КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Вопросы защиты персональных данных и противодействия их утечке

Сергей Вахонин

Директор направления
систем ИБ
sv@cyberprotect.ru

КИБЕРПРОТЕКТ

Что такое персональные данные?

Ключевые определения

Персональные данные

Любая информация, относящаяся прямо или косвенно к определенному или **определяемому** физическому лицу (субъекту персональных данных)

* Федеральный закон "О персональных данных" N 152-ФЗ

Personally identifying information (PII)

Имена и фамилии людей, даты рождения, места регистрации, адреса электронной почты, номер паспорта, налоговые идентификаторы (ИНН) и прочая подобная информация

Sensitive personal information (SPI)

Конфиденциальные персональные данные как медицинские записи и истории болезней, биометрические данные, финансовая информация, прочие чувствительные данные

Влияние регуляторов

Типы данных, безопасность и конфиденциальность которых регулируется во всем мире: данные платежных карт, персональные данные сотрудников и клиентов, медицинские данные, интеллектуальная собственность, торговые секреты, коммерческая тайна, государственные классифицированные данные**.**

Международные нормативные требования:

- **GDPR** – регулирует сбор, доступность, конфиденциальность и безопасность **персональных** данных; определяет требования к отчетам о нарушениях. Все еще актуален для российских компаний, работающих с ЕС!
- **HIPAA** – регулирует сбор, доступность, конфиденциальность и безопасность **медицинской** информации;
- **PCI DSS** – регулирует сбор, доступность, конфиденциальность и безопасность данных держателей карт; мониторинг и отчетность. Актуален для большинства российских банков.
- **GLBA** – регулирует сбор и порядок раскрытия **PII**

Российские нормативные требования:

- **ФЗ-152 –** регулирует обращение с персональными данными граждан.
- **СТО БР ИББС** - Стандарты Банка России в области информационной безопасности. Содержат в т.ч. требования по DLP.
- **ГОСТ Р 57580.1-2017** “Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер”. Вступил в силу 1 янв.2018. Обязателен для всех банков! Раздел 7 прямо содержит требования к наличию систем класса DLP.
- **Приказ ФСТЭК № 17** «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

Важнейшие аспекты ФЗ 152

С 1 сентября 2022 года вступили в силу поправки в 152-ФЗ (266-ФЗ от 14.07.2022).

Связка «Пользовательское соглашение – Политика конфиденциальности» более не является достаточным основанием для обработки ПДН.

Теперь необходимо подавать уведомление в РКН и готовить локальные документы по защите ПДн.

Устанавливается штраф для должностных лиц в размере от 5 до 10 тысяч рублей, а для юридических — в размере от 30 до 500 тысяч рублей.

В процессе чтения законопроекта планировали назначить штраф для должностных лиц от 500 тысяч до 1 млн рублей, а ко второму чтению стало от 500 тысяч до 800 тысяч рублей.

Обсуждается

- Обязать Операторов персональных данных оперативно сообщать обо всех кибератаках и утечках персональных данных россиян в уполномоченные органы.
- Ввести принцип оборотных штрафов, если утечка затрагивает данные от 10 тыс. пользователей.
- сделать штрафы за утечку данных соразмерными объемам информации

Сравним: GDPR

Оборотные штрафы

Штрафы могут достигать 20 млн евро или 4 % от годового мирового оборота компании за предыдущий финансовый год.

Жесткие сроки

Срок уведомления о нарушении приватности данных не должен превышать 72 часа.

Information Privacy

Введена правовая норма “Data Protection by Design” как применение принципа “Privacy by Design” в контексте ИТ

Information Privacy = неприкосновенность персональной информации, неприкосновенность персональных данных.
Данное понятие является частью общего понятия "неприкосновенность частной жизни".
Иными словами, "неприкосновенность персональной информации" есть "неприкосновенность частной жизни применительно к информационному контексту".

Сравним: GDPR

Без безопасности нет приватности

Ст.5 GDPR : фундаментальное требование обеспечить “integrity and confidentiality”.	“Безопасность персональных данных, включая защиту от несанкционированной или незаконной обработки и от случайной потери, уничтожения или повреждения”.
Ст.4 GDPR : определение термина «обработка» (“**processing**”).	“Обработка означает любую операцию или набор операций, выполняемых с персональными данными или их множествами, … включая хранение, …, использование, раскрытие посредством передачи, распространения или иными способами”.
Ст.4 GDPR : определение термина «**Personal data breach**».	“Уязвимость персональных данных означает нарушение информационной безопасности, приводящее к случайному или незаконному уничтожению, потере или изменению ПДн, а также несанкционированному раскрытию или доступу к персональным данным, переданным, сохраненным или обработанным иным образом”.
Ст.32 GDPR : определение требований к безопасной обработке данных.	“In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from *accidental or unlawful destruction, loss, alteration,* ***unauthorised disclosure of, or access*** *to personal data* ***transmitted, stored or otherwise processed***.”

