Системы
Информационной
Безопасности

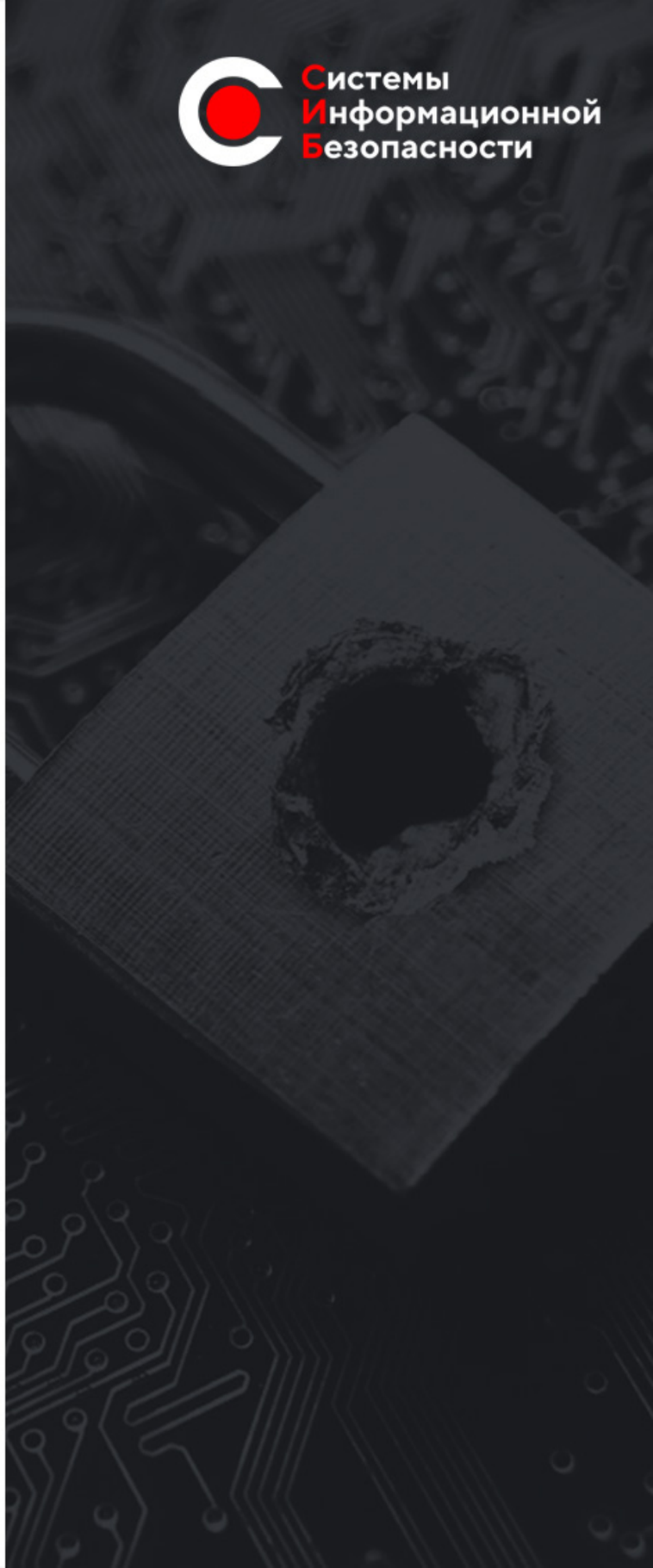
Infrastructure protection:

защита ИТ-инфраструктуры

Защита ИТ-инфраструктуры

Основная задача любой компании, располагающей собственной ИТ-инфраструктурой – обеспечить необходимый уровень ее защищенности. Это важнейшая часть системы обеспечения информационной безопасности организации, позволяющая минимизировать широкий спектр внешних угроз и рисков.

