Валерия Павловна ЕГУРНОВА
студентка специальности «Экономическая безопасность» Тюменского государственного университета, г. Тюмень, v.p.egurnova@mail.ru
Юлия Сергеевна САХНО
кандидат экономических наук, доцент, доцент кафедры экономической безопасности, системного анализа и контроля Тюменского государственного университета, г. Тюмень, y.s.sakhno@utmn.ru

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Аннотация. Внедрение информационных технологий в финансово-кредитную сферу обуславливает повышение актуальности сохранения конференциальной и персонализированной информации, в связи, с чем необходимо рассмотрение комплексных подходов к обеспечению информационной безопасности предприятий, функционирующих в данной отрасли. В настоящей работе раскрыта система обеспечения информационной безопасности организации на примере нескольких крупных банков, в частности ПАО «Сбербанк».
Ключевые слова: информационная безопасность, цифровая экономика, защита данных, утечка данных, угрозы информационной безопасности, ПАО «Сбербанк».

Valeria Pavlovna EGURNOVA
Student of the specialty "Economic Security" at Tyumen State University, Tyumen, v.p.egurnova@mail.ru
Yulia Sergeevna SAKHNO
Candidate of Economic Sciences, Associate Professor of the Department of Economic Security, System Analysis and Control, Tyumen State University, Tyumen, y.s.sakhno@utmn.ru

ENSURING THE INFORMATION SECURITY OF THE ORGANIZATION

Abstract. The introduction of information technologies in the financial and credit sphere causes an increase in the relevance of preserving conference and personalized information, and therefore it is necessary to consider integrated approaches to ensuring information security of enterprises operating in this industry. In this paper, the information security system of the organization is disclosed on the example of Sberbank PJSC.
Keywords: information security, digital economy, data protection, data leakage, threats to information security, Sberbank PJSC.

Современное общество характеризуется повышением объемов обработки, передачи и хранения цифровой информации, необходимой для интенсификации процессов получения данных любого характера, что соответствует задачам внедрения цифровых технологий и переходу социально-экономических отношений на новый, более продвинутый уровень. Широкое использование информационных сетей и технологий в кредитно-финансовой сфере на сегодняшний день обуславливается необходимостью повышения качества предоставляемых организациями данной отрасли финансовых услуг, в том числе по операциям кредитования, инвестиционной деятельности, страховым операциям. В то же время, согласно Указу Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» быстрое развитие информационно-коммуникационных технологий сопровождается повышением вероятности возникновения угроз безопасности граждан, общества и государства [1].

Основными видами угроз, с которыми сталкиваются современные кредитно-финансовые институты можно считать:

– осуществление целенаправленных атак, направленных на возможность получения доступа к корпоративной сети;

– использование программ шифровальщиков, использование которых позволяет обеспечить потери конфиденциальных данных;

– использование вредоносного программного обеспечения, задачами которого является похищение финансовых средств со счетов клиентов;

– осуществление незаконных финансовых операций по споснированию терроризма;

– использование различных программных средств, в том числе методов социальной инженерии с целью осуществления шпионажа и последующего разглашения данных о клиентах финансово-кредитной организации, данных о ее инфраструктуре;

– предоставление недостоверных данных, порочащих репутацию организации.

Актуальность выделенных проблем подтверждается анализом статистических данных, согласно которым только по итогам 2020 г., объем несанкционированных операций, сопровождающихся хищением денежных средств со счетов клиентов, составил 1,579 млрд руб., а число мошеннических операций по персонифицированным электронным средствам платежа, использованным без согласия клиентов, составило порядка 1,5 тысяч случаев [2].

Ввиду выше сказанного, одним из актуальных направлений развития остается решение проблемы по обеспечению информационной безопасности и операционной надежности деятельности финансовых рынков. К данной категории финансовых инструментов относится активное внедрение облачных систем (для предоставления услуг через Интернет), роботизация, расширенная аналитика, визуализация, когнитивные вычисления, технология блокчейн [2].

Блоки, применяемые кредитными организациями, с целью обеспечения информационной безопасностью реализуются на нескольких функциональных уровнях, представленных на рисунке 1.

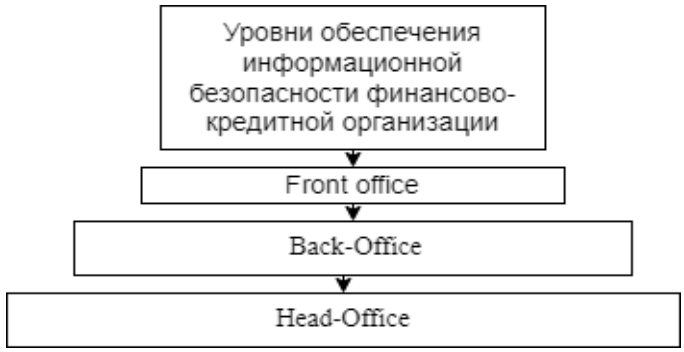

Рис. 1. Уровни обеспечения информационной безопасности

Источник: [3].

Рассмотрим каждый уровень подробнее.

Front-Office. На этом уровне находятся рабочие места, обеспечивающие операционную деятельность банка, обработку платежных поручений, депозитные операции, приобретение ценных бумаг.

Back-Office. Этот модуль обеспечивает оставление отчетности на основе полученной информации, которая в дальнейшем будет передана в Банк России.

Head-Office. Здесь сосредоточены блоки, занимающиеся аналитической работой и интеллектуальной обработкой данных.

Работа всех подсистем производится в отдельных сферах, которые отделены друг от друга межсетевыми экранами. Помимо них, в обязательном порядке используются: антивирусная система защиты, средства, выявляющие вторжения, криптографические средства, средства доверенной загрузки.

