ВНЕДРЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В БАНКОВСКОЙ ОБЛАСТИ
(IMPLEMENTATION OF SECURITY OF INFORMATIONAL TECHNOLOGIES IN BANKING SECTOR)

STATNIK AUREL, student, anul I, TI-192
Academia de Studii Economice a Moldovei
Republica Moldova, mun. Chişinău, str. Mitropolit Gavriil Bănulescu- Bodoni, 61, MD-2005
e-mail autor: s.aurel@mail.ru

Abstract. *The aim of this work is to show the weaknesses in the banking sector and methods for eliminating them using the PSD2 directive, which is already used in the European Union. In Open Banking we can name a few cyber-security vulnerabilities there are fraudulent API-s transaction, session or authentication attacks, injection attack cause serious problems and require good, not to mention the best, security principles. This project presents the opportunities of informational technologies in picking the right tool and the presence of all known security vulnerabilities cares about trust and provides good partnerships with API consumers. Also, with the help of this directive, we must realize all its advantages and move on rather.*
Key words: *PSD2, trust, retail payments, consumers, security, cyber-attack.*

JEL CLASSIFICATION: G21, D12, E42, G24, G28

ВВЕДЕНИЕ.
С момента своего создания банки сразу же вызывали преступный интерес. И этот интерес был связан не только с хранением средств в кредитных организациях, но и с тем, что важная и зачастую секретная информация была сосредоточена в банках о финансово-хозяйственной деятельности многих людей, компаний, организаций и даже целых государств.
Целью данного исследования является поиск наиболее разумного способа, используя информационные технологии для того, чтобы снизить количество кибератак, вызванные плохой безопаснотью. А так же усиление инноваций, конкуренция и эффективность на рынке с помощью директивы PSD2.

ОСНОВНОЕ СОДЕРЖАНИЕ. Чтобы ответить более подробно на этот вопрос, нужно хорошо изучить данную проблему. Статистика показывает, как в ближайшие пять лет экономическая стоимость в результате кибератак в мире будет составлять 5.2 триллионов долларов США.
Анализ литературных источников
В источнике [1] говорится что согласно опросу 571 сообществ банков в 37 штатах, проведенному Конференцией наблюдателей государственных банков, более 70% респондентов оценили кибербезопасность как свою главную проблему. И то что с каждым годом объем нарушений продолжает расти, согласно исследованию Accenture «Стоимость исследования киберпреступности в финансовых услугах: 2019 год», среднее число нарушений выросло на 13% до 152 в 2018 году с 134 в 2017 году.
Кибератаки пагубно повлияли на многие компании, так что они требуют большего внимания «В последние несколько лет все больше организованных и специализированных групп грабят эти финансовые учреждения с помощью вредоносных программ». Банки подвержены атакам «массового рынка», как и любая другая организация [2].
Конечно, банковский сектор является одной из отраслей, которые подвергаются наибольшему риску, учитывая характер данных, которые они хранят. Это означает, что банкам пришлось выделять значительные средства на развитие своей цифровой инфраструктуры для усиления своей кибербезопасности
Какие же технологии мы можем использовать,чтобы иметь отличную кибер безопастность, а так же улучшенную финансовую экосистему и инфраструктуру для банков, финансовых

компаний и предприятий, использующих данные о платежах в интересах потребителей? В ходе иследования, я наткнулся на регламентацию PSD2, которое должно было вступить в силу 14 сентября 2019 года однако Европейское банковское управление (ЕБА) предоставило дополнительные потенциальные исключения и установило новый срок 31 декабря 2020 года.

Описание использованного метода исследования.
На данный момент, я работаю над проектом который включает в себя директиву PSD2, о которой я буду говорить более подробно ниже.
Методология, использованная в исследовании, является «прикладным научным исследованием», которое представляет собой оригинальную исследовательскую деятельность для накопления новых знаний, но ориентированную, прежде всего, к конкретной практической цели.

Результаты. Я провел исследование исходя из читаемой литературы и собственного опыта работы с данной директивой.
В частности, PSD2 предусматривает, что поставщики платежных услуг (PSP) должны создать структуру с соответствующими мерами по смягчению и механизмы контроля для управления операционными рисками и рисками безопасности относящиеся к платежным услугам, которые они предоставляют.
PSD2 требует, чтобы все банки в Европейском союзе открывали свои API публично(Open API).
В PISP клиенты имеют возможность осуществлять прямые платежи со своих банковских счетов, а не использовать кредитную или дебетовую карту в качестве посредника. Это означает, что они теряют защиту, которую им предоставляют схемы их карт, поэтому PSD2 обеспечивает защиту, чтобы склонить чашу весов в свою пользу [3].

ВЫВОДЫ
Правила директивы PSD2 скоро изменят финансовую кибербезопасность. Сегодня банки полагаются на прямое взаимодействие с клиентами и самостоятельно принимают решения о том, является ли конкретная транзакция мошеннической или нет. Основной задачей банков является обеспечение безопасной инфраструктуры для TPP.
Отделение финансовой кибербезопасности должно будет осуществлять точный мониторинг транзакций и,возможно,устанавливать новые правила для предотвращения сложных киберпреступлений. Однако правила PSD2 позволяют банкам блокировать промежуточный доступ к данным счета, если банк предоставляет доказательства того, что действия третьих лиц являются мошенническими или несанкционированными.

БИБЛИОГРАФИЯ
1.https://securityboulevard.com/2019/11/10-statistics-that-summarize-the-state-of-cybersecurity-in-financial-services/
2. Cherepanov A, Jean-Ian B (2016) Modern attacks against Russian financial institutions.
3. https://www.globalbankingandfinance.com/psd2-a-regulation-for-all/

Coordonator ştiinţific: CAPAŢINA VALENTINA, dr., conf. univ.,
Academia de Studii Economice a Moldovei,
Republica Moldova, mun. Chişinău, str. Mitropolit Gavriil Bănulescu- Bodoni, 61, MD-2005
e-mail: vcapatina@yahoo.com