KASPERSKY lab

ПРОМЫШЛЕННАЯ КИБЕРБЕЗОПАСНОСТЬ

www.kaspersky.ru

ЛИДЕРСТВО «ЛАБОРАТОРИИ КАСПЕРСКОГО»

«Лаборатория Касперского», признанный мировой лидер в области корпоративной IT-безопасности, не менее успешно решает уникальные задачи обеспечения кибербезопасности промышленных предприятий.

Прочные позиции в отрасли IT-безопасности и стратегическое лидерство

«Лаборатория Касперского» – крупнейшая в мире частная компания, специализирующаяся на разработке решений для обеспечения информационной безопасности. Продукты и сервисы «Лаборатории Касперского» защищают более 300 миллионов пользователей в 200 странах и территориях, а корпоративная клиентская база насчитывает более 250 000 компаний по всему миру – как представителей малого и среднего бизнеса, так и крупных правительственных и коммерческих организаций.

Евгений Касперский, основатель и генеральный директор «Лаборатории Касперского», является признанным экспертом в области информационных угроз и идеологом кибербезопасности. Под его руководством компания, ведущая успешную борьбу с локальными и глобальными угрозами, заработала отличную репутацию среди пользователей и отраслевых специалистов. За последние годы эксперты «Лаборатории Касперского» первыми обнаружили такие известные и сложные киберугрозы, как Darkhotel, Flame, Gauss, miniFlame, «Красный октябрь», NetTraveler и «Маска», а также проанализировали ряд атак, нацеленных на промышленные компании, в том числе Crouching Yetti, Miancha и BlackEnergy 2.

Ведущие позиции в области анализа угроз

Глобальная сеть безопасности Kaspersky Security Network (KSN) собирает и обрабатывает данные о вредоносной активности на компьютерах более 60 миллионов пользователей продуктов «Лаборатории Касперского» по всему миру, давших свое согласие на участие в проекте. Это позволяет успешно прогнозировать распространение существующих угроз.

В нашем глобальном центре исследований и анализа угроз (GReAT) работает международная команда высококвалифицированных специалистов, чей уникальный экспертный опыт позволяет создавать эффективные решения для противодействия самым сложным угрозам.

Лидерство в исследованиях и инновациях

Будучи частной компанией, «Лаборатория Касперского» не ограничивается краткосрочными финансовыми целями и постоянно вкладывает средства в исследования и разработку продуктов и сервисов. Почти половина из 3000 наших сотрудников занимаются разработкой инновационных технологий, а также глубоким исследованием всех видов кибероружия, методов кибершпионажа, кибердиверсий и других типов угроз.

Благодаря собственной прочной научно-исследовательской базе «Лаборатория Касперского» является признанным лидером в сфере технологий для обеспечения информационной безопасности. Независимые эксперты присуждают нашим продуктам наивысшие оценки чаще, чем решениям других поставщиков[1].

Доверенный партнер правительственных организаций и регулирующих органов

Глубокое исследование угроз всегда было неотъемлемой частью стратегии «Лаборатории Касперского». Международное сообщество специалистов по информационной безопасности и такие авторитетные международные организации, как Интерпол, Европол, подразделение Microsoft Digital Crimes Unit, агентства кибербезопасности и многочисленные компьютерные группы экстренного реагирования, а также международное общество автоматизации (ISA) регулярно привлекают экспертов «Лаборатории Касперского» для консультаций и совместной работы, поскольку признают ведущие позиции специалистов компании в области исследования и анализа киберугроз. Сейчас мы тесно сотрудничаем с регулирующими органами России и США по вопросам защиты критически важной инфраструктуры и в связи с разработкой платформы промышленной кибербезопасности.

