Используемые понятия

SEARCHINFORM
INFORMATION SECURITY

- **Информация** – сведения (сообщения, данные) независимо от формы их предоставления.
- **Информационная система** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.
- **Информационная безопасность (ИБ)** применительно к отдельной информационной системе – состояние информационной системы, при котором она наименее восприимчива к вмешательству и нанесению ущерба со стороны третьих лиц.
- **Автоматизированная система управления технологическими процессами (АСУ ТП)** — совокупность аппаратно-программных средств, которые осуществляют контроль и управление производственными и технологическими процессами, поддерживают обратную связь, воздействуют на ход процесса при отклонении его от заданных параметров, а также обеспечивают регулирование и оптимизацию управляемого процесса.

Почему это вас касается?

SEARCHINFORM
INFORMATION SECURITY

1 Органы власти, учреждения и предприятия, которым принадлежат информационные системы, сети, АСУ, функционирующие в сферах топливно-энергетического комплекса, атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, науки и энергетики, являются субъектами КИИ (п. 8 ст. 2 ФЗ от 26.07.2017 № 187-ФЗ). Требования по защите распространяются на все информационные системы этих субъектов.[1]

2 Руководителям предприятий – субъектов КИИ, системообразующих предприятий российской экономики, стратегических акционерных обществ, государственных корпораций и компаний предписано принимать дополнительные организационные меры к защите информационной инфраструктуры под личную ответственность. Также субъекты КИИ не смогут использовать средства защиты информации из недружественных стран с 2025 г. (Указ Президента РФ от 01.05.2022 № 250).

3 Госзаказчикам запрещено закупать иностранное ПО для использования на объектах КИИ с 31 марта 2022 г. и использовать такое ПО с 1 января 2025 г. (Указ Президента РФ от 30.03.2022 № 166)

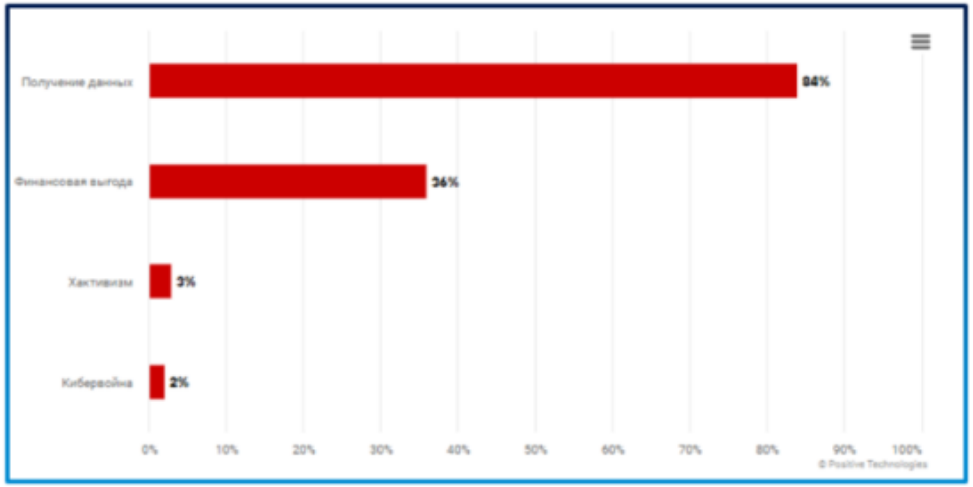
1. https://lukatsky.ru/aiovg_videos/dialog-s-fstek-rossii-vitaliy-lyutikov-otvechaet-na-voprosy-spetsialistov-ib-17-02-2021-bis-tv

Давайте разбираться

SEARCHINFORM
INFORMATION SECURITY

Зачем вас атаковать?

В 2020-2021 годах основные мотивы злоумышленников – личная выгода и шпионаж.



90% российских компаний подверглись кибератакам в 2021 году.

20% из них понесли финансовый ущерб.

В мире:

- Май 2021 – ЧС в 17 штатах США, турбулентность на нефтяных рынках из-за успешной кибератаки на трубопровод Colonial Pipeline.
- Июнь 2021 – приостановка деятельности крупнейшего мирового поставщика мяса JBS Foods. Злоумышленникам выплачено 11 млн долларов выкупа. В магазинах по всему миру выросли цены на мясо.

2022 год: кибервойна

SEARCHINFORM
INFORMATION SECURITY

В новой реальности хактивизм — основная мотивация.

В 2022 году зафиксированы масштабные атаки злоумышленников на российские предприятия различного размера и сферы деятельности: от атомных электростанций и ОПК до пищевых производств. [1,2,3]

Эксперты информационной безопасности сошлись во мнениях о том, что теперь информационным угрозам подвержены информационные системы любых российских организаций.[4]

Чего хотят злоумышленники

1. Дефейс;
2. Шумиха;
3. Порча и уничтожение данных;
4. Хищение данных;
5. Материальная выгода.

