Сегодня информация играет ключевую роль в любой деятельности. Технологии современности предоставляют много возможностей: простоту обработки, быстроту передачи адресатам и гибкость манипуляции. Информационный прогресс приводит к замене ручной деятельности человека, что способствует зависимости общества от компьютеров. Процесс использования новейших технологий в работе организаций получил название "автоматизация".

Комьютерные техгологии заметно упростили совершение преступлений, к которым относятся кража, мошенничество, шпионаж, клевета. С развитием компьютерных технологий стали возникать новые виды преступлений: фишинг, распространение вредоносных программ, хищение компьютерной информации, спам, DoS-атаки. В связи с этим киберпреступность является межгосударственной серьезной проблемой.

Многие ученый нашей страны уделяли внимание вопросам кибербезопасности. Так, Д.А. Тершуков обосновал необходимость информационной безопасности как составной части национальной безопасности страны. Проблемы информационной безопасности исследовались в научных трудах Е. А. Муньковой, А. В. Шободоевой.

Отдельные аспекты развития и становления информационных отношений, вопросы осуществления противодействия киберпреступности рассматривались ведущими отечественными учеными Т. А. Гончаровой, Л. В. Набоковым, Н. А. Казаковой, А. А. Петюковой, Б. А. Тарчоковым. Однако указанные исследования в основном сосредоточены на теоретических аспектах киберпреступности. Впрочем беспокойство, связанное с масштабами и влиянием пандемии COVID-19, заставляет предприятия анализировать текущую ситуацию и разрабатывать меры, которые следует принять для защиты информации.

Целью исследования является анализ тенденций развития киберпреступности и построение оптимистичного и пессимистичного прогнозов. Были использованы методы скользящей средней для прогнозирования; методы математической статистики; методы общей теории статистики, а именно относительных, абсолютных и средних величин, методы синтеза и анализа. Были применены графический и табличный методы визуализации данных.

Проведем анализ сведений о преступлениях, которые были совершены с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации в России.

Анализируя данные за период с 2022 по 2024 гг., можно отметить устойчивый рост числа преступлений, совершённых с использованием информационно-коммуникационных технологий. Так, в 2023 году количество преступлений с использованием сети Интернет выросло на 38,2%, а в 2024 году — ещё на 26,1% по сравнению с аналогичными периодами предыдущих лет. Преступления, связанные со средствами мобильной связи, увеличились на 42,2% в 2023 году и на 19,6% в 2024 году.

Наибольшую динамику продемонстрировали мошенничества и кражи с использованием ИКТ, составившие до 71% всех киберпреступлений. Рост мошенничеств с электронными платежами и банковскими картами составил 28,1% в 2023 году и 4,5% в 2024 году. Одновременно наблюдается увеличение числа преступлений, связанных с хищением данных, незаконным доступом к компьютерной информации и распространением фишинговых атак.

Отрицательный прирост зафиксирован по некоторым категориям преступлений, таким как использование вредоносных программ (снижение на 41% в 2022 году с последующей стабилизацией показателей в 2023 году). Также снизилось число преступлений, связанных с организациями азартных игр и кибертеррористической деятельностью.

Несмотря на высокие темпы роста ключевых категорий киберпреступлений, их распределение остаётся относительно стабильным, при этом совокупное влияние таких статей, как фиктивные электронные платежи, создание и распространение вредоносных программ, а также террористическая активность, не оказывает значительного влияния на общую структуру киберпреступности.

На основе данных лаборатории Касперского был проведен анализ развития угроз в сфере информационных систем по всему миру за период I квартал 2023 — III квартал 2024.

За исследуемый период сократилось количество мобильных угроз на 28%, мобильных банковских троянцев на 69%, возросло количествомобильных троянцев-вымогателей на 57%, уменьшилось на 32% количество новых модификаций шифровальщиков (таблица).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Квартал | Мобильные угрозы | Мобильные банковские троянцы | Мобильные троянцы-вымогатели | Новые модификации шифровальщиков |
| Q1 2023 | 307529 | 57601 | 1767 | 3089 |
| Q2 2023 | 370327 | 59167 | 1318 | 1917 |
| Q3 2023 | 438962 | 21674 | 1855 | 11387 |
| Q4 2023 | 246802 | 14169 | 6125 | 6105 |
| Q1 2024 | 389178 | 11729 | 1990 | 7070 |
| Q2 2024 | 376418 | 13019 | 2611 | 4456 |
| Q3 2024 | 222444 | 17822 | 2779.8 | 2109 |
| Темп роста Q3 2024 к Q1 2023, % | 72 | 31 | 157 | 68 |

На основе данных лаборатории Касперского за заданные кварталы нами были построены прогнозы следующих угроз: мобильных угроз, мобильных банковских троянцев, мобильных троянцев-вымогателей, новых модификаций шифровальщиков.

При этом на протяжении четырех лет — с 2019 г. по 2023 г. — наблюдается рост количества новых зарегестрированных CVE.

По данным Kasperky Secure Network, после предоставления компанией OpenAI публичного доступа к GPT-3 в конце 2022 года, злоумышленники использовали её для создания персонализированных убедительных писем для целевого фишинга. К тому же, данная языковая модель использовалась для генерации последующих реплик после получения ответа от получателя фишингового сообщения. Была обнаружена вредоносная компания, которая эксплуатировала приобретающую популярность ChatGPT, которая заключалась в предоставлении фальшивых данных для доступа к платной версии языковой модели с правдоподобной ссылкой на скачивание поддельной версии ChatGPT для Windows. По ссылке на устройство загружался троянец, который воровал учетные данные из многих популярных браузеров.

Были обнаружены в магазине Google Play вредоносные приложения, которые маскируются под модифицированные версии Telegram на уйгурском, традиционном и упрощённом китайском языках. Описания для данных приложений содержали схожие иллюстрации приложения с офицальной страницы Telegram в магазине. В коде приложений был обнаружен шпионский модуль, задачей которого являлась постоянная слежка за работой приложения и отправка данных на сервер злоумышленников: контакты, сообщения, названия чатов, имя и телефон учетной записи.

В рассылке от Openwall Oopen Source Security было заявлено об обнаружении бэкдора в XZ, которая встроена во многие популярные дистрибутивы Linux. Для доступа к функциям systemd на таких дистрибутивах, как Debian, Ubuntu и Fedora, использовался модифицированный OpenSSH, который зависил от этой библиотеки. Вредоносный код был внедрён в феврале и марте 2024 года. Полагается, что целью атаки являлось в добавление sshd возможности удаленного выполнения кода