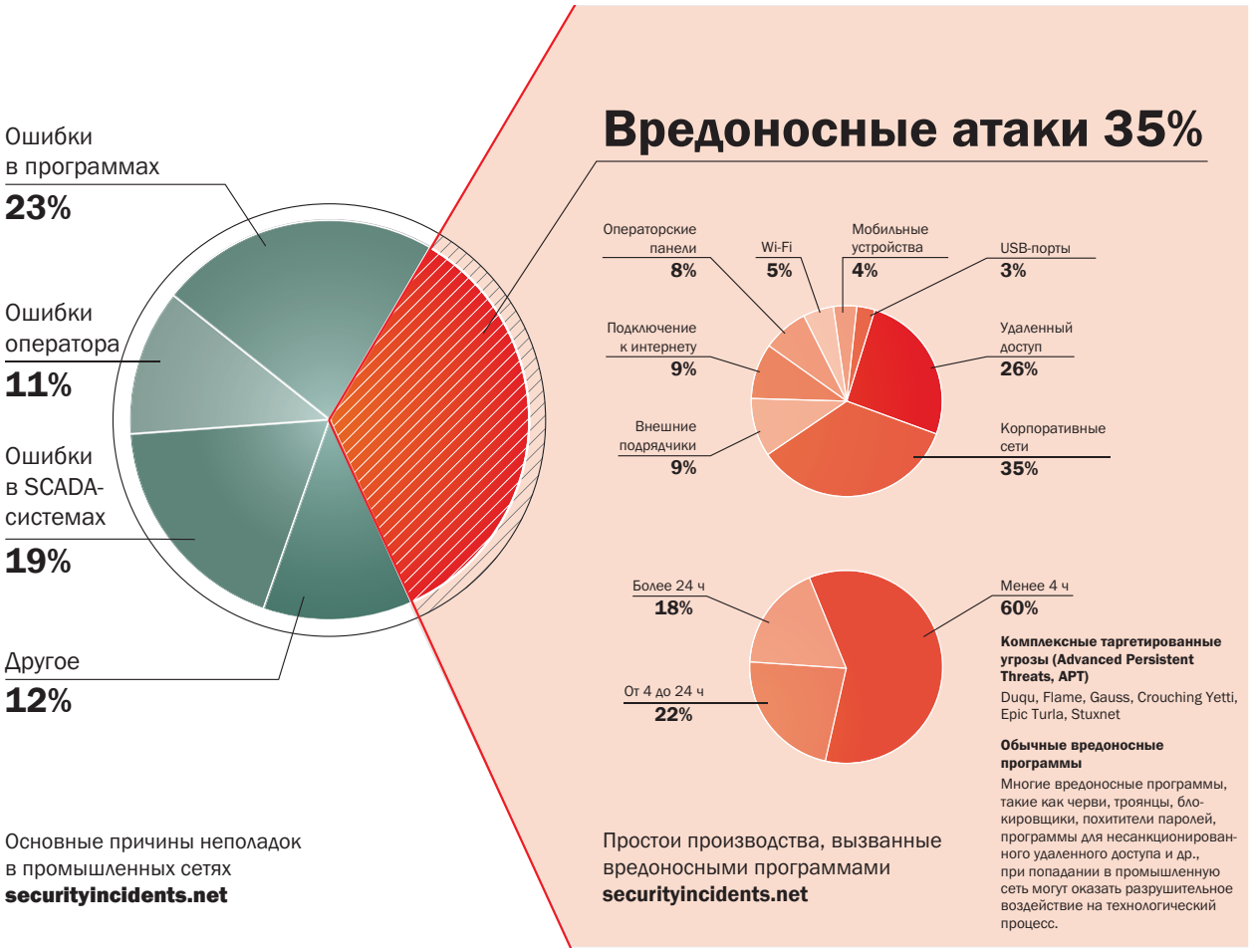
[1] http://kaspersky.ru/top3

КИБЕРБЕЗОПАСНОСТЬ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ: ТЕКУЩАЯ СИТУАЦИЯ

Последнее исследование, проведенное институтом SANS, показало, что лишь 9% IT-специалистов в промышленном секторе уверены, что безопасность их систем ни разу не нарушалась. При этом 16% заявили, что не проводят никаких регулярных процедур для обнаружения угроз, в том числе из-за того, что не хотят привлекать лишнее внимание к уязвимостям системы.

Однако жертвой атаки может стать не только ее прямая мишень. Помимо комплексных таргетированных угроз (таких как Citadel, Crouching Yeti/Havex, Miancha или BlackEnergy 2), нацеленных на промышленные компании, современные промышленные предприятия также уязвимы для угроз, изначально предназначенных для бизнес-сред.

Жертвой вредоносной атаки может стать не только ее непосредственная мишень



Основные причины неполадок в промышленных сетях **securityincidents.net**

Простои производства, вызванные вредоносными программами **securityincidents.net**

Корпоративные сети промышленных предприятий могут использоваться для проведения атак на системы управления технологическими процессами (АСУ ТП). Например, в ходе кибератаки Crouching Yetti фишинговые технологии и известные уязвимости в ПО Adobe, установленном в корпоративной сети, использовались для заражения OPC-серверов, развернутых в индустриальной сети. Злоумышленники похищали информацию из систем SCADA и выводили из строя незащищенные системы управления технологическим процессом, стирая данные на компьютерах.

Червь Conficker не предназначался специально для атаки на индустриальные системы, однако его обнаружили в медицинском оборудовании для поддержания жизнеобеспечения. Кроме того, есть основания полагать, что червь открыл двери масштабным атакам на другие промышленные системы. Червь Conficker способен вызвать перегрузку сети и остановить необходимые для функционирования всей системы процессы.