1. https://www.gazeta.ru/science/news/2022/07/19/18157748.shtml?updated
2. https://newizv.ru/news/tech/04-04-2022/kiberataki-na-produktovyy-sektor-rossii-idut-so-storony-ukrainskih-hakerov
3. https://xakep.ru/2022/08/09/ta-428-attacks/
4. Конференция «ЦИПР-2022». Экспертная сессия. От защиты персональных данных до критической инфраструктуры https://www.youtube.com/watch?v=FQepFPjU0AY

Из 2022 в 2023

SEARCHINFORM
INFORMATION SECURITY

Синергия хактивизма и выгоды, атаки на импортозамещенное ПО

С марта 2023 года активна украинская группировка вымогателей Shadow. Злоумышленники атакуют российские промышленные предприятия и используют специальное ПО для проникновения в Linux-инфраструктуру.[1]

Россия заняла первое место в мире по увеличению числа вредоносных объектов в АСУ ТП и на третье – по количеству.

Самая частая угроза в российских АСУ ТП – фишинг.[2]

Прогноз экспертов:

на 70%	вырастет число утечек информации
на 40%	вырастет число внешних кибератак
на 15%	вырастет число фишинговых атак

1. https://news.ru/russia/rossijskie-promyshlennye-kompanii-atakovala-ten/
2. https://xakep.ru/2023/03/07/scada-stats/

Выполняем требования регуляторов

SEARCHINFORM
INFORMATION SECURITY

Статья 7 ФЗ «О безопасности критической информационной инфраструктуры РФ». ПП РФ от 20.12.2022 № 2360.	Обязательное категорирование объекта КИИ. Необходимость повторного категорирования и актуализации данных об объектах КИИ.	Определение категории значимости предприятия самостоятельно или с привлечением экспертов, согласование с ФСТЭК.
Статья 10 ФЗ «О безопасности критической информационной инфраструктуры РФ». Приказ ФСТЭК № 239 от 25.12.2017.	1. Создание системы безопасности объекта КИИ, обеспечение ее функционирования. 2. Предотвращение, выявление и ликвидация последствий неправомерного доступа к информации или иных несанкционированных действий с ней. 3. Непрерывное взаимодействие с системой ГосСОПКА.	Установка систем классов DLP и DCAP.
Указы Президента РФ от 01.05.2022 г. № 250 и от 30.03.2022 № 166. ПП РФ от 22.08.2022 № 1478.	1. Обязательное создание ИБ-подразделений и должности заместителя руководителя по ИБ или возложение обязанностей по ИБ на существующих сотрудников или подразделения. 2. Немедленная реализации мер, решения о необходимости которых принимаются ФСБ и ФСТЭК в пределах их компетенции. 3. Запрет закупок зарубежных СЗИ по 223-ФЗ, запрет их использования с 2025 г. 4. Запрет использования СЗИ из недружественных стран с 2025 г. для всех субъектов КИИ	Установка систем классов SIEM и DLP.

Выполняем требования регуляторов

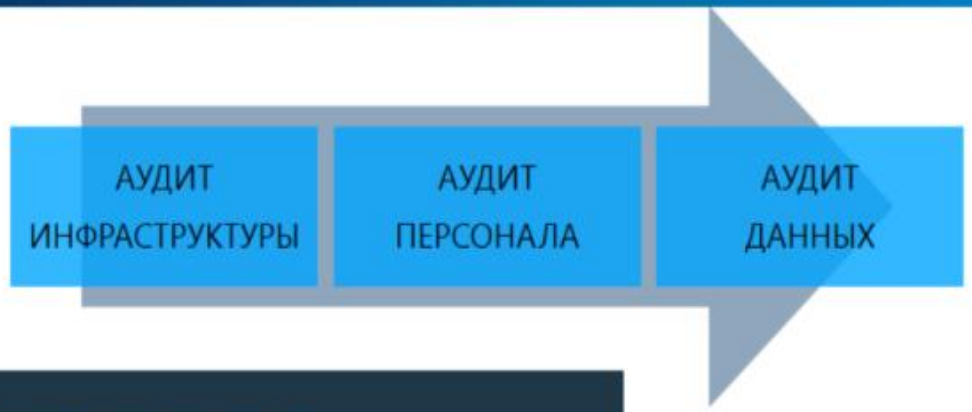
SEARCHINFORM
INFORMATION SECURITY

Федеральный закон № 152-ФЗ «О персональных данных» с изменениями от 14.07.2022 Приказ ФСТЭК № 17	1. Применение части мер защиты КИИ к обеспечению безопасности персональных данных. 2. Взаимодействие операторов персональных данных с ГосСОПКА. 3. Обязанность уведомлять Роскомнадзор об утечках персональных данных и принятых к ликвидации и расследованию инцидентов мерах. 4. Обязанность уведомлять Роскомнадзор об обработке и трансграничной передаче данных.	Применение DLP, DCAP и SIEM-систем для защиты персональных данных. Настройка SIEM-системы для взаимодействия с ГосСОПКА в части передачи информации о состоянии ИСПДн.
Приказ ФСТЭК № 31 от 14.03.2014	Внедрение на оснащенных автоматическими средствами управления технологическими процессами (АСУ ТП) критически важных, потенциально опасных, представляющих повышенную опасность для людей и окружающей среды объектах средств защиты информации. Обеспечение защиты информации при эксплуатации АСУ ТП от несанкционированного доступа при помощи сертифицированных средств защиты..	Создание центров SOC на промышленных предприятиях. Использование систем классов VM, IRP, SIEM и SOAR.