Рассмотрим принципы разработки и внедрения принципов обеспечения информационной безопасности на примере нескольких крупных банков.

В АО «Альфа-Банк» используется система криптозащиты, построенная на основе международно-признанного протокола SSL, обеспечивает шифрование персональных данных пользователей с использованием стойкого криптоалгоритма на основе 128-битного ключа. Для обеспечения безопасной работы в сети корпоративных пользователей используется криптографический микропроцессор, встроенный в электронный ключ eToken PRO, который служит:

– для идентификации пользователя. Каждый ключ eToken PRO имеет уникальный серийный номер, записанный в защищенной памяти микросхемы и напечатанный на корпусе ключа;

– строгой двухфакторной аутентификации пользователей при подписи документов. Данная процедура проверки позволяет достоверно убедиться в том, что абонент, предъявивший электронный ключ eToken, является его законным владельцем;

– формирования аналога собственноручной подписи (АСП) документов, защищающего электронный документ от подделки и обеспечивающего целостность, авторство и конфиденциальность подписываемых документов [4].

АО «Россельхозбанк» использует DLP-решение Solar Dozor, которое оптимизировано для задач выявления ранних признаков корпоративного мошенничества и проведения полномасштабных расследований. Чтобы бороться с внутренними нарушениями, в Solar Dozor реализован широкий набор специализированных инструментов, в числе которых — полный архив коммуникаций сотрудников [5].

ПАО «Сбербанк» разрабатывает единые правила и стандарты для всех организаций, находящихся с ним в едином информационном поле. Для каждой отдельно взятой фирмы ПАО «Сбербанк устанавливает собственный риск-профиль, в расчет которого включено более шестнадцати факторов риска.

Следующая ступень обеспечения информационной безопасности в исследуемой организации — использования современных технологий, в частности, ПАО «Сбербанк» в данных целях использует платформу BI.ZONE, на которой обобщается вся информация о информационных рисках, и инцидентах, являющихся нарушением информационной безопасности. Данная платформа в режиме реального времени позволяет отслеживать состояние всех компаний,

обобщенных в единую систему с позиций информационной безопасности, а также позволяет оценить эффективность защиты персонализированной информации.

Третья ступень обеспечения информационной безопасности ПАО «Сбербанк» — распределение рисков и ответственности. В настоящее время в организации действует четыре типа соглашения о цифровой безопасности, которые зависят от уровня интеграции в инфраструктуру. В них отражены меры соответствия минимальной степени защиты, зафиксирована ответственность за вероятные инциденты/ущербы, которые могут быть нанесены экосистеме в совокупности. Выполнять данное соглашение юридически в обязательном порядке для всех.

Четвертая ступень обеспечения информационной безопасности ПАО «Сбербанк» агломерация опыта и знаний. Так, одним из условий обеспечения информационной безопасности организации является присутствие в организации подразделения, которое отвечает за информационную безопасность, либо такого сотрудника.

Пятая ступень выражена концентрированностью на страже интересов клиентов, даже при совершении ими нетипичных действий или ошибок при эксплуатации систем и программных продуктов [6]. В Сбербанке функционирует центр фрод-мониторинга, опекающий потребителей банковских услуг и при осуществлении любых необычных операций связывающийся с клиентами, пресекая мошеннические действия кибер-преступников.

Так же в рамках организации функционирует фрод-мониторинг, эффективность работы центра которого на сегодняшний день достигла лучших в мировом масштабе показателей и приблизительно 97% операций, являющихся мошенническими, кредитная организация хеджирует и не допускает совершения преступления.

Таким образом, можно сказать, что ПАО «Сбербанк» проводит огромнейшую каждодневную работу для изменения внутреннего ландшафта управления рисками информационной безопасности, постоянно интегрирует принципы информационной культуры, осуществляет обучающие мероприятия персонала, что в конечном итоге позволяет решить многие из проблем обеспечения информационной безопасности. Благодаря трансформации систем обеспечения информационной безопасности по примеру ПАО «Сберабанк» банки смогут обеспечивать сохранность и безопасность данных, что значительно повысит доверие к банковской системе РФ в целом.

Необходимо подчеркнуть, что принятие действенных мер по предотвращению атак, утечки конфиденциальной информации клиентов, а также несанкционированного доступа к денежным средствам потребителей банковских услуг — необходимое условие эффективного развития банковского сектора в будущем.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 02.07.2021 № 400 // КонсультантПлюс: надежная правовая поддержка: [официальный сайт]. 1997-2022. URL: http://www.consultant.ru/document/cons_doc_LAW_389271/ (дата обращения: 09.11.2021).
2. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств // ЦБ.ру [сайт]. URL: https://cbr.ru/analytics/ib/review_1q_2q_2020/ (дата обращения: 25.11.2021).
3. Соловьев С.В., Язов Ю.К. Информационное обеспечение деятельности по технической защите информации // Вопросы кибербезопасности, 2021. № 1(41). С. 69-79.
4. Политика в отношении обработки персональных данных в Альфа-Банке // АО «Альфа-Банк» [официальный сайт] 2001-2022. URL: https://alfabank.ru/about/personal_politics/ (дата обращения: 25.11.2021).
5. Информационная политика АО «Россельхозбанк» // АО «Россельхозбанк» [официальный сайт] 2000-2022. URL: https://www.rshb.ru/download-file/377160/?ysclid=l34r8ijp8n (дата обращения: 25.11.2021).
6. Информационная политика ПАО Сбербанк // ПАО «Сбербанк» [официальный сайт] 1997-2022. URL: https://www.sberbank.com/common/img/uploaded/files/pdf/normative_docs/informatsionnaya_politika_rus.pdf (дата обращения: 25.11.2021).