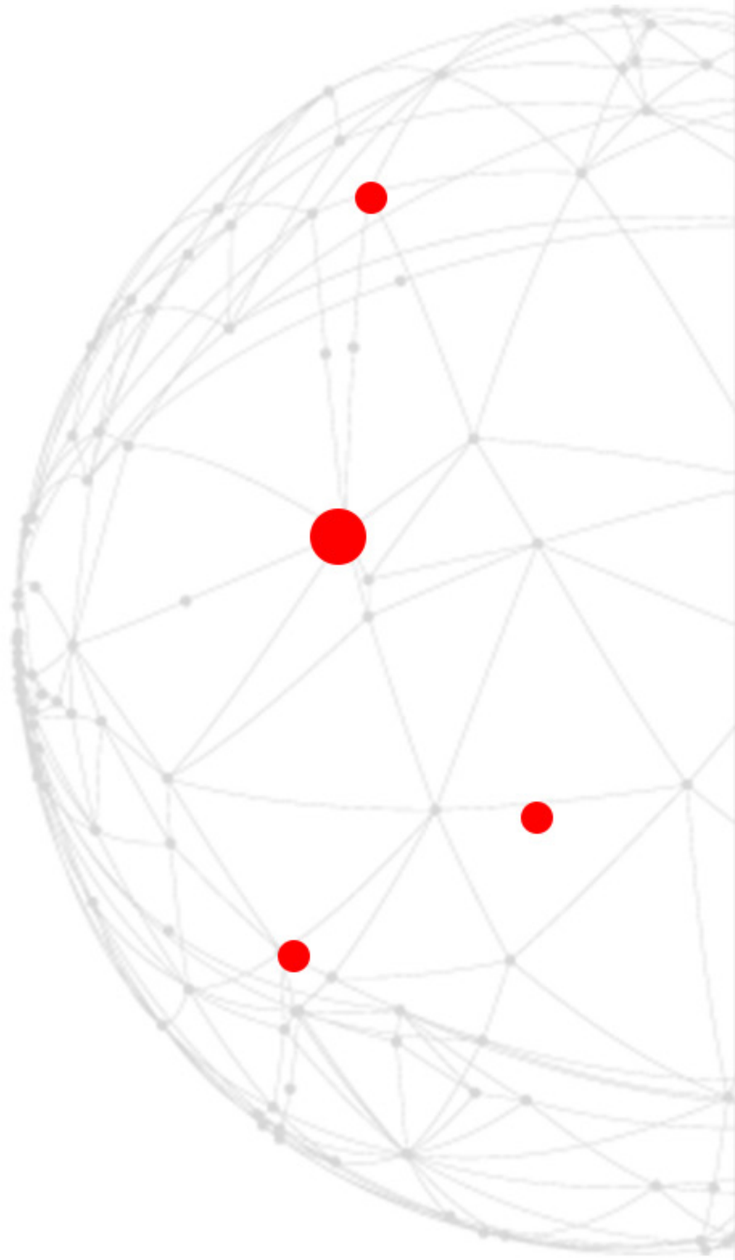
Большинство хакерских атак на корпоративный сектор становятся возможными из-за недостаточной защищенности сетевого периметра организаций, использования небезопасных средств удаленного доступа к корпоративным сетям, несвоевременно установленным обновлениям серверного ПО, применения малоэффективных средств сетевого мониторинга или уязвимостям в применяемых политиках безопасности корпоративной сети.



Системы
Информационной
Безопасности

Атаки на инфраструктуру компаний статистика

- В 2019 году 31% организаций в мире сталкивались с тем или иным видом кибератак, направленных на свою инфраструктуру*
- Среднее время обнаружения успешной целевой атаки на инфраструктуру составляет 98 дней для финансовых организаций и 197 дней для остальных компаний в мире.**
- Средний ущерб от кибератаки в мире составляет 5 000 000 $***



Личный опыт

В нашей практике мы сталкивались со случаями, когда инфраструктура компании подверглась активной атаке спустя год после факта взлома.

*По данным Cisco Cybersecurity Reports
** По данным исследования компании Zdnet
*** По данным исследования Ponemon Institute

Системы
Информационной
Безопасности

Атаки на инфраструктуру компаний основные причины

Большинство хакерских атак на корпоративный сектор становятся возможными из-за:

- недостаточной защищенности сетевого периметра организаций;
- использования небезопасных средств удаленного доступа к корпоративным сетям;
- несвоевременно установленным обновлениям серверного ПО;
- применения малоэффективных средств сетевого мониторинга;
- уязвимости в применяемых политиках безопасности корпоративной сети;
- недостаточных или отсутствующих процессов обеспечения информационной безопасности

Атаки на инфраструктуру
-почему опасно

Системы Информационной Безопасности

В случае успешного осуществления кибератаки основными целями атакующих чаще всего являются:

- распространение вирусов-шифровальщиков с последующим вымогательством.

- кража персональных данных для перепродажи на черном рынке.

- вывод финансовых средств через рабочие места, оборудованные системами ДБО.

Системы
Информационной
Безопасности

Защита ИТ-инфраструктуры

-наше решение

- Найдем все слабые места в процессах и инфраструктуре.
- Подготовим набор рекомендаций по улучшению и оценку текущих средств ИБ.
- Составим дорожную карту улучшений текущего состояния.
- Поможем реализовать каждый из этапов дорожной карты.
- Приведем в соответствие к лучшим мировым практикам по защите инфраструктуры.

Системы
Информационной
Безопасности

Наше решение
-что дает?

- Актуальную оценку текущего уровня защищенности вашей сети, инфраструктуры, критичные и уязвимые элементы в ней, возможные векторы атак.

- Надежную и отказоустойчивую платформу для ваших сервисов.

- Повышение операционной эффективности за счет удобного и безопасного удаленного доступа ваших сотрудников к рабочему.

- Возможность оценить состояние и защищенность вашей инфраструктуры в любой момент времени.

- Выполнение требований государственных регуляторов и надзорных органов.

Системы
Информационной
Безопасности

Наше решение

-как начать?

Подписать NDA.

Заполнить опросный лист.

Прислать указанные документы нам на почту.

Системы
Информационной
Безопасности

Как с нами связаться?

+7 495 766-05-38
info@is-systems.org