https://doi.org/10.24182/2073-9885-2020-13-3-20-31

М. А. Доценко

Студент,
travis110011@gmail.com

Финансово-экономический факультет,
Финансовый университет при Правительстве РФ,
Москва, Российская Федерация

Система экономической безопасности в сфере IT-технологий в Банке Тинькофф

Аннотация: *В настоящее время автоматизация процессов в компаниях является необходимым процессом, так как она совершенствует их деятельность. Средством автоматизации является внедрение и использование информационных технологий. Автор рассматривает систему экономической безопасности в сфере IT-технологий в Банке Тинькофф.*

Ключевые слова: *информационные технологии, информационная безопасность, риски.*

M. A. Dotsenko

Student,
travis110011@gmail.com

Faculty of Finance and Economics,
Financial University under the Government of the Russian Federation,
Moscow, Russian Federation

Economic security system in the field of IT technologies at Tinkoff Bank

Annotation: *Currently, automation of processes in companies is a necessary process, as it improves their activities. The automation tool is the introduction and use of information technologies. The author examines the system of economic security in the field of IT technologies in Tinkoff Bank.*

Keywords: *information technologies, information security, risks.*

Сегодня потребность в применении эффективных и адекватных реальной действительности технологий и компьютерных программ возрастает. Произошло смещение акцентов в формулировании критериев эффективности систем управления, поскольку качество экономических

решений зависит от скорости принятия, степени их адекватности и возможности использования прогнозных моделей.

Информационные технологии – это особый сектор экономики, который отвечает за создание компьютерных систем, их программирование и управление компьютерными сетями[1]. Классификации информационных технологий по виду обрабатываемой информации представлена в таблице 1.

Таблица 1

Классификация информационных технологий по виду обрабатываемой информации [2]

Информация	Информационные технологии
Текст	Текстовые редакторы и процессоры
Данные	Электронные таблицы Базы данных Алгоритмические языки
Графика	Графические редакторы
Удаленные объекты	Сетевые технологии
Знания	Экспертные системы
Объекты реального мира	Мультимедиа

Информационные технологии резко увеличивают темпы изменений в экономике. Информация стимулирует скорость развития технологий. Поэтому ИТ – это технология, которая увеличивает скорость технического прогресса. На корпоративном уровне информационные технологии могут способствовать улучшению обслуживания клиентов и снижению затрат. Важное знание информационных технологий заключается в том, что они позволяют реорганизовать бизнес и делать вещи, которые раньше были невозможны, которые приносят пользу клиентам, например, сокращение времени цикла, улучшение порядка заказов и меньший объем складских запасов[3].

[1] Федотова Е. Л. Информационные технологии в профессиональной деятельности: учеб. пособие / Е.Л. Федотова. – Москва: ИД «ФОРУМ»: ИНФРА-М, 2018. С. 27.

[2] Сакова Т. Г. Информационные технологии в сфере экономической безопасности [Электронный ресурс]: учеб. пособие / Т.Г. Сакова, О.В. Юдина. – Самара: Изд-во Самар. гос. экон. ун-та, 2019. https://lms2.sseu.ru/pluginfile.php/321743/mod_resource/content/1/Пособие Сакова Юдина.pdf.

[3] Степура М.А. Использование информационных технологий в экономике. Дневник науки. 2020. № 1 (37). С. 36.

Информационные технологии позволяют передавать большие объемы точной информации практически в любую точку за относительно короткий период времени. Использование информационных технологий в системе экономической безопасности представляет собой набор стратегий кибербезопасности, которые предотвращают несанкционированный доступ к активам компании, таким как компьютеры, сети и данные. Он поддерживает целостность и конфиденциальность конфиденциальной информации, блокируя доступ искушенных хакеров.

Интернет-безопасность включает в себя защиту информации, отправляемой и получаемой в браузерах, а также безопасность сети с использованием веб-приложений [4]. Эти средства защиты предназначены для мониторинга входящего интернет-трафика на наличие вредоносных программ и нежелательного трафика. Эта защита может быть в виде брандмауэров, защиты от вредоносных программ и программ-шпионов.

