ФБК

Аудит | Консалтинг | Право

# Информационная безопасность в современных реалиях: что ожидать и что делать

**Курило Андрей Петрович,**

Советник по информационной безопасности ФБК и ФБК CS, КТН, доцент

# План выступления

1. Реалии, наступившие после 24 февраля. Характеристика. Что было, что стало, что ожидать. Как изменилась модель нарушителя и его цели.

2. Состояние системы в целом, характеристика последствий.

3. Выводы о готовности системы в целом, самые грубые нарушения.

4. Реакция наших регуляторов, нормативные требования, законодательство по направлениям.

5. Что делать, к чему и как готовиться.

# Общая характеристика

- Кибератаки усиливаются одновременно с политическими обострениями.
- Против нашей страны идет война в информационном пространстве, в основном в ней участвуют хакеры из Украины.
- США не вмешиваются, а наблюдают.
- На современном этапе эта война отличается тем, что в ней сейчас применяется не самое разрушительное оружие, скорее традиционный и банальный набор хорошо известных средств.
- Можно считать, что первый пик обострения прошел, сейчас наступает период осмысления с обеих сторон.
- Следующая фаза обострения – начало следующего года

# Основные направления кибератак

- Атаки на отказ в обслуживании (DDoS-атаки).
- Атаки на Web – сервисы.
- Атаки, нацеленные на проникновение в инфраструктуру через: уязвимости в ПО, зараженную почту, ошибки в настройках систем управления доступом.
- Атаки на финансовые средства путем организации мошенничеств с использованием инструментов социальной инженерии.

Дополнительно возникла проблема обеспечения надежного функционирования средств и систем защиты в связи с почти мгновенным уходом с российского рынка зарубежных фирм, отзывом сертификатов и лицензий.

# Как поменялись объекты атак

До этих событий основным приоритетом с точки зрения выбора объекта атаки у хакеров были финансовые организации.

**Сейчас объектами атак являются:**

- Индустриальные объекты
- Объекты критической инфраструктуры
- Объекты критической информационной инфраструктуры
- Системы управления, включая системы госуправления
- IT- компании и поставщики - число атак выросло на 200%
- Сервисы электронного правительства
- Медиаресурсы

# Цели атак

До известных событий основной целью злоумышленников было хищение финансовых средств.

**Новые цели хакеров:**

- нарушение работы государственных, общественных
и финансовых институтов, организаций фирм;
- хищение и уничтожение данных;
- морально-психологическое воздействие на общество.

# Основные векторы атак: DDoS-атаки

1. Резко возросла интенсивность атак (самое простейшее и давно и хорошо известное средство ведения информационных войн)
2. Более 90% наших компаний испытывали затруднения.
3. В целом, это было ожидаемо, недооценили их покрытие и суммарную мощность.
4. Длительность некоторых атак - месяцы.
5. Некоторые российские компании попали под атаки и не справились, что привело к временной утрате их работоспособности и потере сервисов.

В целом, проблема решается при организации взаимодействия с провайдерами.

# Основные векторы атак: Атаки на Web-сервисы

1. Резко увеличилось число таких атак в начальный период.
2. Причины успешных атак – в основном, неправильная конфигурация систем.
3. Разрушительных последствий не было.
4. Атаки легко парировались путем выполнения своевременно выпущенных рекомендаций НКЦКИ.

# Основные векторы атак: Атаки с целью проникновения в инфраструктуру

1. Эксплуатация уязвимостей (поиск и попытки эксплуатации уязвимостей в настройках и архитектуре информационных систем) – 50% всех атак.
2. Задача формальная и хорошо известная в процедуре пентестирования. Эффективность отражения атак этого типа зависит от оперативности обработки уязвимостей и своевременности пентестирования.
3. Атаки через зараженные почтовые отправления (фишинг) - на втором месте по числу атак.
4. Наблюдались факты использования программ-шифровальщиков.

Атаки через почтовые отправления представляются крайне опасными, так как  статистика говорит о том, что пользователи открывают каждое 7-е письмо с неизвестным содержанием. Ожидается рост подобных атак в первой декаде нового 2023 года.