GDPR в ИТ (ИБ) реальности

GDPR – технологически нейтральный закон

GDPR не определяет, какие именно технологии следует использовать для реализации защиты данных.

GDPR = защита определенного типа данных

Положения GDPR не применяются к данным, которые содержат любую другую информацию, **кроме** персональных или данных, содержащих личную информацию (PII). .

Технические требования

- Анализ содержимого данных на соответствие политике защиты PII
- Возможность обеспечить выполнение действий, необходимых для предотвращения утечки данных (требование анализа в режиме реального времени).

Пример

Отправка электронной почты, не содержащей персональные данные, не нарушает требования GDPR. Отправка сообщения с личной информацией (без согласия субъекта данных) – нарушает.

Единственное различие – содержание данных в сообщении (*PII или нет*).
Единственный способ различить – анализ всего содержимого данных до передачи.

Чем проще сценарий утечки данных – тем более он вероятен

Использование сотрудниками консьюмерских («ширпотреб») ИТ-сервисов и устройств для решения как личных, так и рабочих задач, приводит к размытию границ. Пользователь становится “центром” в информационных процессах, что резко повышает значимость его дисциплины при использовании корпоративных данных.

Отсутствие фокуса на безопасности

Практически все сетевые приложения (социальные сети, облачные хранилища, мессенджеры), созданные **для удобства пользователей**, для удовлетворения их социальных потребностей – функционируют абсолютно **без какой-либо обратной связи** с инструментарием корпоративной безопасности.

Решения принимаются пользователем

Модель информационной безопасности потребительских приложений основывается на том, что **все решения** о способах и уровне авторизации, аутентификации и уровне доступа к данным принимает конечный **пользователь** – который далеко не всегда является владельцем данных, будучи при этом сотрудником организации.

Дилемма для ИБ

Полный запрет личных устройств приводит к отказу от всех преимуществ консьюмеризации и BYOD как стратегии, стимулирующей сотрудников эффективно решать рабочие задачи с личных, удобных в использовании устройств широкого потребления и персонализированных сервисов.

Полное доверие – оставляет в силе все риски и угрозы. Концепция Zero trust – снова в тренде…

Удобство использования, повышение эффективности

Предприятию выгодно обеспечить сотрудникам максимально комфортный доступ к персональным коммуникациям, в том числе – в рабочее время, поскольку такие коммуникации повсеместно используются для бизнеса,
а значит, повышается эффективность производственных процессов и результативность труда сотрудников..

Рост количества и качества угроз и рисков ИБ

- Попадание в корпоративную ИС запрещенного и вредоносного контента
- Умышленные или непреднамеренные утечки конфиденциальной информации
- Неспособность традиционных решений обеспечить безопасность данных
- Частная собственность сотрудников на используемые устройства

Как утекают данные

Анализ на примере персональных данных

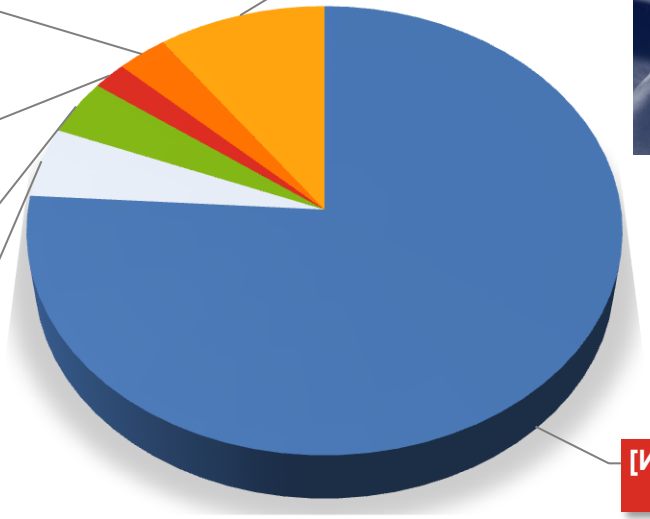
Утечки через фотографирование рабочих экранов составляют *всего лишь 10%*

Мессенджеры, социальные сети, ... , [ЗНАЧЕНИЕ]