1. https://rspectr.com/articles/kriticheskoe-importozameshhenie
2. https://lukatsky.ru/aiovg_videos/dialog-s-fstek-rossii-vitaliy-lyutikov-otvechaet-na-voprosy-spetsialistov-ib-17-02-2021-bis-tv

Аудит и категоризация

SEARCHINFORM
INFORMATION SECURITY



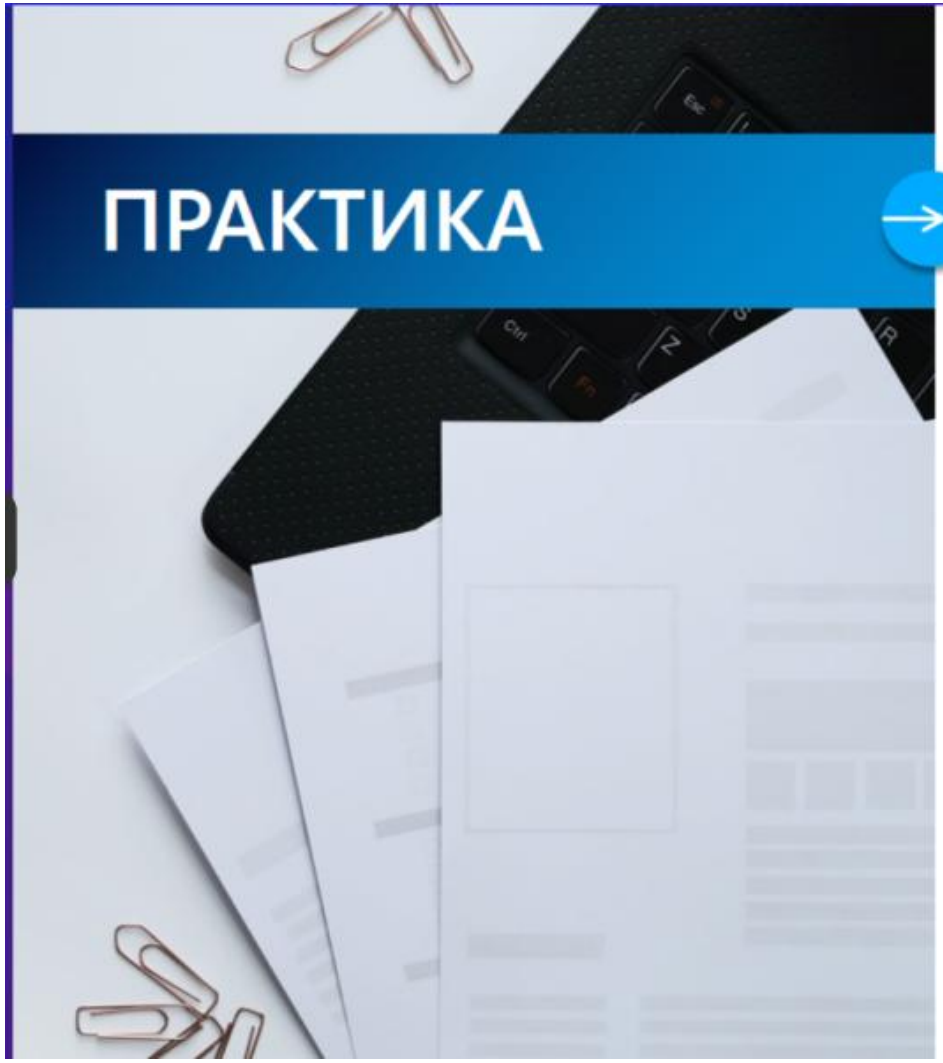
- **Аудит инфраструктуры**
- **Аудит данных**
- Аудит персонала
- Криптозащита
- Разграничение доступа
- Предотвращение утечек
- Анализ информации
- Контроль операторов

DCAP отвечает на важные вопросы внутренней информационной безопасности:

- Какие файлы содержат критичную для бизнеса информацию (техническую, финансовую, клиентскую) ?
- Сколько в компании таких данных и где они находятся?
- Кто имеет к ним доступ и может их редактировать?

Какие задачи решает?

- Классификация конфиденциальных данных
- Аудит прав доступа
- Изоляция критичных документов
- Контроль и блокировки действий пользователей