Информационные технологии на сегодняшний день стали неотъемлемой частью деятельности в различных сферах, банковская сфера не является исключением. Информационные технологии служат средством автоматизации выполнения различных функций, а также снижают издержки, совершенствуют бизнес-процессы банков, увеличивают и оптимизируют конечный результат.

Объектом исследования выступил АО «Тинькофф Банк».

Основным направлением деятельности Банка является предоставление качественных розничных банковских онлайн-услуг физическим лицам и юридическим лицам в сегменте малого и среднего бизнеса. Акцентом деятельности 2020 года является создание, продвижение и развитие финансовых и дополняющих сервисов с целью формирования современной высокотехнологичной экосистемы, отвечающей текущим и будущим потребностям розничных и корпоративных клиентов. Ряд ранее инновационных подходов Банка в области удаленного, онлайн- и мобильного обслуживания широко перенимаются иными участниками банковского сектора, что способствует развитию отрасли в целом до уровней, превышающих большинство аналогов в зарубежных странах. Одновременно данный подход способствует качественной продуктовой, сегментной и региональной диверсификации источников прибыли Банка.

[4] Федотова Е. Л. Информационные технологии в профессиональной деятельности: учеб. пособие / Е.Л. Федотова. – Москва: ИД «ФОРУМ»: ИНФРА-М, 2018. С. 29.

Особенность банка состоит в том, что у банка нет отделений: все его клиенты обслуживаются дистанционно через онлайн-каналы и контакт-центр. В облачном колл-центре банка работает более 10 000 сотрудников, что делает его одним из самых крупных в Европе. Собственная сеть представителей из 2500 человек по всей России позволяет доставлять продукты уже на следующий день после заявки. Вся численность сотрудников банка в 2019 г. около 25 тыс. чел.[5]

Банк развивает экосистему Tinkoff.ru, которая предоставляет финансовые и лайфстайл-услуги. Помимо классических банковских продуктов в нее входят инвестиции, путешествия, обслуживание бизнеса, ипотека, страхование, мобильный оператор, развлечения и образование (рис. 1).

Тинькофф представляет собой технологическую компанию с банковской лицензией. Примерно 70% сотрудников штаб-квартиры – IT-специалисты, которые каждый день создают лучшие цифровые продукты в России. Список известных внедрений ИТ-систем в компании за последние три года представлен в таблице 2.

Таблица 2

Список известных внедрений ИТ-систем в АО «Тинькофф Банк» за 2018–2020 гг. [6]

Интегратор	Продукт	Технология	Год
Ростелеком-Solar (ранее Solar Security, Солар Секьюрити)	Solar JSOC	ИБ – Межсетевые экраны, ИБ – Предотвращения утечек информации, ИБ – Система обнаружения мошенничества (фрод)	2020
Эверпоинт (Everpoint)	Everpoint: Бизнес-навигатор МСП	BI, ГИС – Геоинформационные системы	2019
StarForce Technologies (Протекшен Технолоджи)	Комплексные проекты по информационной безопасности	ИБ – Антивирусы, ИБ – Антиспам, ИБ – Аутентификация, ИБ – Межсетевые экраны, ИБ – Предотвращения утечек информации	2019
Без привлечения консультанта или нет данных	Единая биометрическая система (ЕБС), Ключ Ростелеком	ИБ – Биометрическая идентификация	2018
Центр Высоких Технологий (ЦВТ)	Мобильное приложение	ИТ-аутсорсинг, Офисные приложения	2018
Ant Financial Services Group	Alipay		2018

Проекты самого АО «Тинькофф Банк» представлены в таблице 3.

[5] https://www.tinkoff.ru/.
[6] Там же.

Рис. 1. Экосистема АО «Тинькофф Банк» [7]

[7] https://www.tinkoff.ru/.