Облачные файловые хранилища; 2%

Электронная почта, веб-почта; 4%

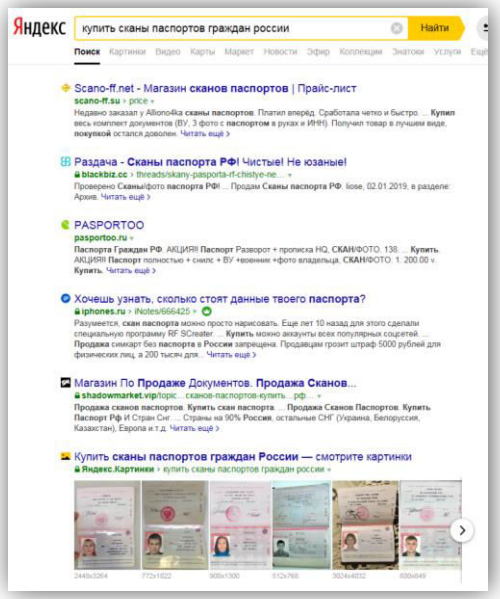
Печать документов, бумажный носитель; 5%



[ИМЯ КАТЕГОРИИ] **[ЗНАЧЕНИЕ]**

[ИМЯ КАТЕГОРИИ]; [ЗНАЧЕНИЕ]

Продажа персональных данных



- Базы персональных данных в формате Excel, содержащие ФИО, пол, телефон, полные паспортные данные, СНИЛС, адрес регистрации и проживания реализуются по 20-25 копеек за одну запись.
- Ценность персональных данных без сканов документов невелика, так как они применяются в основном для спама и телефонного мошенничества
- Сканы документов могут быть использованы для получения онлайн-займов и поэтому весьма востребованы криминальными элементами

В России с начала 2022-го произошло более 40 крупных утечек баз персональных данных, скомпрометировано 300 млн записей (Роскомнадзор)

Немного объективной статистики

83%

of organizations studied have had more than one data breach.

60%

of organizations' breaches led to increases in prices passed on to customers.

79%

of critical infrastructure organizations didn't deploy a zero trust architecture.

19%

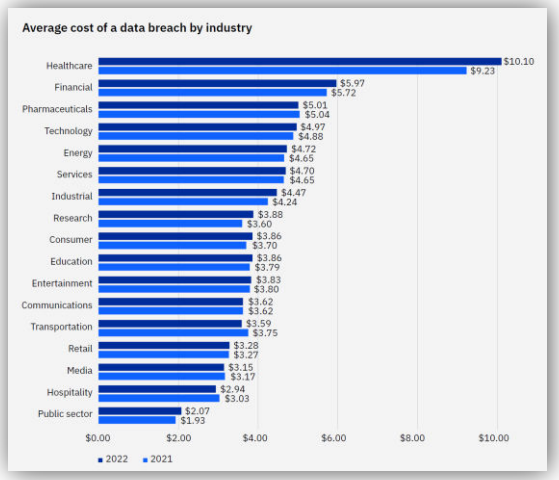
of breaches occurred because of a compromise at a business partner.

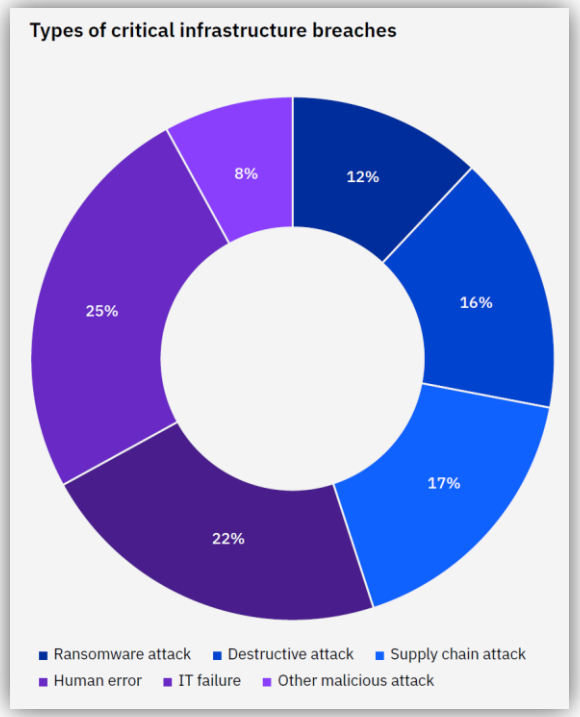
45%

of the breaches were cloud-based.