При этом традиционные методы защиты, такие как физическое разделение индустриальной и корпоративной сети или сокрытие внутреннего устройства индустриальной сети, не отвечают современным требованиям промышленной кибербезопасности, поскольку в промышленную инфраструктуру активно проникают технологии, используемые в корпоративных сетях, например, технология Ethernet.

ПРОМЫШЛЕННАЯ КИБЕРБЕЗОПАСНОСТЬ ПРЕДЪЯВЛЯЕТ ОСОБЫЕ ТРЕБОВАНИЯ

Требования к кибербезопасности для индустриальных и корпоративных сетей сильно отличаются, хотя угрозы, направленные на них, во многом совпадают. Многие стратегии IT-безопасности строятся вокруг защиты информации и опираются на принцип КЦД: **конфиденциальность**, **целостность** и **доступность** данных. Для промышленных систем приоритетом является непрерывность работы, поэтому их защита подразумевает обеспечение **доступности**, **целостности** и **конфиденциальности данных**. Из-за этой особенности промышленных систем даже самое лучшее решение для обеспечения кибербезопасности является бесполезным, если ставит под угрозу непрерывность технологических процессов.

1. ДОСТУПНОСТЬ
2. ЦЕЛОСТНОСТЬ
3. КОНФИДЕНЦИАЛЬНОСТЬ

1. КОНФИДЕНЦИАЛЬНОСТЬ
2. ЦЕЛОСТНОСТЬ
3. ДОСТУПНОСТЬ

ЦЕЛОСТНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ ПРОМЫШЛЕННОЙ КИБЕРБЕЗОПАСНОСТИ

Для обеспечения промышленной кибербезопасности необходимо обязательно использовать процессно-ориентированный подход, включающий обучение сотрудников, проведение анализа процессов, используемых технологий, состава оборудования и программного обеспечения, разработку модели угроз, выбор и развертывание специализированных защитных решений, а также техническую поддержку. Такой подход требует привлечения надежных поставщиков систем по обеспечению кибербезопасности индустриальных объектов.

«Лаборатория Касперского» придерживается целостного подхода к обеспечению промышленной кибербезопасности:

- В области промышленной кибербезопасности не существует единого решения, эффективного для всего многообразия защищаемых систем. Поэтому обеспечение промышленной кибербезопасности необходимо начинать с обследования состояния киберзащиты промышленного объекта. Затем следует провести обучение сотрудников и постепенно внедрять специализированные решения, не препятствующие нормальному течению технологических процессов. Это единственный способ обеспечить полнофункциональную защиту, не нарушая работу предприятия. Каждая минута простоя в производственном процессе приносит убытки, поэтому установка любых продуктов должна выполняться под руководством квалифицированных специалистов, готовых круглосуточно ответить на любые вопросы, связанные с функционированием средств защиты.
- В любой стратегии безопасности ключевую роль играет человеческий фактор. Поэтому важно повышать информированность сотрудников защищаемого предприятия в области кибербезопасности, в том числе руководителей высшего звена и начальников IT-отделов, а также производственных инженеров. Например, наша игровая симуляция Kaspersky Industrial Protection Simulation (KIPS) помогает оценить всю важность кибербезопасности индустриального объекта – даже тем сотрудникам, которые не занимаются техническими вопросами.
- «Лаборатория Касперского» предлагает решения, основанные на уникальных технологиях и созданные специально для индустриальных сетей. Эти решения исключительно отказоустойчивы, не препятствуют течению технологических процессов и могут работать в условиях физического разделения индустриальной и корпоративной сети. Кроме того, «Лаборатория Касперского» предлагает широкий спектр специализированных профессиональных услуг и помогает снизить риски, связанные с кибербезопасностью промышленной инфраструктуры, без непосредственной установки технических средств.

СТРАТЕГИЧЕСКИЙ ПОДХОД «ЛАБОРАТОРИИ КАСПЕРСКОГО»

УРОВЕНЬ 4
Планирование бизнеса и логистика

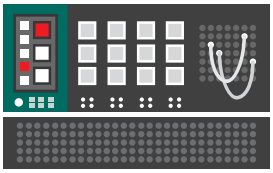
Управление всей цепочкой снабжения. Определение основного режима работы предприятия: производство, использование материалов, доставка и транспортные операции

УРОВЕНЬ 3
Управление производственными операциями

Хранение, обработка и анализ информации о продукции и оптимизация производственного процесса

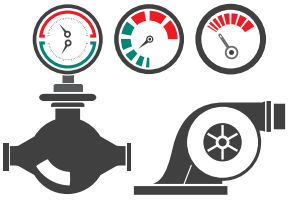
УРОВНИ 2, 1
Управление операциями
Автоматическое управление
Дискретное управление

Мониторинг, диспетчерский контроль и автоматическое управление производственным процессом