Таблица 3

ИТ-технологии АО «Тинькофф Банк»[8]

Продукт	Технология
Тинькофф Олег Голосовой помощник	Речевые технологии
Тинькофф Инвестиции Брокерская платформа	Системы дистанционного банковского обслуживания
Тинькофф Конструктор сайтов	CMS – Системы управления контентом
Tinkoff Junior	Системы дистанционного банковского обслуживания
Тинькофф Ипотека	Системы дистанционного банковского обслуживания
Тинькофф Инвестиции: Веб-терминал для торгов на бирже	Системы автоматизации торговли
Тинькофф Банк Поиск недвижимости	ГИС – Геоинформационные системы
Tinkoff VoiceKit ИБ	Биометрическая идентификация, Речевые технологии
Тинькофф Интернет-эквайринг	Системы дистанционного банковского обслуживания
Тинькофф АЗС	Мобильное приложение Тинькофф
Тинькофф Суперприложение (Tinkoff Super App)	Системы автоматизации торговли, Системы дистанционного банковского обслуживания
Тинькофф "Кеша" Цифровой банкомат ИБ	Средства шифрования, Системы дистанционного банковского обслуживания
Тинькофф Аутсорсинговый колл-центр	Call-центры, SaaS – Программное обеспечение как услуга, ИТ-аутсорсинг
Тинькофф: Личный кабинет	Системы дистанционного банковского обслуживания

Тинькофф Банк – это не классический банк, а ИТ-компания с банковской лицензией. У этого банка нет офисов, а все вопросы, возникающие у клиентов, решаются дистанционно. В штате банка есть большое количество разработчиков, администраторов систем, представители сторонних организаций, которых руководство привлекаем на аутсорс. В связи с чем, у банка имеется такая проблема экономической безопасности как постоянная необходимость контролировать сотрудников, работающих удаленно. Таких специалистов АО «Тинькофф Банк» контролирует на точках входа в инфраструктуру банка. Деятельность сотрудников, имеющих удаленный рабочий доступ к внутрикорпоративным системам, также контролируется.

Для АО «Тинькофф Банк» характерны риски, которые присущи ИТ-компаниям (рис. 2).

[8] https://www.tinkoff.ru/invest/news/250169/.

