УДК 537.531

ОЦЕНКА РИСКОВ КИБЕРБЕЗОПАСНОСТИ В ФИНТЕХ КОМПАНИЯХ

Мотуз А. А., студент гр. 861402

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Петров С.Н. – канд. техн. наук, доцент

Аннотация. Представлены основные типы угроз кибербезопасности, оценены риски данных угроз.

Ключевые слова. Угрозы кибербезопасности, вредоносное ПО, оценка рисков.

Аудит информационной системы - это процесс сбора и оценки доказательств для определения того, была ли компьютерная система разработана для поддержания целостности данных, защиты активов, эффективного достижения целей организации и эффективного использования ресурсов.
Для защиты от киберугроз необходимы следующие компоненты:
– Надежный брандмауэр и прокси-сервер
– Антивирусное программное обеспечение
– Своевременное и частое сканирование сетевых уязвимостей
Финтех компаниям (организациям, которые при построении своих бизнес-моделей в сферах финансовых услуг используют современные технологии и IT-продукты) следует проводить внутреннюю/внешнюю оценку рисков, включая тестирование на проникновение, сканирование уязвимостей, социальную инженерию и анализ бизнес-процессов, связанных с безопасностью данных. Они также должны разработать дорожную карту облачных вычислений, основанную на подверженности бизнес-рискам (низкий-высокий), стоимости владения и возможности возврата инвестиций в переход на облако.
Необходимость количественной оценки рисков и возможное влияние нарушений безопасности на репутацию мотивируют к более строгим процедурам внутреннего аудита и оценки рисков.
Согласно ежегодного отчету агентства Европейского Союза по сетевой и информационной безопасности (ENISA) об инцидентах в сфере телекоммуникационной безопасности за 2018 год, сегодня организации должны учитывать четыре основных типа ИТ-рисков: риски безопасности, риски доступности, риски производительности и риски соответствия требованиям. Риски безопасности представляют собой несанкционированный доступ к информации: утечка данных, конфиденциальность данных, мошенничество и безопасность конечных точек. Риски безопасности включают также широкие внешние угрозы, такие как вирусы, а также более целенаправленные атаки на конкретные приложения, конкретных пользователей и конкретную информацию.
Для оценки величины угрозы необходимо оценить:
– вероятность её реализации;
– потенциал злоумышленника, реализующего угрозу.
Решение о степени критичности угрозы информационной безопасности принимается в соответствии с таблицей 1.

Таблица 1 – Матрица рисков

Потенциал злоумышленника	Вероятность выполнения			
	Низкая 0	Средняя 1	Высокая 2	Крайне высокая 3
Низкий 0	0	1	2	3
Средний 1	1	2	3	4
Высокий 2	2	3	4	5

Для каждой из выявленных угроз оценивается ее вероятность, потенциал реализующего угрозу нарушителя и, как следствие, степень критичности угрозы.
Из общего списка угроз формируется список критических угроз, которые следует блокировать в первую очередь (угрозы, находящиеся в красной зоне – имеющие 4-5 баллов). В таблицах 2, 3 представлены угрозы для клиентов (физических лиц) и сетевых объектов.
Угрозы хищения у клиентов [2-3] (физических лиц):

– заражение вредоносным ПО (клиент);
– халатность заказчика (социальная инженерия, разглашение или утеря аутентификационных данных);
– халатность сотрудников финтех компании (некомпетентность в обслуживании);
– умышленные действия сотрудника финтех компании;
– фишинг.
Угрозы обслуживанию, хищения у клиентов (юридических лиц):
– заражение вредоносным ПО (клиент);
– халатность сотрудника финтех компании (некомпетентность в обслуживании);
– умышленные действия сотрудника финтех компании;
– фишинг;
Угроза потери контроля над сетевыми объектами [4] :
– использование возможностей финтех компании для атаки на клиентов;
– использование возможностей финтех компании для получения доступа к информации внутри сети.
Угрозы полной/частичной утраты или недоступности активов:
– вредоносное ПО (инфраструктура, AWS);
– DoS/DDoS-атаки;
– APT-атака.
Угроза потери/недоступности банка данных при использовании облачных технологий:
– DoS/DDoS-атаки на провайдера.
Утечка конфиденциальной информации из-за некомпетентности сотрудников:
– отправка по открытым каналам связи;
– компрометация учетных записей администратора.

Таблица 2 – Угрозы хищения у клиентов (физических лиц)

№	Угроза	Потенциал нарушителя	Вероятность выполнения	Критическая область
1	Заражение вредоносным ПО (клиент)	2 (высокий)	3 (крайне высокая)	5
2	Заражение вредоносным ПО (финтех компания)	2 (высокий)	1 (средняя)	3
3	Умышленные действия третьих лиц	2 (высокий)	3 (крайне высокая)	3
4	Халатность заказчика (социальная инженерия, разглашение или утеря аутентификационных данных)	2 (высокий)	3 (крайне высокая)	5
5	Халатность сотрудников финтех компании (некомпетентность в обслуживании)	2 (высокий)	2 (высокая)	4
6	Умышленные действия сотрудника финтех компании	2 (высокий)	2 (высокая)	4
7	Фишинг	2 (высокий)	2 (высокая)	4
9	Скимминг	2 (высокий)	1 (средняя)	3
11	Подбор кодового слова у клиента	1 (средний)	2 (высокая)	3

Таблица 3 – Угроза потери контроля над сетевыми объектами

№	Угроза	Потенциал нарушителя	Вероятность выполнения	Критическая область
12	Возможность финтех компании участвовать в рассылке спама	2 (высокий)	1 (средняя)	3
13	Использование возможностей финтех компании для участия в DDoS-атаках	2 (высокий)	1 (средняя)	3
14	Использование возможностей финтех компании для атаки на клиентов	2 (высокий)	2 (высокая)	4
15	Использование возможностей финтех компании для получения доступа к информации внутри сети	2 (высокий)	2 (высокая)	4

Список использованных источников:

1. ISO/IEC 27001 Information technology. Security techniques. Information security management systems. [Электронный ресурс]. – Режим доступа: https://www.iso.org/ru/standard/54534.html.

2. Regulation (EU) 2016/679 Of The European Parliament And Of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). [Электронный ресурс] – Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri= CELEX:02016R0679-20160504
3. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. [Электронный ресурс] – Режим доступа: https://eur-lex.europa.eu/eli/dir/1995/46/oj.
4. Risk analysis framework for a cloud specific environment [Электронный ресурс]. – Режим доступа: https://studylib.net/doc/8837952/risk-analysis-framework-for-a-cloud-specific-environment.