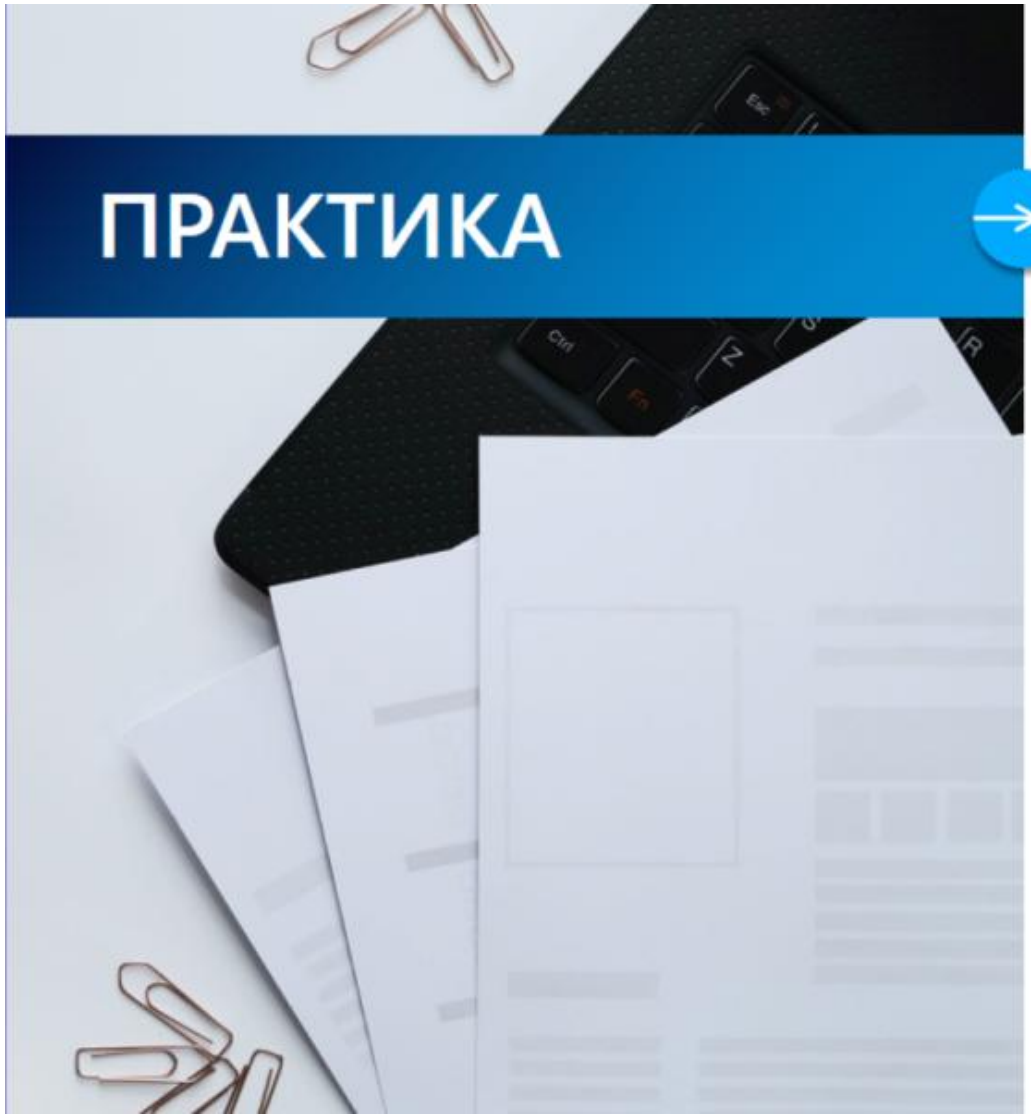


ПРАКТИКА

Что произошло: Содержимое файл-сервера компании зашифровали. При этом следов вируса-шифровальщика не обнаружилось

Как раскрыли: SIEM-система зафиксировала перебор паролей к сервисам с внешних IP-адресов, а также успешный вход учетной записи с правами доменного администратора и ее последующее использование.