# Основные векторы атак: Атаки с целью проникновения в инфраструктуру

5. Проникновение в систему путем эксплуатации  слабостей в парольной защите и эксплуатации слабых и скомпроментированных аутентификационных данных (слабые пароли, аутентификационные данные уволившихся сотрудников).
6. Как показала практика, это самый простой и самый опасный способ атаки, вызывающий самые тяжелые последствия.
7. Социальная инженерия. Ничем не примечательно и есть осторожные предположения, что пик мошеннических звонков прошел. Однако, на этом фоне растет фрод и фишинг в интернете.
8. Уход фирм, изменение лицензионной политики в целом преодолены, однако риски эксплуатации импортных средств защиты выросли существенно, особенно при реализации сложных схем получения обновлений через третьи лица.

Основная задача в части защиты инфраструктуры - замена импортных продуктов на отечественные, пусть даже путем понижения некоторых характеристик, например, производительности.

# Выводы: (А) Противник

- Цели противника понятны, но не достигнуты, катастрофы не случилось.
- Идет консолидация, обучение и переподготовка сил нападающих.
- Совершенствуется система управления атаками.
- Противник работает вдумчиво, не торопясь.
- Инструменты для атак распространяются бесплатно.
- Технически растет скорость реализации атак, справиться с ними можно только путем использования автоматизированных средств.
- Ожидается  смещение векторов атак на сложные атаки, связанные с проникновением в систему путем применения зараженной почты (включая фрод) и эксплуатации уязвимостей с последующим нанесением неприемлемого ущерба.

# Выводы: (Б) Российская инфраструктура

- Можно сказать, что наша система безопасности в целом справилась с кибератаками.
- Достигнутые результаты, отчасти, обусловлены низкой квалификацией атакующих. Если уровень подготовки атакующих будет выше, ситуация может измениться.
- Кредитно-финансовая сфера оказалась в лучшем положении.
- Кто инвестировал в безопасность, оказался в лучшем положении.
- Крайне опасны атаки на АСУ ТП. Лучший способ защиты на данный момент – полная физическая изоляция (воздушный зазор).
- Явные проблемы отзыва лицензий пока преодолены.
- Существенно повлияли в положительную сторону указы Президента №166 и №250.
- Заметно улучшили работу регуляторы.

# Оценка российских организаций по результатам проверок

## Результаты проверок ФСТЭК (выборка 500 организаций):

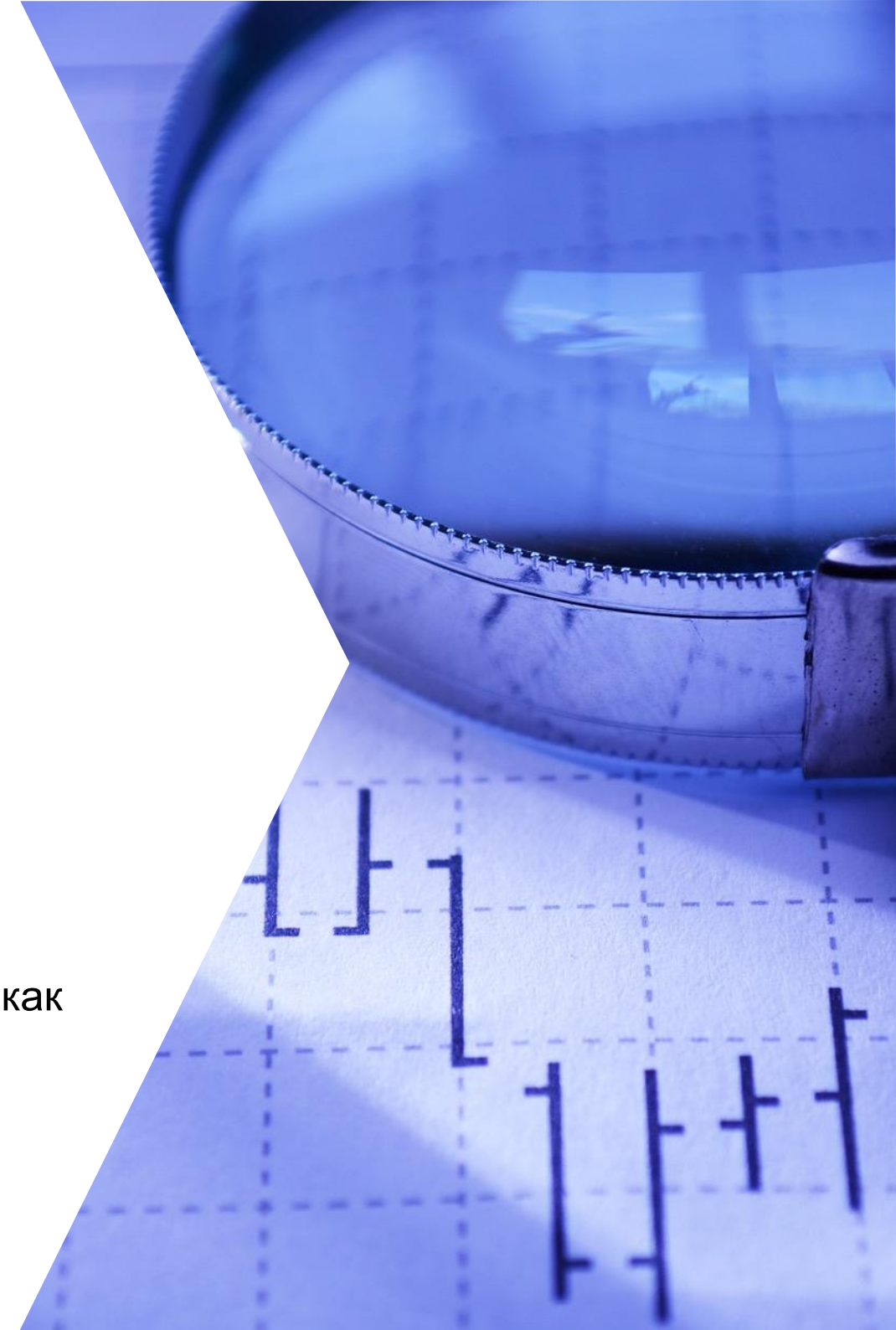
- В 40% организаций не выполнены элементарные требования по безопасности в части устранения слабых паролей.
- В 34% организаций не проведены проверки периметра, есть слабости.
- В 50% организаций не выполняются меры безопасности при работе в с подрядчиками.

