УДК 336.7

КИБЕРПРЕСТУПНОСТЬ В БАНКОВСКОЙ СФЕРЕ

Волков А.Н.

к.э.н., доцент

Уральский государственный экономический университет,

Екатеринбург, Россия

Заборовская А.Е.,

к.э.н., доцент

Уральский государственный экономический университет,

Екатеринбург, Россия

Червяков А.В.,

студент

Уральский государственный экономический университет,

Екатеринбург, Россия

Аннотация

В статье рассмотрено понятие «кибербезопасности» и «киберпреступности», а также изучены основные виды кибератак и способы борьбы с ними. Были проанализированы перспективы развития кибербезопасности с помощью искусственного интеллекта, рассмотрены различные типы кибератак, от фишинга и вредоносного ПО до DDoS-атак и SQL-инъекций, каждая из которых представляет серьезную угрозу для финансовых учреждений и их клиентов. Учитывая постоянно развивающийся ландшафт киберпреступности, авторы делают вывод о том, что банки должны принимать комплексный подход к безопасности, сочетающий технические решения, организационные меры и обучение персонала. Целью исследования является изучение основных понятий в банковской сфере кибербезопасности, видов кибератак и рассмотрение перспектив развития безопасности банковского сектора.

Ключевые слова: кибербезопасность, банк, фишинг, информационные технологии, кибератака

CYBER CRIME IN BANKING INDUSTRY

Volkov A.N.,
PhD, Associate Professor,
Ural State University of Economics,
Ekaterinburg, Russia
Zaborovskaya A.E.,
PhD, Associate Professor,
Ural State University of Economics,
Ekaterinburg, Russia
Cherviakov A.V.,
Student,
Ural State University of Economics,
Ekaterinburg, Russia

Abstract

The article examines the concept of «cybersecurity» and «cybercrime», as well as studies the main types of cyber attacks and ways to combat them. The prospects for the development of cybersecurity with the help of artificial intelligence were analyzed, various types of cyberattacks were considered, from phishing and malware to DDoS attacks and SQL injections, each of which poses a serious threat to financial institutions and their clients. Given the ever-evolving cybercrime landscape, the authors conclude that banks must take a comprehensive approach to security, combining technical solutions, organizational measures and personnel training. The purpose of the article is to study the main concepts in the banking sector of

cybersecurity, types of cyberattacks and consider the prospects for the development of security in the banking sector.
Keywords: cybersecurity, bank, phishing, information technologies, cyber attack

В наше время – время высокоинтеллектуальных решений одной из важнейших конкурентных особенностей в банковском секторе является внедрение инноваций и развитие информационных технологий, но данный процесс обуславливается также появлением новых видов мошенничества. Финансовый сектор традиционно является привлекательным для различного рода мошенников. Киберпреступность набирает обороты с каждым годом, ее масштабы растут с такой же скоростью, что и ежегодные потери кредитных организаций. Сложность борьбы с этим явлением заключается в новизне проблемы и отсутствии практики борьбы с киберпреступностью, а также трудоемкостью в анализе и минимизации рисков. Киберпреступность, обладая высокой степенью латентности, остается одним из главных сдерживающих факторов распространения систем электронного банкинга в кредитно-финансовой сфере. В связи с этим развитие научных подходов к решению данных проблем, несомненно, будет способствовать своевременному принятию эффективных защитных мер, обеспечивающих безопасность работы в киберпространстве. Появление таких исследований – это очередной шаг к детальному изучению всех особенностей предоставления как банковских, так и в целом финансовых услуг в киберпространстве [1, с. 56].

Понятие кибербезопасности и киберпреступности является относительно молодым, поэтому не имеет общепринятого определения.

Конвенция Совета Европы «О преступности в киберпространстве» определяет киберпреступления, как действия, совершаемые против конфиденциальности, целостности, а также доступности компьютерных систем,

сетей и информации, и злоупотребления данными системами, сетями и данными в преступных целях.

Ховард Р. использует термин «кибербезопасность» в качестве всеобъемлющего обозначения работы, которую выполняют специалисты-практики. За прошедшие годы в сообществе появилось множество синонимов, имеющих то же значение. Вот лишь некоторые из них:

1. цифровая безопасность;
2. безопасность информационных технологий (ИТ);
3. ИТ-безопасность;
4. информационная безопасность (InfoSec).

Все они обозначают одно и то же, поэтому используются как взаимозаменяемые [2, с. 32].

Самыми основными угрозами кибербезопасности являются: фишинговые атаки; вредоносное ПО (Malware): вирусы, трояны, вымогатели (ransomware); атаки на сети: DDoS-атаки, SQL-инъекции, атаки на межсетевые экраны (firewall); мобильные угрозы: безопасность мобильных банковских приложений и т.п.