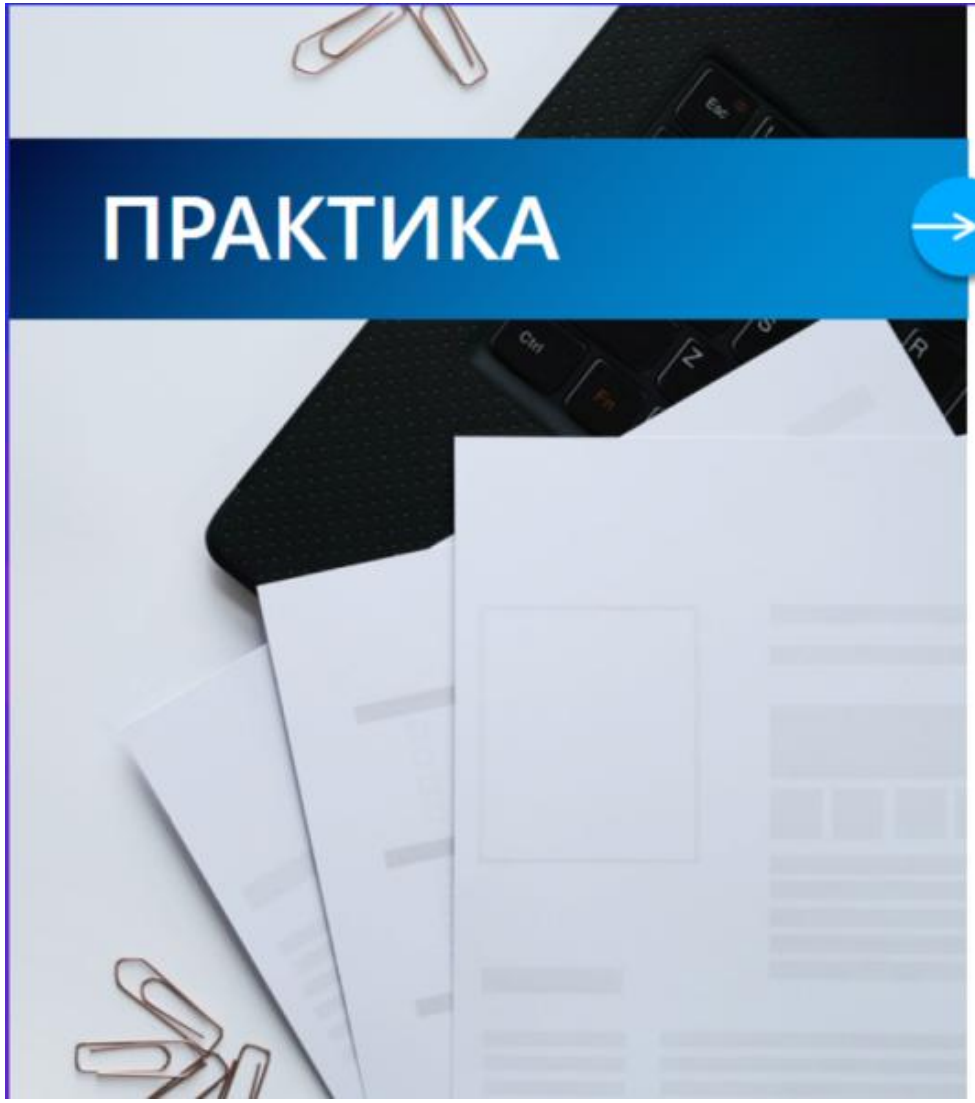
SEARCHINFORM
INFORMATION SECURITY



Что произошло: После увольнения системного администратора сети в компании «легли».

Расследование: Сотрудник создал отложенное правило применения нулевой конфигурации. Через 2 недели оно было применено и уничтожило конфигурации сетевого оборудования. На полноценное восстановление работы ушло много времени и потребовалось привлечение компании-разработчика.

SEARCHINFORM
INFORMATION SECURITY



ПРАКТИКА

Что произошло: После установки системы классификации данных ИБ-служба обнаружила, что на сервере нарушается политика разграничения доступа.

Расследование: Дальнейший анализ показал, что в общем доступе хранится **до трети конфиденциальных файлов организации.** Данные классифицировали и навели порядок в файловой системе.

SEARCHINFORM
INFORMATION SECURITY

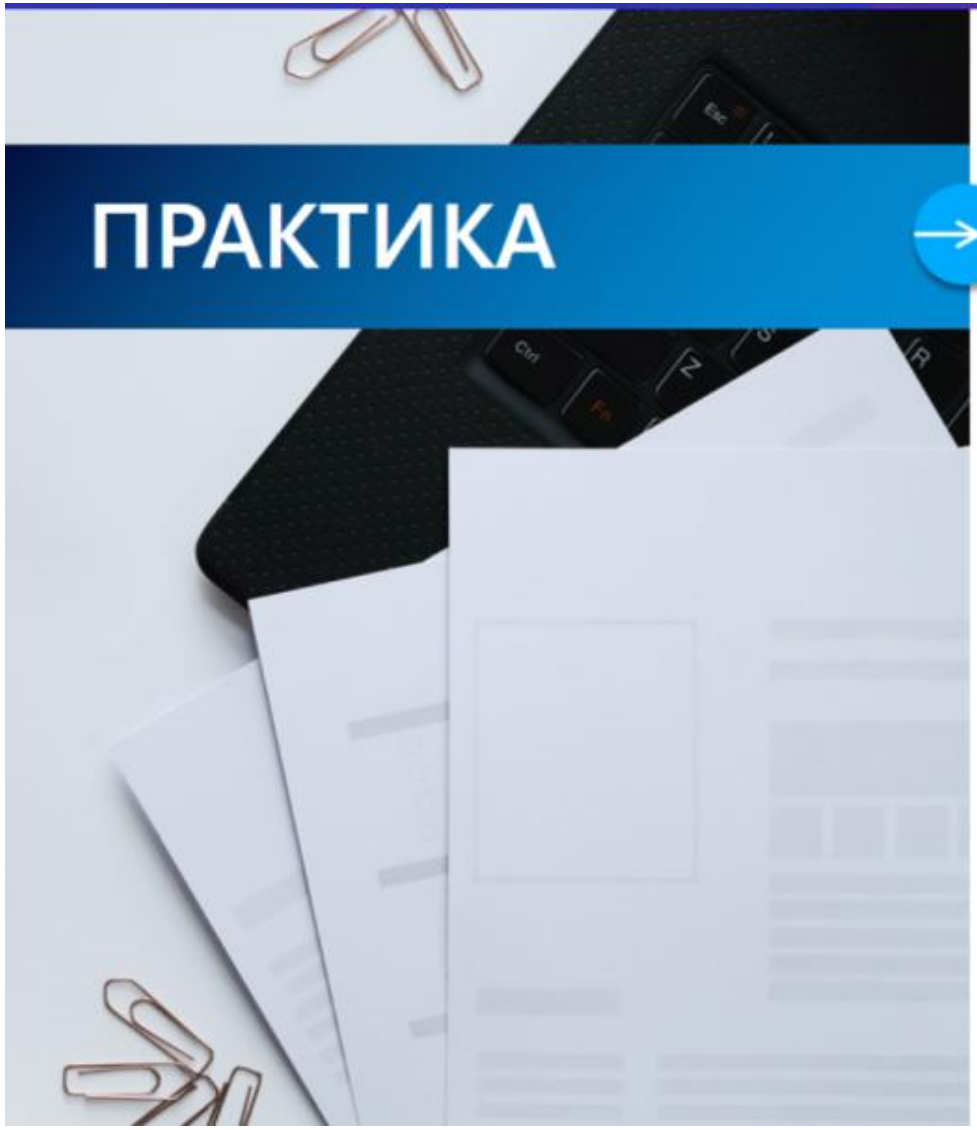
Аудит и категоризация

SEARCHINFORM
INFORMATION SECURITY

Аудит персонала дает понимание:

- Чем, кроме работы, занимаются сотрудники?
- Какими сервисами пользуются с рабочих мест?
- На каких устройствах они сидят?
- Передают ли кому-то пароли и учетные данные?
- Используют ли они корпоративные учетные данные на публичных сервисах?

