования сохранить достигнутый уровень защиты. Первый способ – это отказ от попыток обновить ПО и поддерживать работу уже скачанного. Второй способ – использование отечественного ПО. Третий способ – использование Open Source. Open Source – это программное обеспечение с открытым кодом, доступ к которому есть у всех пользователей в сети. Open Source используется вместо импортного ПО.

Библиографические ссылки

1. Концепция обеспечения кибербезопасности в банковской сфере / Постановление Правления Нац. Банка Респ. Беларусь. – Минск, 2019.

2. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями: СТБ П 34.101.41-2009. – Введ. 01.01.13. – Минск: Госстандарт: Белорус. гос. ин-т стандартизации и сертификации, 2013. – 13 с.

3. Менеджмент рисков информационной безопасности. Методы обеспечения безопасности: СТБ ISO/IEC 27005-2012. – Введ. 01.01.13. – Минск: Госстандарт: Белорус. гос. ин-т стандартизации и сертификации, 2013. – 60 с.

4. Система менеджмента информационной безопасности. Методы обеспечения безопасности: СТБ ISO/IEC 27001-2011. – Введ. 01.01.12. – Минск: Госстандарт: Белорус. гос. ин-т стандартизации и сертификации, 2012. – 27 с.

5. Обеспечение информационной безопасности банков Республики Беларусь. Общие положения: СТБ П 34.101.41- 2009. – Введ. 01.01.10. – Минск: Госстандарт: Белорус. гос. ин-т стандартизации и сертификации, 2010. – 31 с.

6. Белорусские и российские организации исключены из международного сообщества по борьбе с киберугрозами [Электронный ресурс] // Редакция Dev.by. – URL: https://devby.io/news/belarusskie-i-rossiiskie-organizatsii-isklucheny-iz-mezhdunarodnogo-soobschestva-po-borbe-s-kiberugrozami (дата обращения: 02.04.2022).