Таким образом, можно провести условную классификацию методов совершения киберпреступлений.

Фишинг - это тип киберпреступления, который использует социальную инженерию для обмана людей с целью получения конфиденциальной информации, такой, как пароли, номера кредитных карт, данные банковских счетов и личные данные. В банковской сфере фишинг представляет особую опасность из-за потенциальных финансовых потерь как для клиентов, так и для самих банков.

Фишинговые атаки обычно осуществляются, к примеру, через электронную почту: злоумышленники рассылают электронные письма, которые выглядят как сообщения от легитимных организаций (банков, платежных

систем, сервисов онлайн-банкинга). Письма часто содержат ссылки на поддельные веб-сайты, которые имитируют настоящие сайты банков. Они могут требовать обновления информации об аккаунте, подтверждения транзакций или предупреждать о подозрительной активности.

Также распространен смс-фишинг. Аналогично электронной почте, злоумышленники отправляют текстовые сообщения, содержащие вредоносные ссылки или просьбы ввести конфиденциальную информацию.

И самый классический вид фишинговых атак - это звонки. Злоумышленники могут звонить жертвам, представляясь сотрудниками банка, и выманивать конфиденциальную информацию под разными предлогами.

Комплексный подход, сочетающий технические и организационные меры, является наиболее эффективным способом защиты банковской сферы от фишинговых атак. Постоянное обновление защитных мер и обучение персонала являются ключом к успешной борьбе с этим видом киберпреступности.

Вредоносное ПО (Malware) представляет собой серьезную угрозу для банковской сферы, способную нанести значительный финансовый ущерб и нарушить работу банковских систем. Наиболее распространенные типы Malware в финансовой сфере это:

- вирусы;
- трояны;
- вымогатели.

Вирусы - это программы, которые могут самовоспроизводиться и распространяться, заражая другие файлы и системы. В банковской сфере вирусы могут уничтожать данные, заражая файлы баз данных, финансовые отчеты, клиентскую информацию, вирусы могут привести к значительным потерям данных. Могут нарушать работу систем, так как заражение серверов или рабочих станций может привести к сбоям в работе банковских систем, что может парализовать операции и привести к финансовым потерям. Некоторые

вирусы создают «черные входы» в системе, позволяющие злоумышленникам получить доступ к системе в будущем.

Трояны - это вредоносные программы, маскирующиеся под полезные приложения. В банковской сфере трояны могут красть конфиденциальную информацию. Они могут регистрировать нажатия клавиш (keylogger), воровать данные учетных записей, номера кредитных карт и другую конфиденциальную информацию. Могут управлять системой удаленно, злоумышленники могут использовать троян для удаленного управления зараженным компьютером, позволяя им манипулировать банковскими операциями или красть деньги. Также могут создавать ботнеты. Трояны могут превратить зараженный компьютер в часть ботнета - сети зараженных компьютеров, используемых для проведения DDoS-атак или рассылки спама.

Вымогатели - это вид вредоносного ПО, который шифрует файлы на компьютере жертвы и требует выкуп за их расшифровку. В банковской сфере ransomware может зашифровать критически важные данные: данные клиентов, финансовые отчеты, базы данных, что приведет к остановке работы банка и значительным финансовым потерям. Могут угрожать раскрытием конфиденциальной информации, если выкуп не будет уплачен, и, соответственно, требовать значительные суммы выкупа, которые могут быть огромными, особенно если речь идет о крупных банках.

Защита от Malware требует комплексного подхода, включающего:

1. Антивирусное ПО. Использование надежного антивирусного программного обеспечения с регулярным обновлением баз данных.

2. Многофакторная аутентификация (MFA). Защита от несанкционированного доступа к учетным записям.

3. Системы обнаружения вторжений (IDS/IPS). Мониторинг сетевого трафика на предмет подозрительной активности.

4. Регулярное резервное копирование данных. Регулярное создание резервных копий данных, хранящихся в безопасном, изолированном месте.

5. Обучение персонала. Обучение сотрудников безопасному использованию компьютерных систем и распознаванию фишинговых атак.

6. Политика безопасности информации. Разработка и внедрение четкой политики безопасности информации в банке.

7. Сегментация сети. Разделение сети на изолированные сегменты для ограничения распространения Malware.

Постоянное обновление защитных мер и обучение персонала являются ключом к успешной защите банковских систем от вредоносного ПО. Внедрение современных технологий безопасности, таких как системы машинного обучения для обнаружения угроз, также играет ключевую роль в укреплении кибербезопасности банков.