- Аудит инфраструктуры
- Аудит данных
- **Аудит персонала**
- Криптозащита
- Разграничение доступа
- Предотвращение утечек
- Анализ информации
- Контроль операторов



ПРАКТИКА

Что произошло: Легитимный вход под "несуществующим" сотрудником.

Расследование: Сотрудник, который был принят на работу, но не отработал ни единого дня, вел бурную активность в корпоративной инфраструктуре.

SEARCHINFORM
INFORMATION SECURITY

Криптозащита

SEARCHINFORM
INFORMATION SECURITY

Криптосредства, основные требования:

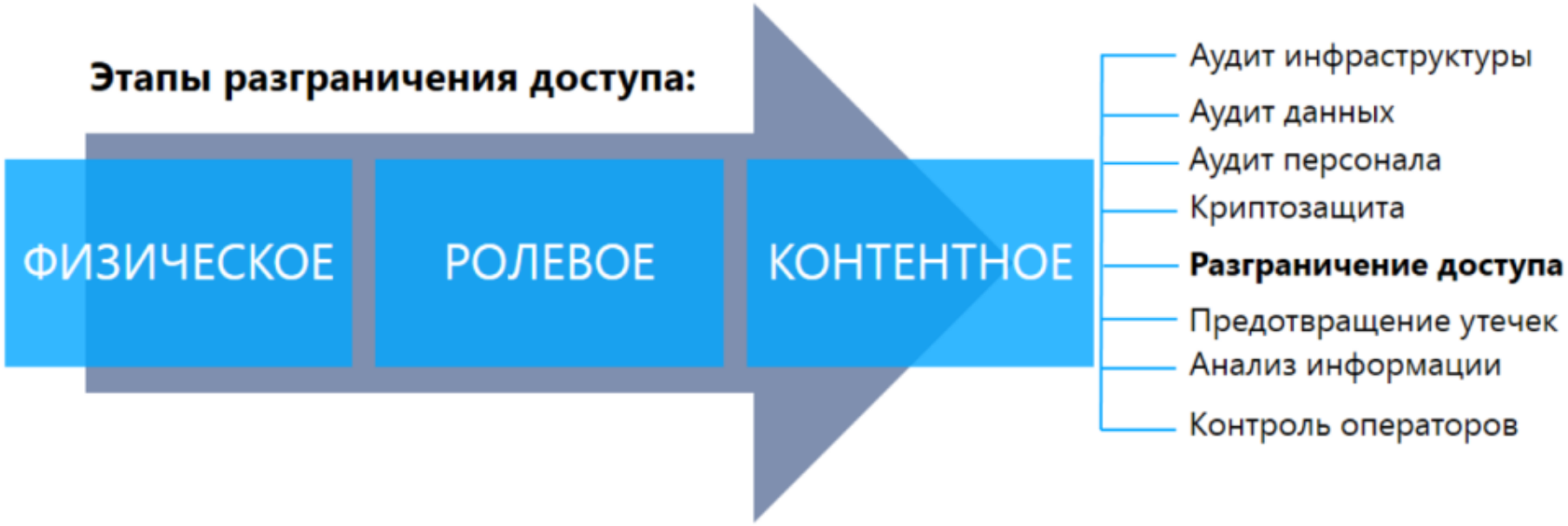
- Иметь принудительный режим работы, когда ошибки и неправомерные действия пользователя исключены
- Применяться к каналам передачи
- Применяться к данным
- Иметь контентно-зависимые правила
- Управляться ИБ-специалистом

- Аудит инфраструктуры
- Аудит данных
- Аудит персонала
- **Криптозащита**
- Разграничение доступа
- Предотвращение утечек
- Анализ информации
- Контроль операторов

Классические криптоинструменты обеспечивают безопасное хранение и передачу, но не защищают от небезопасного использования.

Разграничение доступа

SEARCHINFORM
INFORMATION SECURITY



Разграничение доступа решает административную проблему,
но не защищает от «продвинутых» угроз (взломы, инсайд).