59%

Percentage of organizations that don't deploy zero trust





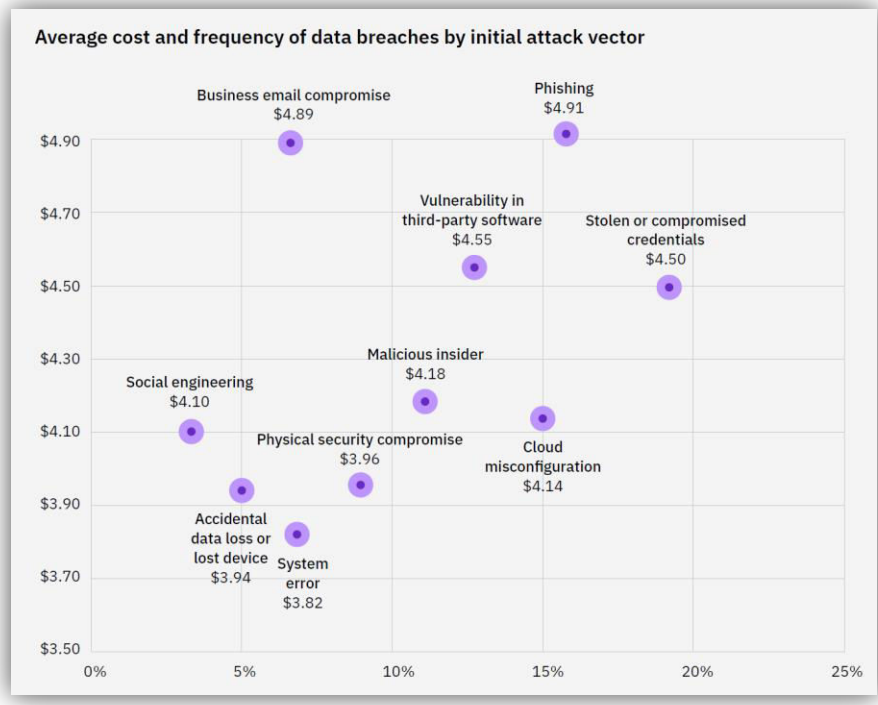
Ponemon: 3,600 separate interviews with individuals at 550 organizations that suffered a data breach between March 2021 and March 2022

Ponemon INSTITUTE

КИБЕРПРОТЕКТ

Источники: "Cost of a Data Breach", **Ponemon Institute & IBM Security, 2022** ; "Insider Threat Report", Cybersecurity Insiders, 2018; "Data Protection Risks & Regulations in the Global Economy, Ponemon Institute, 2017; CSO Online, 2017; "Insider Data Breach Survey", Opinion Matters, 2019; 2020 Cost of a Data Breach Report" Ponemon Institute LLC, July 2020; "2020 Cost of Insider Threats Global Report" Ponemon Institute LLC, February 2020; "Best Practices: Mitigating Insider Threats" Forrester Research, May 2019

Немного объективной статистики



90% организаций чувствуют себя уязвимыми перед лицом инсайдерских угроз - 53% сообщают, что подверглись атаке со стороны инсайдеров за последние 12 месяцев

72% сотрудников делятся конфиденциальной или иной защищаемой информацией компании

35% сотрудников поделились информацией, **не подозревая,** что ей не следует делиться.

Годовой ущерб от утечек, связанных с инсайдерами (~ 45% всех нарушений)

- **31% увеличение** за последние 2 года
- Средний **по всему миру: $11,45 млн.**
- В среднем за **Малый и средний бизнес: $7,68**
- **89% от стоимости** связано с действиями после инцидента (реактивная защита)

Антивирусы, брандмауэры, шифрование **и даже бэкапы** не защищают от внутренних утечек данных

КИБЕРПРОТЕКТ

Источники: “Cost of a Data Breach”, **Ponemon Institute & IBM Security, 2022** ; “Insider Threat Report”, Cybersecurity Insiders, 2018; “Data Protection Risks & Regulations in the Global Economy, Ponemon Institute, 2017; CSO Online, 2017; “Insider Data Breach Survey”, Opinion Matters, 2019; 2020 Cost of a Data Breach Report” Ponemon Institute LLC, July 2020; “2020 Cost of Insider Threats Global Report” Ponemon Institute LLC, February 2020; “Best Practices: Mitigating Insider Threats” Forrester Research, May 2019

Почему без DLP не обойтись?

Единственно доступная сегодня технология, удовлетворяющая всем требованиям защиты от утечки персональных данных

Защита стратегически важной информации

Непрерывный контроль всех возможных каналов информационного обмена и хранимых данных

Соответствие требованиям регуляторов

Обеспечение соответствия требованиям стандартов за счет полноценного контроля каналов передачи данных и устройств хранения информации, журналирования событий и инструментария расследования инцидентов

Выявление инцидентов

- Повышение эффективности ИБ - реагирование на события, связанные с вопросами защиты данных

- Аудит журналов DLP-системы

- Выявление инсайдеров-злоумышленников, нелояльных сотрудников.