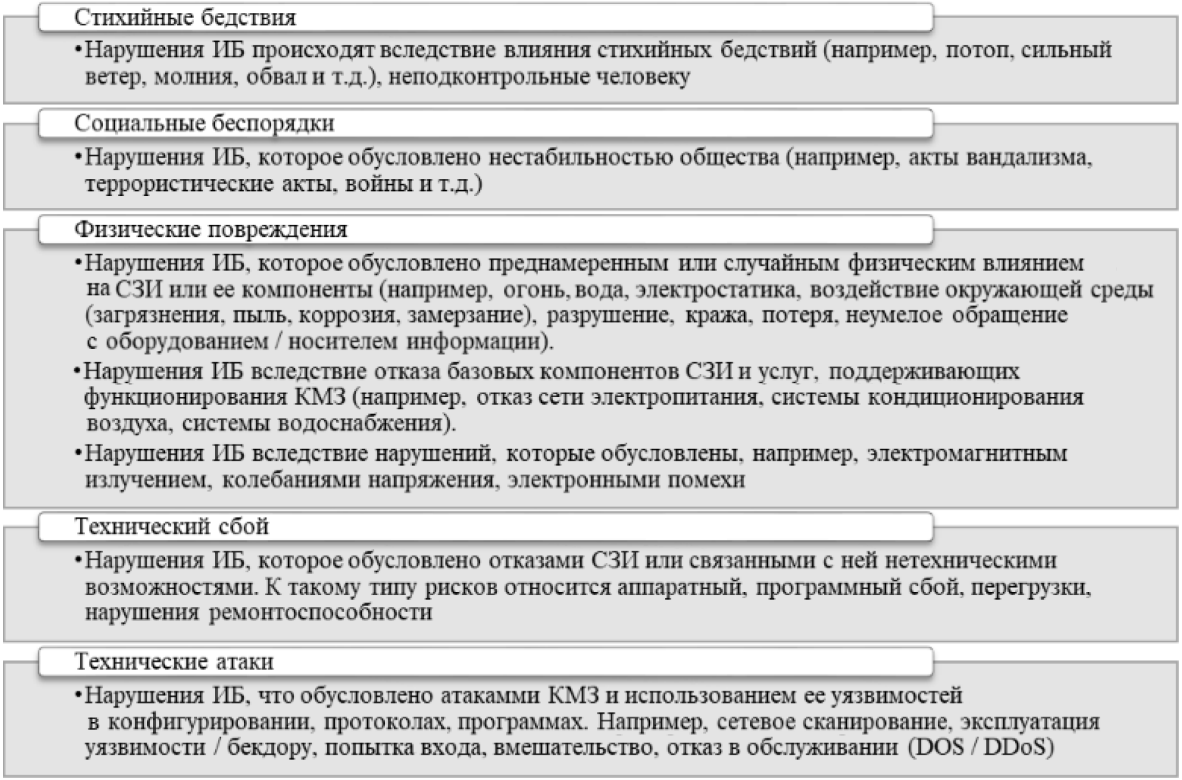

Рис. 2. Риски, которые присущие АО «Тинькофф Банк» [9]

[9] Разработано автором.

Также в тренде целевые атаки, которые бок о бок идут с социальной инженерией, и DDoS-атаки, которые никуда не исчезли. С этими явлениями работать гораздо проще, чем с вирусами, которые злоумышленники пишут для целенаправленных действий. Стандартные антивирусы не обнаруживают зловредных объектов, которые написаны для объекта атаки. Системы, которые позволяют фиксировать такие целевые атаки на конкретную финансовую организацию и выявлять риски на лету – это другой класс безопасности.

В банке регулярно проводится аудит безопасности. У банка есть несколько регулярных аудитов. Есть аудиты информационной безопасности, которые банк обязан совершать в сроки, регламентированные регулятором – Центральным банком России. Как правило, такая проверка проводится один раз в год.

Существуют аудиты безопасности, которые руководство банка организует в отношении ряда критических систем в течение месяца или квартала. По внутреннему регламенту проверка систем проводится раз в три месяца.

В течение последних лет в сфере безопасности банк внедрил такие крупные проекты в сфере информационной безопасности, как например, внедрение системы класса Mobile Device Management. Многие сотрудники банка хотят иметь доступ к почте, отвечать на сообщения, быть мобильными и эффективными вне офиса. Раньше доступ на устройство выдавался через почтовый сервер. При такой реализации существовали риски утраты рабочих файлов и данных в результате пропажи или кражи самого устройства. Вся информация шла по «незащищенному» каналу связи. Варианты перехвата могли быть самыми разными.

В банке долго искали решение на рынке, обратились к оценкам Gartner. В итоге остановились на одном из пяти вендоров. Это решение позволяет всю рабочую почту держать на устройстве в защищенном паролем контейнере. В контейнер помещаются рабочий календарь, почта, заметки. Передача почты с сервера банка на конечное устройство осуществляется по защищенному каналу.

Если пользователь потерял устройство, то не всегда сразу сообщает в службу поддержки, что у него были установлены мобильные корпоративные сервисы Тинькофф Банка. А здесь оператор по безопасности через MDM может оперативно отреагировать.

Концепция BYOD активно развивается, ведь Тинькофф Банк стремится быть на шаг впереди классических игроков. Недавно пользователей BYOD было порядка 150, а сейчас их количество превышает 300 [10]. В прошлом году специалисты банка окончательно внедрили DLP-систему, докупив модуль для контроля над e-mail, web-трафиком, удаленными рабочими станциями и конечными пользователями.