Атаки на сетевую инфраструктуру банков представляют собой серьезную угрозу, способную привести к финансовым потерям, нарушению работы банковских систем и ущербу репутации. Рассмотрим наиболее распространенные типы таких атак:

DDoS-атака - это попытка сделать недоступным веб-сайт или онлайн-сервис, перегрузив его большим количеством запросов с множества источников (ботнета). В банковской сфере DDoS-атака может вывести из строя онлайн-банкинг, то есть клиенты не смогут получить доступ к своим счетам, совершать платежи или управлять финансами, прервать работу платежных систем. Это может привести к задержкам платежей, сбоям в обработке транзакций и финансовым потерям, нарушить работу внутренних систем банка. Атака может затронуть не только внешние сервисы, но и внутренние системы банка, что приведет к полной остановке работы на неопределенное время.

SQL-инъекция - это методика взлома, использующая уязвимости в веб-приложениях, для выполнения вредоносных SQL-запросов к базе данных. В

банковской сфере SQL-инъекции могут получить доступ к конфиденциальным данным. Злоумышленники могут получить доступ к данным клиентов, финансовым отчетам и другой конфиденциальной информации, хранящейся в базе данных. Также они могут изменять данные в базе данных, например, переводить деньги на чужие счета.

Межсетевой экран (Firewall) - это устройство или программное обеспечение, которое контролирует и фильтрует сетевой трафик, предотвращая несанкционированный доступ к сети. Атаки на Firewall могут быть направлены на обход Firewall, то есть злоумышленники пытаются найти уязвимости в Firewall, чтобы обойти его защиту. DoS-атаки на Firewall, перегрузка Firewall большим количеством запросов, чтобы вывести его из строя, взлом настроек Firewall, изменение настроек Firewall для получения несанкционированного доступа.

Комплексная защита от атак на сеть требует постоянного мониторинга, анализа угроз и внедрения многоуровневой системы безопасности, включающей как аппаратные, так и программные средства защиты. Регулярное обновление программного обеспечения и обучение персонала также являются крайне важными аспектами обеспечения безопасности.

Если рассматривать перспективы развития кибербезопасности в банковской сфере, то стоит уделить внимание искусственному интеллекту (ИИ).

Искусственный интеллект играет все более важную роль в повышении уровня кибербезопасности банковской сферы. Его применение позволяет автоматизировать многие процессы, обрабатывать огромные объемы данных и выявлять угрозы, которые невозможно обнаружить традиционными методами.

Направления использования искусственного интеллекта в сфере кибербезопасности (рис. 1) разнообразны.

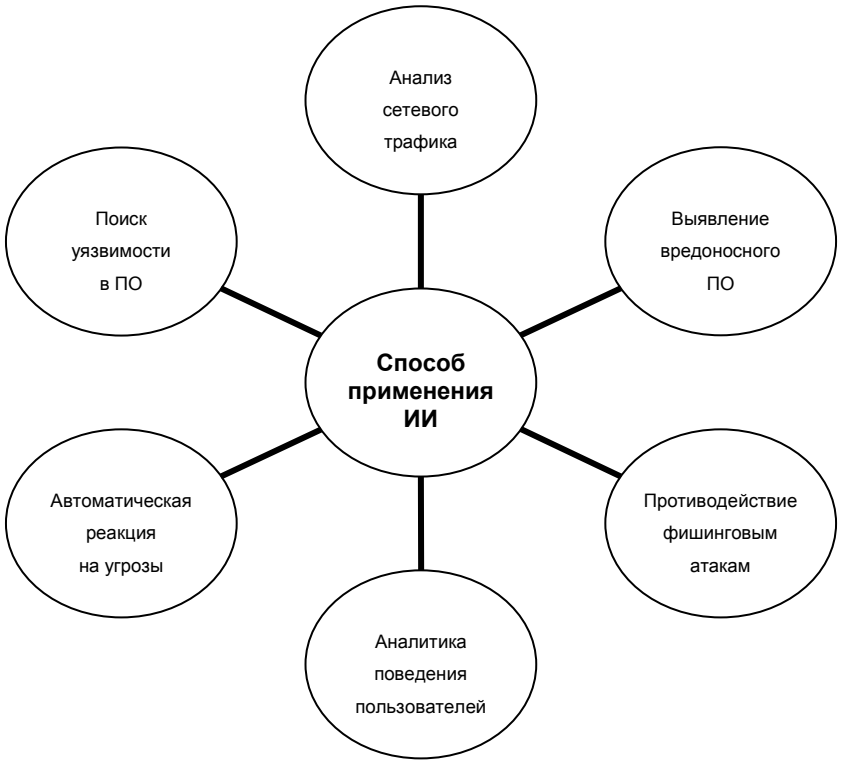

Рис. 1 - Использование искусственного интеллекта в сфере кибербезопасности[1]