Контроль исполнения политики хранения

Превентивная защита данных, размещенных в корпоративной ИТ-инфраструктуре

CYBER Protego

История создания

1996
Выпущена первая версия DeviceLock как специализированное решение класса Endpoint Device/Port Control

2008
Продукт DeviceLock расширен рядом новых модулей и перешел в категорию DLP-решений под именем **DeviceLock DLP**

2020-2021
Acronis приобретает компанию DeviceLock

Ноябрь 2021: Киберпротект выпускает Акронис DLP Защиту 9.0

2022
Киберпротект выпускает комплекс под новым именем Cyber Protego, выпущены версии 9.x, Актуальная – 9.3.1 (июль 22)

Cyber Protego позволяет

Минимизировать угрозу инсайдерской утечки данных

Недопущение утечки данных путем блокировки несанкционированных попыток передачи, сохранения или печати данных, регистрация всех связанных событий

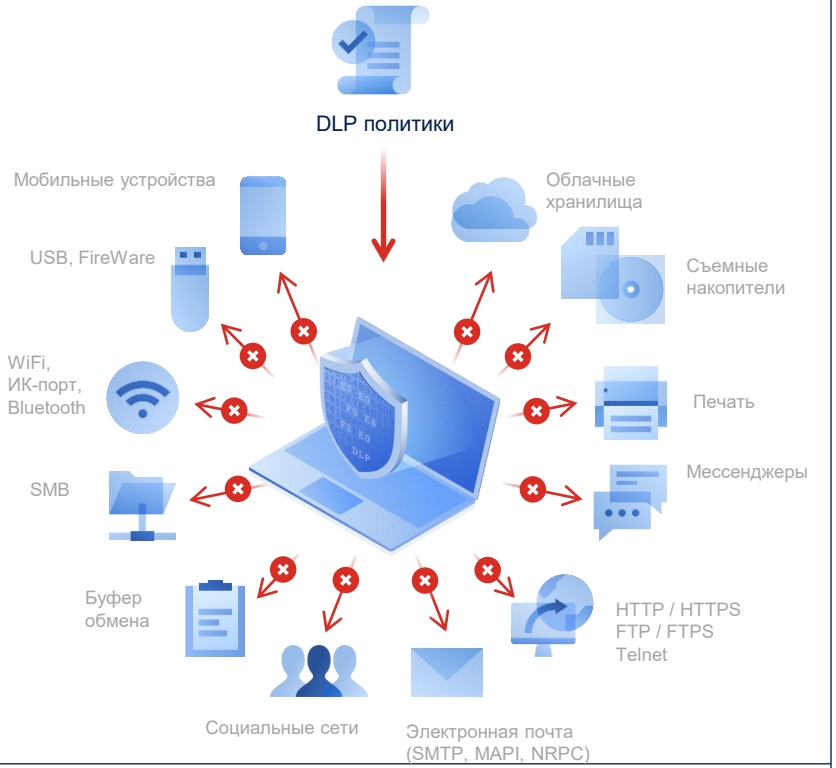
Обеспечить прозрачность защиты данных

Единое решение для защиты данных при их передаче через все каналы для всех пользователей, прозрачная интеграция в Active Directory.

Встроенные инструменты построения отчетов, просмотра и анализа событий, связей и действий сотрудников.

Обеспечить выполнение требований регуляторов

Снижение рисков информационной безопасности, обеспечение соответствия требованиям стандартов и норм ИТ-безопасности за счет принудительного (гарантированного) применения политик защиты данных.



Что умеет Cyber Protego?

ПРЕДОТВРАЩЕНИЕ УТЕЧЕК ДАННЫХ (КОНТРОЛЬ ДОСТУПА)

- Контроль всех видов устройств и интерфейсов
- Контроль множества каналов сетевых коммуникаций
- Технологии контентной фильтрации (**включая детектирование ПДн**) – в **режиме реального времени**

ДЕТАЛЬНЫЙ МОНИТОРИНГ СОБЫТИЙ

- Детализированное протоколирование событий
- Теневые копии для большинства контролируемых каналов передачи данных
- User Activity Monitor
- Тревожные оповещения

СКАНИРОВАНИЕ ХРАНИМЫХ ДАННЫХ

- Автоматическое устранение выявленных нарушений политики безопасного хранения данных
- Различные режимы сканирования (локально, удаленно)
- Работа по заданному расписанию, автоматические отчеты

АНАЛИЗ АРХИВА СОБЫТИЙ

- Полнотекстовый поиск по теневым копиям в централизованном или распределенном архиве DLP-системы
- Автоматическое выполнение поисковых запросов по расписанию
- Статистические отчеты, графы связей
- Досье пользователя

Контролируемый удаленный доступ к данным

Cyber Protego TS

Агент функционирует “внутри” терминальной сессии

- Приложения, опубликованные на гипервизорах
- Локальные виртуальные машины
- Терминальные сессии рабочих столов, в т.ч. опубликованных на гипервизорах
- Решения для виртуализации от Microsoft (RDS/RDP), Citrix (XenApp, XenDesktop) и VMware (VMware View)
- Детектирование перенаправленных устройств в сессии независимо от используемых протоколов (Microsoft RDP/RemoteFX, Citrix ICA/HDX)
- Никаких агентов на удаленном устройстве!