Была также внедрена SIEM-система. Она позволяет собирать и коррелировать все логи со всех устройств сети, которые есть, показывать правила, нестандартные ситуации и незамедлительно информировать о нештатных ситуациях офицера ИБ. SIEM-система обрабатывает логи и производит корреляцию. Оператору теперь ни к чему тратить время на ручной поиск объектных инцидентов: система предоставляет некий предварительный результат, с которым специалисту необходимо ознакомиться и принять решение.

Это некий web-шлюз внутри банка, по которому в защищенном режиме записываются логи о входе в корпоративные системы удаленных сотрудников и администраторов. В случае инцидента, служба безопасности банка конкретно сможет найти причину и сделать выводы на будущее, чтобы избежать аналогичных последствий.

Также в банке завершен проект по защите баз данных. Для этого банком было приобретено и внедрено серьезное решение. В первую очередь защищаются те базы, где содержится критически важная информация по клиентам. Инициатором всех проектов, связанных с информационной безопасностью, был департамент безопасности банка. В его состав входит управление информационной безопасности, которое взаимодействует с ИТ-подразделением.

Один из крупнейших проектов, который на стадии реализации, это защита от APT-атак. В банке долго тестировали большие, сложные системы, которые позволяют отлавливать специфические атаки и противодействовать им. Возможно, количество пользователей корпоративными системами возрастет, в связи с чем получит развитие MDM-решения.

Кроме того, в АО «Тинькофф Банк» возникшие инциденты разделяются по виновникам и каналам происшествий. В банке принято разделять виновников на внешних и внутренних, а инциденты – по кана-

[10] Интервью с вице-президентом по безопасности Тинькофф Банка // http://www.tadviser.ru/index.php/Статья:Интервью_с_вице-президентом_по_безопасности_Тинькофф_Банка.

лам, поскольку необходимо понимать, как предотвращать возможные атаки на банк и минимизировать количество рисков. В банке все автоматизировано в плане информационной безопасности, проводится постоянный анализ и улучшаются процессы ИБ.

Основные каналы, которые подвергаются рискам – это наиболее важные коммуникационные системы. В первую очередь речь идет о корпоративной почте [11]. Если проблемы спама решаются специализированными средствами, то для предотвращения утечек информации в банке установлена DLP-система. Риски того, что специалист банка может умышленно или не осознанно отправить служебную информацию по почтовому каналу, существуют всегда.

Второй важный канал взаимодействия сотрудников с банком – web-канал. Здесь также служба безопасности банка все тщательно контролирует. В зависимости от функционала, сотрудникам предоставляется различный доступ в интернет, а некоторым работникам разрешен только определенный список сайтов. За последний годы количество нарушений со стороны персонала заметно сократилось. Чем больше сотрудник знает о правилах работы в банке и информационной безопасности, тем меньше он что-то нарушает.

А чтобы повышать грамотность сотрудников банка для них была запущена учебная программа. Обучение в обязательном порядке проходят новые специалисты, получая необходимые навыки по работе с корпоративной почтой, интернетом, со съемными носителями, антивирусной защитой и так далее. Программа была сделали интерактивной, чтобы она действительно была интересной для слушателей. Иногда основой для лекций становятся случаи из практики банка. Например, в одном из прошлых лет банк подвергся мощной DDoS-атаке. Специалисты по информационной безопасности установили исполнителей и совместно с правоохранительными органами привлекли их к уголовной ответственности. Из этого кейса был сделан хороший урок.

Банком были усилены внешние системы и налажено взаимодействие с компаниями, которые предоставляют специализированные услуги по чистке трафика от DDoS-атак. Как правило, учебная программа изменяется раз в полгода, она модернизируется и из нее убираются устаревшие элементы.

[11] Коммуникационные риски // https://www.sites.google.com/site/kyrsbez/21.

Таким образом, выполненные Банком проекты позволяют поддерживать в нем высокий уровень автоматизации бизнес-процессов и обрабатывать нарастающий поток операций с высокой степенью надежности. Рост информационных систем соответствует темпам развития бизнеса Банка, а результаты деятельности подтверждают оптимальный выбор ИТ-технологий.