DLP: Перехват

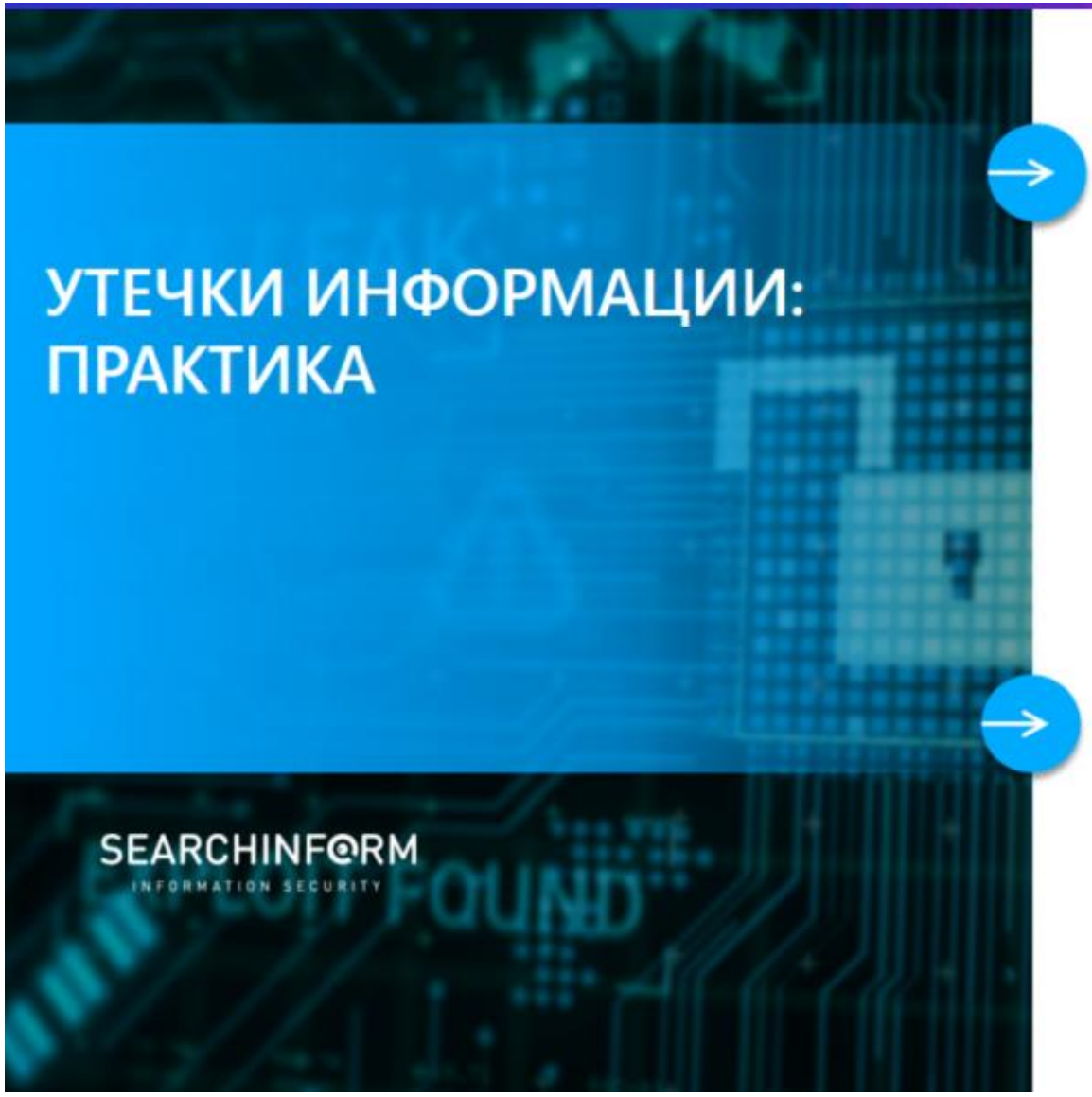
SEARCHINFORM
INFORMATION SECURITY

DLP должна:

- Контролировать **все** каналы передачи
- Иметь тотальную базу данных

- Аудит инфраструктуры
- Аудит данных
- Аудит персонала
- Криптозащита
- Разграничение доступа
- **Предотвращение утечек**
- Анализ информации
- Контроль операторов

✓ **Все каналы коммуникаций под надзором**
✓ **Доступен архив теневых копий**



Умышленные или случайные публикации, пересылки третьим лицам и публикация защищаемой информации в силу неправомерного доступа.

Бывший сотрудник компании в сфере ТЭК сохранил доступ к технической документации на разработки и продал ее в частные руки.*

Торговля служебной информацией в пользу разведок, криминальных организаций и пр.

Руководитель оборонного завода в корыстных целях передал за рубеж информацию о разработках предприятия.**

*- http://geoinform.ru/eks-rukovoditel-goskompanii-v-sfere-tek-zaderzhan-za-peredachu-razrabotok-za-2-mlrd-rublej/
** - https://readovka.news/news/35234

DLP: Анализ

SEARCHINFORM
INFORMATION SECURITY

DLP включает:

- Проработанные алгоритмы анализа.
- Развитую система отчетности.
- Гибкую систему оповещений.

- Аудит инфраструктуры
- Аудит данных
- Аудит персонала
- Криптозащита
- Разграничение доступа
- Предотвращение утечек
- **Анализ информации**
- Контроль операторов

Правила ИБ работают в автоматизированном режиме для каналов передачи данных, но без надзора остается «внесетевая» активность сотрудников.

ПРАКТИКА

Что произошло: сработала политика по наркотическому словарю – сообщения топ-менеджера руководителя по реализации товаров в мессенджере очевидно содержали кодовое слово и автомобильный номер.

Расследование: выяснилось, что коды были номерами машин из корпоративного автопарка. Руководитель кадровой службы переправлял наркотики в регионы России.