Особенности реализации и преимущества

Полноценный DLP-контроль в любых условиях – в офисе или вне его с автоматическим переключением DLP-политик

Контентная фильтрация **в режиме реального времени**

Централизованное управление, включая интеграцию в MS Active Directory

User Activity Monitor (UAM), интегрированный в DLP-политики, с записью до и после события

Защита данных в средах виртуализации **Cyber Protego TS**

Наибольшая широта охвата потенциальных каналов утечки данных

Высочайший уровень **самозащиты агентов**

Автоматические действия по устранению нарушений хранения данных (Discovery)

Независимый от приложений и портов контроль сетевых протоколов, встроенный **резидентный модуль DPI** (Deep Packet Inspection)

Некоторые планы развития

Поддержка ОС Linux

Начаты работы над агентом под ALT Linux и полноценной поддержкой PostgreSQL.

Разделение ролей (ИТ & ИБ)

Поддержка ролевой модели в новой веб-консоли.

Полное обновление интерфейса.

Начаты работы над веб-консолью.

Серверный анализатор трафика

Есть интеграция с **EtherSensor**, будем делать свой шлюз.

Развитие функций UAM

Планируем добавлять много разного (подключение к рабочему столу, запись звука, камеры…).

Конструктор отчетов.

Планируем интегрировать внешний генератор отчетов произвольного состава.

Развитие аналитического блока.

Запланирован новый компонент – Cyber Protego Analytics в формате веб-консоли с новыми отчетами, дашбордами и поиском

Развитие Discovery.

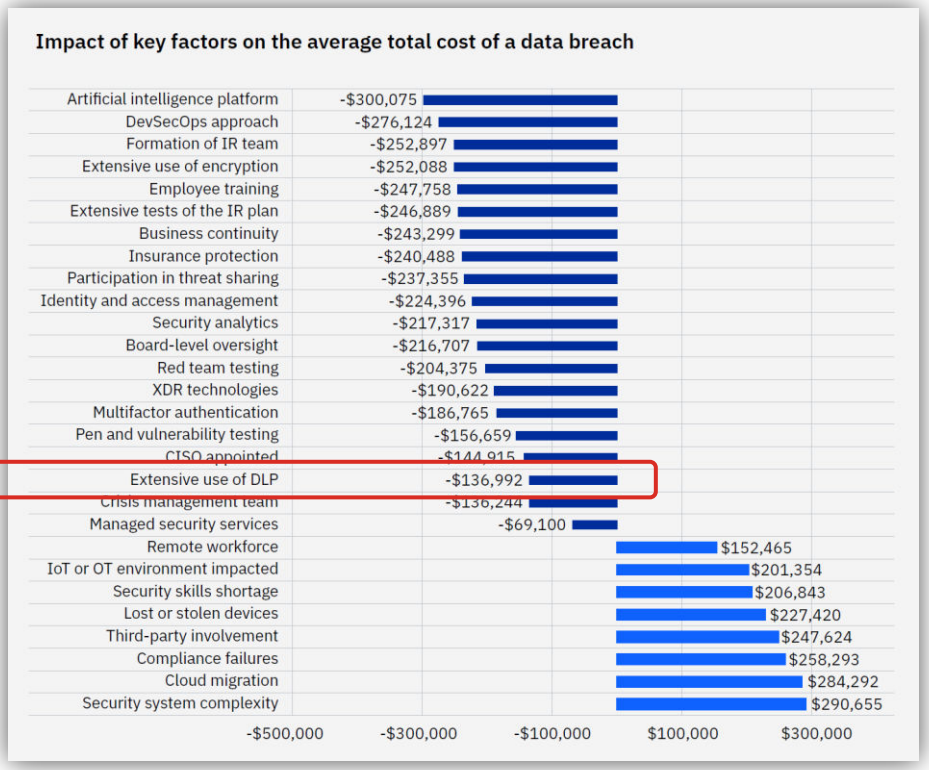
Расширение компонента функциями **DCAP** .

Интеграция DLP-функций в Cyber Files.

Интеграция Protego с продуктом Cyber Files и/или расширение его DLP-возможностями.

Еще немного статистики?