ИИ-системы могут анализировать огромные объемы сетевого трафика в режиме реального времени, выявляя аномалии и подозрительную активность, которые могут указывать на кибератаки. Это позволяет быстрее реагировать на угрозы и предотвращать их распространение. ИИ способен анализировать характеристики файлов и коды для идентификации вредоносного ПО, даже неизвестных образцов (zero-day exploits). Это особенно важно, так как традиционные антивирусные программы часто не могут обнаружить новые угрозы. ИИ-алгоритмы способны анализировать текст электронных писем, веб-сайтов и других источников, выявляя признаки фишинга, такие как подозрительные ссылки, грамматические ошибки и несоответствия в дизайне.

[1] Составлен авторами

ИИ может анализировать поведение пользователей в банковской системе, выявляя отклонения от обычных шаблонов, которые могут сигнализировать о мошеннических действиях.

ИИ-системы могут автоматически блокировать подозрительные запросы, вредоносный трафик и вредоносные файлы, минимизируя время реакции на угрозы. ИИ может ускорить процесс расследования кибератак, анализируя большие объемы данных и предоставляя информацию для быстрого принятия решений.

ИИ используется для улучшения точности биометрической аутентификации, повышая безопасность доступа к мобильным банковским приложениям, может анализировать данные о транзакциях, выявляя подозрительные операции и предотвращая мошенничество.

ИИ помогает выявлять уязвимости в программном обеспечении, которое используется в банковской сфере. На основе анализа данных о кибератаках ИИ помогает в разработке более эффективных методов защиты и алгоритмов шифрования.

Однако, использование ИИ в кибербезопасности также имеет свои ограничения:

- зависимость от качества данных: эффективность ИИ зависит от качества и количества данных, используемых для обучения моделей;

- возможность обмана: злоумышленники могут попытаться обмануть ИИ-системы, используя методы обфускации или создавая новые типы атак, на которые технология не настроена;

- стоимость внедрения и обслуживания: внедрение и обслуживание ИИ-систем может быть дорогостоящим.

Несмотря на эти ограничения, технология ИИ является мощным инструментом в борьбе с киберпреступностью в банковской сфере. Дальнейшее развитие и совершенствование ИИ-технологий обещает значительно повысить

уровень защиты банковских систем и снизить риски кибератак. Комбинирование ИИ с другими методами кибербезопасности, такими как многофакторная аутентификация и обучение персонала, позволит создать наиболее надежную и эффективную систему защиты.

Кибербезопасность в банковской сфере является критическим аспектом, требующим постоянного внимания и инвестиций. Особого внимания при этом в сфере реализации кибербезопасности заслуживают перспективы использования искусственного интеллекта. ИИ предлагает революционные возможности для обнаружения и предотвращения угроз, автоматизации процессов реагирования на инциденты и повышения общей устойчивости банковских систем. Однако, важно помнить, что ИИ не является панацеей, и его эффективное внедрение требует тщательного планирования, инвестиций в инфраструктуру и постоянного обучения специалистов. Успешная киберзащита банковской сферы будет зависеть от способности финансовых учреждений адаптироваться к новым угрозам, использовать передовые технологии, такие как ИИ, и поддерживать тесное сотрудничество между собой и с регулирующими органами.

Данный процесс находится в постоянном развитии, поскольку связан с особенностями рефлексии «второго порядка». То есть, каждый дополнительный метод защиты от киберпреступников вызывает ответную реакцию в виде изобретения дополнительных способов обмана. «Гонка вооружений» в этом случае должна быть на стороне закона и защиты интересов клиентов и вкладчиков, поэтому ресурсы, выделяемые на проведение мероприятий по кибербезопасности, должны быть сопоставимы со степенью угрозы. Только комплексный и постоянно обновляемый подход может обеспечить необходимый уровень защиты в условиях постоянно эволюционирующего мира киберпреступности.

Библиографический список:

1. Кибербезопасность в условиях электронного банкинга: практическое пособие / А. А. Бердюгин, А. Б. Дудка, С. В. Конявская [и др.]; под редакцией П. В. Ревенкова. — Москва: Прометей, 2020. — 522 с.

2. Ховард Р. Кибербезопасность: главные принципы — СПб.: Питер, 2024. — 320 с.: ил. - (Серия «Библиотека программиста»).ISBN 978-5-4461-2201-1

Оригинальность 79%