SEARCHINFORM
INFORMATION SECURITY

Контроль оператора

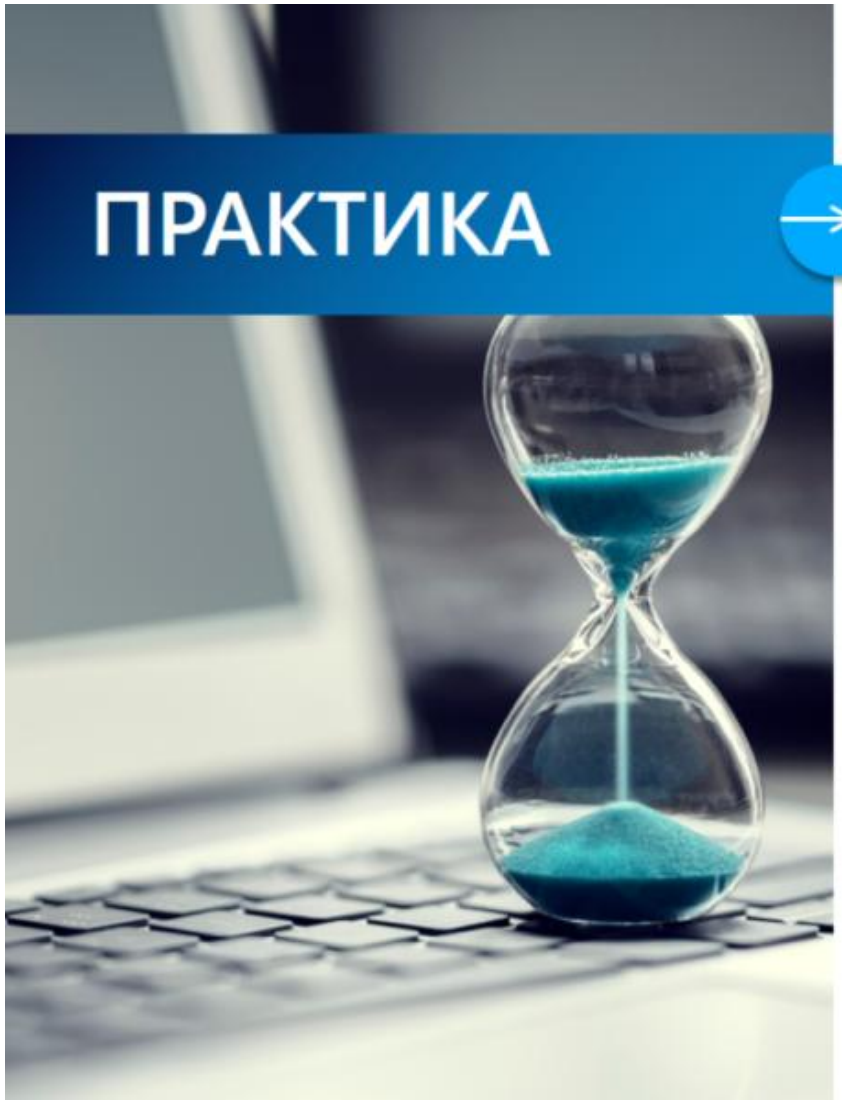
SEARCHINFORM
INFORMATION SECURITY

Контроль оператора включает:

- Видеозапись
- Аудиозапись
- Категорирование работы
- Файловый надзор
- Запись веб-камер
- Онлайн-контроль

- Аудит инфраструктуры
- Аудит данных
- Аудит персонала
- Криптозащита
- Разграничение доступа
- Предотвращение утечек
- Анализ информации
- **Контроль операторов**

Контроль оператора позволяет оценивать эффективность деятельности сотрудников и отслеживать деструктивное поведение вне работы за компьютером



После анализа выяснилось, что 52 из 700 сотрудников организации тратили по **15–20 часов в неделю на развлекательные ресурсы** и онлайн-игры. От нецелевого использования рабочего времени учреждение ежегодно теряло более 10 млн руб. Штат оптимизирован.

SEARCHINFORM
INFORMATION SECURITY

Результат мероприятий

SEARCHINFORM
INFORMATION SECURITY

Итак, резюмируем:

SEARCHINFORM
INFORMATION SECURITY

Высокий уровень информационной безопасности в существующих условиях – не только обязательное требование, но и **конкурентное преимущество** предприятия.

1 Выполнение обязательных требований

- Создание ИБ-подразделения, определение компетентного руководителя;
- Категорирование объектов КИИ;
- Оценка защищенности объектов КИИ;
- Создание системы защиты информации (принятие организационных мер, приобретение сертифицированных отечественных технических средств защиты информации или ИБ-аутсорсинг);
- Организация расследования инцидентов и взаимодействия с ГосСОПКА.

2 Качественное обеспечение защищенности ИС

- Понимание наиболее опасных для конкретного предприятия киберугроз;
- Выбор и внедрение необходимых средств защиты информации;
- Повышение компетенций своих ИБ-специалистов;
- Противодействие «человеческому фактору»: повышение уровня цифровой грамотности и кибергигиены всего персонала предприятия.

- *31% российских промышленных компаний увеличили ИБ-бюджеты.*
- *51% российских компаний создали или создают ИБ-отделы по итогам 2022 года.*
- *78% проводят ИБ-обучение сотрудников.*