Ponemon INSTITUTE



КИБЕРПРОТЕКТ

КИБЕРПРОТЕКТ

100% российская компания • Продукты входят в реестр Российского ПО
Участник Сколково • Офис в Иннополисе • Ведущие разработчики в штате
Член АРПП "Отечественный софт", РУССОФТ, АПКИТ

2016
Компания становится технологическим партнером Acronis и начинает разрабатывать собственные на основе технологий Acronis

2017
Акронис Защита Данных и Акронис Защита Данных Расширенная вошли в Единый реестр российских программ

2018-2020
Расширение продуктового портфеля, статус резидента Сколково и Иннополис, двукратный рост штата

2021
Компания переименована в КИБЕРПРОТЕКТ
Новые продукты выходят под мастер-брендом «КИБЕР …»

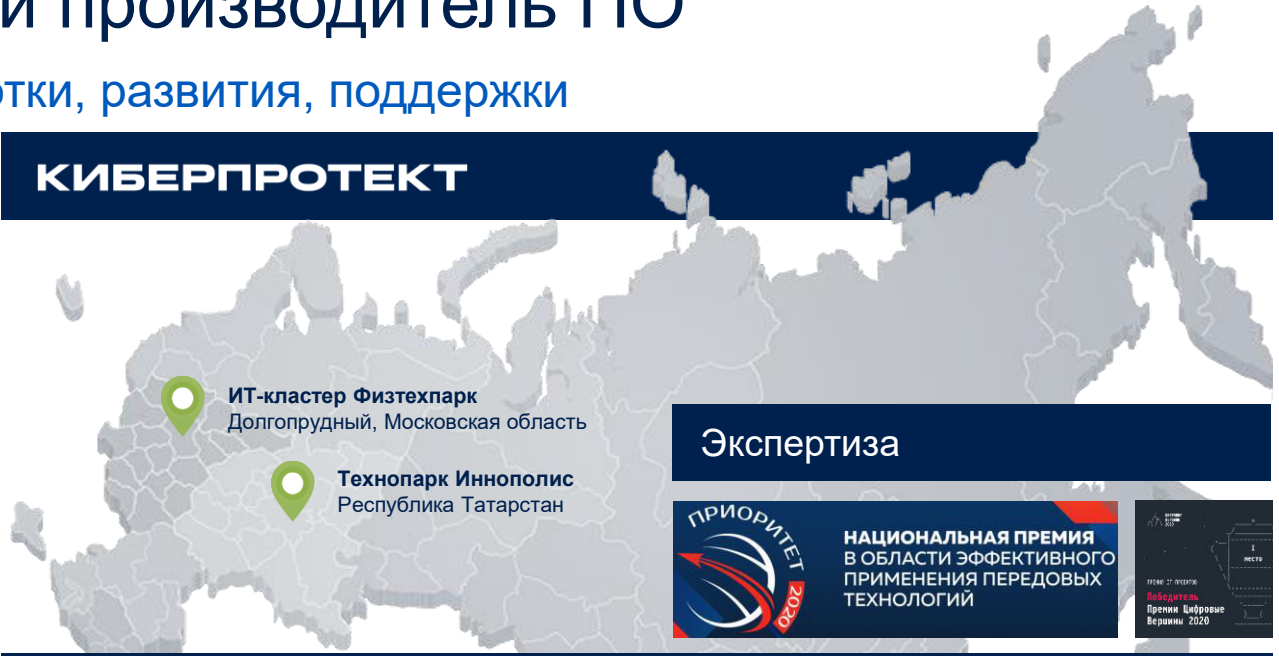
КИБЕРПРОТЕКТ РАНЕЕ Акронис Инфозащита

Отечественный производитель ПО

Полный цикл разработки, развития, поддержки

Примеры внедрений

КИБЕРПРОТЕКТ



ИТ-кластер Физтехпарк
Долгопрудный, Московская область

Технопарк Иннополис
Республика Татарстан

Экспертиза

ПРИОРИТЕТ 2020
НАЦИОНАЛЬНАЯ ПРЕМИЯ В ОБЛАСТИ ЭФФЕКТИВНОГО ПРИМЕНЕНИЯ ПЕРЕДОВЫХ ТЕХНОЛОГИЙ

Участие в проектах и ассоциациях, резидентный статус

АРПП Отечественный софт
Sk Сколково
ЦИФРОВАЯ ЭКОНОМИКА
RUS®SOFT
АПКИТ
INNOPOLIS UNIVERSITY

Продукты и решения

КИБЕР Бэкап

Резервное копирование
ИТ-систем любой сложности
с централизованным управлением
и оптимизацией хранения

КИБЕР Бэкап Облачный

Резервное копирование данных в физических, виртуальных и облачных средах **для поставщиков услуг**

Единый реестр Минцифры

Сертификация ФСТЭК

КИБЕР Протего

Программный комплекс
предотвращения утечек используемых,
передаваемых и хранимых данных

КИБЕР Инфраструктура

Масштабируемое, экономичное и универсальное программно-определяемое решение: виртуализация, хранилище и сеть

Часть экосистемы
отечественного ПО с постоянно расширяющейся **сетью технологических партнёрств**