## Результаты проверок Positive Technologies показывают:

- В ходе пентестов 96% организаций оказались не защищены от проникновения в локальную сеть; во всех этих организациях был получен полный контроль над инфраструктурой.
- В среднем для проникновения во внутреннюю сеть компании злоумышленнику могло бы потребоваться пять дней и четыре часа.
- В 85% проверенных организаций были выявлены критически опасные уязвимости и уязвимости высокой степени опасности, связанные с недостатками парольной политики.
- В 60% компаний обнаружены уязвимости критического и высокого уровня опасности, связанные с использованием устаревших версий ПО.

# Главные замечания по результатам проверок

1. Не устраняются уязвимости, в том числе и старые и хорошо известные.
2. Установлены слабые пароли.
3. Ошибки в настройках систем защиты и оборудования ИС.
4. Не устанавливаются рекомендованные обновления.
5. Фактическое состояние ЗО КИИ, не соответствует заявленному в учетных материалах.
6. Плохо хранятся резервные копии ПО, их как правило невозможно развернуть.



## Основные выводы

**1.** Процесс управления ИБ в стране плохо организован.

**2.** Необходимо вводить методический подход, опирающийся на построение системы безопасности с опорой на выявление группы «неприемлемых» событий безопасности с организацией защиты от них в первую очередь.

**3.** Растет роль процедуры оперативного управления безопасностью, реализуемой через мониторинг событий и инцидентов безопасности и создание центров оперативного управления безопасностью.

# Позиция регуляторов

- Усиление контроля и требований к ИБ организаций.
- Рост роли НКЦКИ.
- Реализация Указа №166.
- Реализация Указа №250.
- Изменения в ФЗ о ПДн в части усиления контроля за оборотом ПДн.
- Проект ФЗ об оборотных штрафах за утечки ПДн.
- Изменение классификации ЗО КИИ: к ним будет относится большее число объектов.
- Усиление административной ответственности за невыполнение требований по информационной безопасности и непредставление информации в НКЦКИ.

# Что нужно делать организациям

- Помнить, что обеспечение информационной безопасности - это работа не для государства или регулятора, а для самого себя.
- Выполнить все требования нормативной базы – аудит, оценка соответствия, анализ защищенности и др. контрольные мероприятия.
- В первую очередь – проверить пароли, политику управления доступом, установку актуальных обновлений.
- Срочно провести тестирование на проникновение, делать это регулярно.
- Подготовиться и провести киберучения.

ФБК

Аудит | Консалтинг | Право

# Спасибо за внимание!

ул. Мясницкая, 44/1,
Москва, Россия 101990

T: (495) 737 5353
Ф: (495) 737 5347
E: fbk@fbk.ru

**fbk.ru**

**fbk-pravo.ru**