В перспективе произойдет усиление государственного регулирования банковской сферы. Центральный банк будет усиливать регулирование деятельности коммерческих банков [12]. Компании в свою очередь будут противостоять возрастающим вызовам высокотехнологичных мошенников и хакеров. Все это будет происходить на фоне развития ИТ-отрасли и технологий. Вместе с этим, развиваются новые угрозы, которым банки вынуждены будут противостоять.

Список литературы

1. Интервью с вице-президентом по безопасности Тинькофф Банка // http://www.tadviser.ru/index.php/Статья:Интервью_с_вице-президентом_по_безопасности_Тинькофф_Банка.
2. Коммуникационные риски // https://www.sites.google.com/site/kyrsbez/21.
3. Орлова И.А., Степанова Д.С. Основные тренды развития цифровых технологий в банковской сфере. Инновационные технологии в машиностроении, образовании и экономике. 2019. Т. 22. № 2 (12). С. 71–74.
4. Очкасова Е.О., Буслаева И.Ю., Строева Т.С. Роль информационных технологий в банковской сфере. Научно-практические исследования. 2019. № 7-1 (22). С. 12–14.
5. Сакова Т. Г. Информационные технологии в сфере экономической безопасности [Электронный ресурс]: учеб. пособие / Т.Г. Сакова, О.В. Юдина. – Самара: Изд-во Самар. гос. экон. ун-та, 2019. https://lms2.sseu.ru/pluginfile.php/321743/mod_resource/content/1/Пособие Сакова Юдина.pdf.
6. Степура М.А. Использование информационных технологий в экономике. Дневник науки. 2020. № 1 (37). С. 36.
7. Федотова Е. Л. Информационные технологии в профессиональной деятельности: учеб. пособие / Е.Л. Федотова. – Москва: ИД «ФОРУМ»: ИНФРА-М, 2018. 367 с.

[12] Орлова И.А., Степанова Д.С. Основные тренды развития цифровых технологий в банковской сфере. Инновационные технологии в машиностроении, образовании и экономике. 2019. Т. 22. № 2 (12). С. 74.

8. Шандриков А. С. Информационные технологии: учебное пособие / А. С. Шандриков. 3-е изд., стер. – Минск: РИПО, 2019. 443 с.
9. https://www.tinkoff.ru/.
10. https://www.tinkoff.ru/invest/news/250169/.

References

1. Interview with Tinkoff Bank's Vice President for security // http://www.tadviser.ru/index.php/Статья:Interviewee-президентом_по_безопасности_Тинькофф_банка.
2. Communication risks // https://www.sites.google.com/site/kyrsbez/21
3. Orlova I. A., Stepanova D. S. Main trends in the development of digital technologies in the banking sector. Innovative technologies in mechanical engineering, education and economy. 2019. Vol. 22, No. 2 (12). Pp. 71–74.
4. Achkasov E. A., Buslaev, Y. I., Stroeva T. S. the Role of information technology in the banking sector. Scientific and practical research. 2019. # 7-1 (22). Pp. 12–14.
5. Sakova T. G. Information technologies in the sphere of economic security [Electronic resource]: textbook. manual / T. G. Sakova, O. V. Yudina. – Samara: publishing house of Samar state economy. UN-TA, 2019. https://lms2.sseu.ru/pluginfile.php/321743/mod_resource/content/1/Handbook of Sakov Yudin. pdf.
6. Stepura M. A. Use of information technologies in the economy. Journal of science. 2020. no. 1 (37). P. 36.
7. Fedotova E. L. Information technologies in professional activity: textbook. manual / E. L. Fedotova. – Moscow: FORUM publishing house: INFRA-M, 2018. 367 p.
8. Information technologies: a textbook / A. S. Shandrikov. 3rd ed., ster. Minsk: RIPO, 2019. 443 p.
9. https://www.tinkoff.ru/.
10. https://www.tinkoff.ru/invest/news/250169/.