CommuniGate Pro
ROSA
alt linux
МойОфис
ASTRA LINUX®
Р7-ОФИС
РЕДОС
ICL ТЕХНО
AccentOS®
PROFESSIONAL Postgres
HOSTVM

КИБЕРПРОТЕКТ

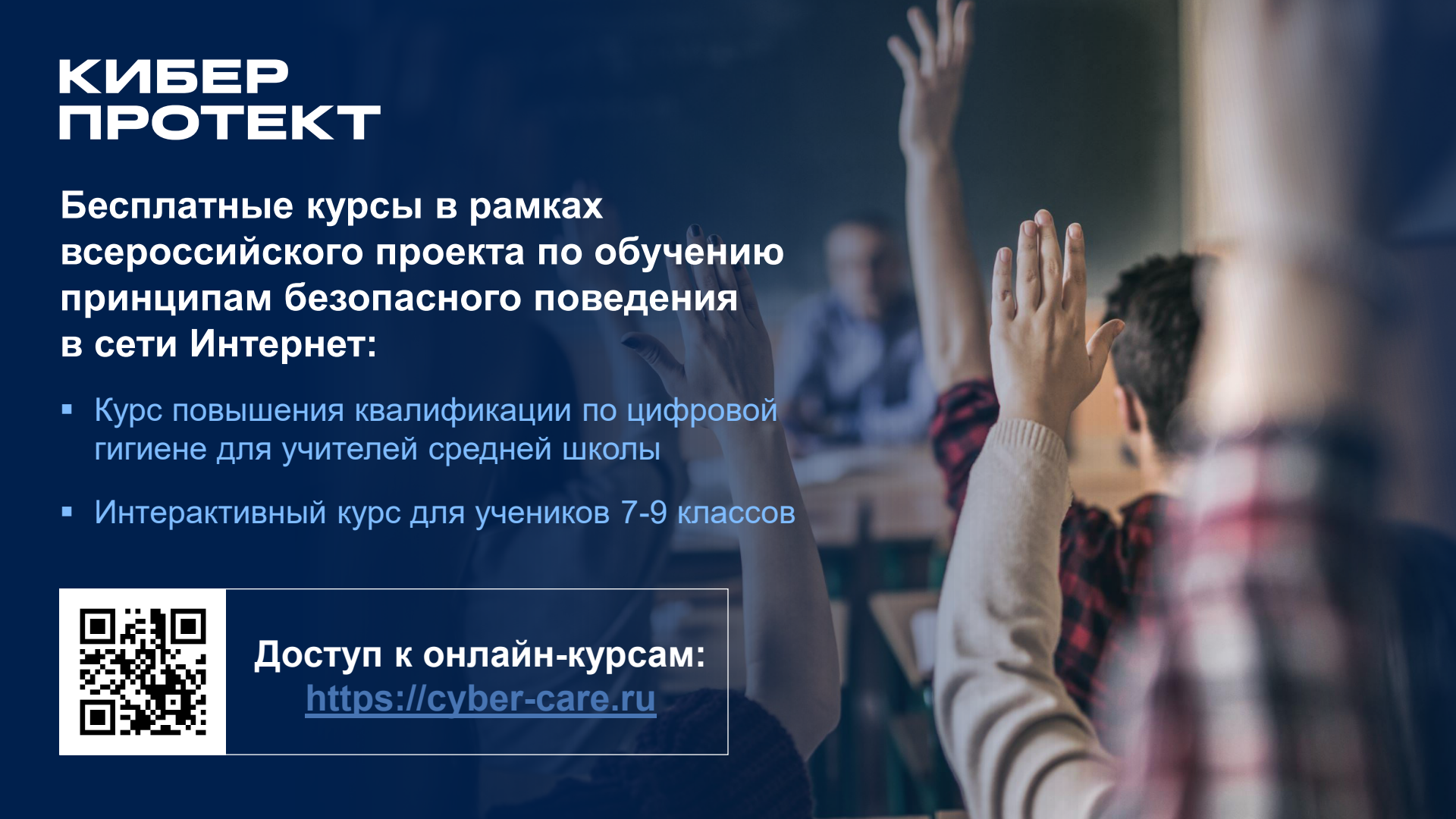
СКОРО CYBER Files

КИБЕР
ПРОТЕКТ

Бесплатные курсы в рамках всероссийского проекта по обучению принципам безопасного поведения в сети Интернет:

- Курс повышения квалификации по цифровой гигиене для учителей средней школы
- Интерактивный курс для учеников 7-9 классов

Доступ к онлайн-курсам:
https://cyber-care.ru



СПАСИБО!

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Сергей Вахонин

Директор направления систем ИБ

sv@cyberprotect.ru

cyberprotect.ru

КИБЕРПРОТЕКТ