Измерение и задание параметров производственного процесса

УРОВЕНЬ 0
Физический



Физические устройства

Kaspersky Security для бизнеса и профессиональные услуги

Kaspersky Industrial CyberSecurity (KICS)

Физическая безопасность

ПРЕИМУЩЕСТВА ДЛЯ КЛИЕНТОВ

Всесторонняя защита

Решение Kaspersky Industrial CyberSecurity (KICS) охватывает все аспекты защиты промышленных предприятий. Сюда входит:

- Обучение и информирование руководителей высшего звена, инженеров и специалистов по IT-безопасности.
- Комплексная защита промышленного объекта техническими средствами: от уровня бизнес-управления до уровня диспетчерского управления.
- Интеграция системы в существующую инфраструктуру клиента, которая не требует изменений в существующих бизнес-процессах.
- Обеспечение непрерывности технологического процесса.

Специализированные средства обеспечения промышленной кибербезопасности

Каждая технологическая сеть имеет свои особенности, которые делают ее уникальной. Наше решение для обеспечения кибербезопасности промышленных объектов является масштабируемым и гибко настраиваемым, что позволяет адаптировать его к требованиям любого индустриального объекта.

Выбирая защиту «Лаборатории Касперского», промышленные предприятия получают полный доступ к интеллектуальным ресурсам и экспертным знаниям, накопленным более чем за десять лет нашей работы в сфере промышленной кибербезопасности. Ядро нашей команды, отвечающей за предоставление профессиональных услуг, составляют эксперты и технические специалисты в области защиты индустриальных объектов.

Каждая минута простоя в производственном процессе приносит убытки, поэтому установка и эксплуатация любых продуктов должны выполняться под руководством квалифицированных специалистов, готовых круглосуточно ответить на любые вопросы, связанные с работой технологий безопасности.

Помимо работы в рамках соглашений о технической поддержке, «Лаборатория Касперского» предлагает экспертное расследование инцидентов безопасности и предоставление регулярных отчетов по актуальным угрозам на основе данных, собранных специалистами нашего глобального центра исследований и анализа угроз.

Наиболее эффективная защита обеспечивается сочетанием технологий и интегрированных экспертных услуг, обучения и информирования сотрудников. «Лаборатория Касперского» предлагает промышленным предприятиям широкий спектр экспертных сервисов, в том числе:

- оценку уровня безопасности, включая тест на проникновение и разработку и реализацию политик и процедур;
- реагирование на инциденты, в том числе анализ вредоносного ПО и устранение последствий заражения;
- консультации для государственных учреждений и регулирующих органов.

Будущее промышленной кибербезопасности

Опираясь на свой многолетний опыт, «Лаборатория Касперского» активно разрабатывает технологии кибербезопасности, отвечающие требованиям промышленных объектов. Наша долгосрочная стратегия предусматривает разработку безопасной операционной системы, воплощающей наше представление о фундаментальной концепции кибербезопасности не только для индустриальных сетей, но и для любых других критически важных объектов и индустриального интернета вещей.

«Лаборатория Касперского» является доверенным партнером и поставщиком решений для обеспечения кибербезопасности для ведущих промышленных предприятий, которые много лет пользуются нашими технологиями. Компания также тесно сотрудничает с ведущими поставщиками решений для промышленной автоматизации, такими как Siemens, Schneider Electric, Emerson, Rockwell Automation и др. Взаимодействие с вендорами АСУ ТП гарантирует совместимость решений «Лаборатории Касперского» с производственными технологиями клиентов, что позволяет обеспечить надежную защиту промышленных предприятий, не подвергая риску непрерывность существующих технологических процессов.

«Лаборатория Касперского» специализируется на промышленной кибербезопасности

Согласно данным Forrester Research, сегодня игнорирование киберугроз, нацеленных на индустриальную инфраструктуру, может привести к катастрофическим последствиям. Предприятия, выбирающие поставщиков решений для обеспечения безопасности, должны «ориентироваться на наличие специализированных экспертных знаний в области промышленной автоматизации»[2]. В отчете Forrester «Лаборатория Касперского» упоминается в числе немногих поставщиков, предлагающих специализированные решения для обеспечения промышленной кибербезопасности, безукоризненно исполняющих взятые на себя обязательства и обладающих необходимым опытом и экспертными знаниями в этой сфере.

«Лаборатория Касперского» является одним из первопроходцев в области создания специализированных систем защиты промышленных предприятий и постоянно ведет исследования и разработку решений, которые успешно противостоят постоянно развивающимся угрозам для промышленных и критически важных инфраструктур.

Нарушение промышленной безопасности может иметь серьезные негативные последствия, далеко выходящие за рамки финансового ущерба и потери деловой репутации. Во многих случаях защита промышленных систем от киберугроз требует учета важных экологических, социальных и макроэкономических факторов. Количество угроз, нацеленных на критически важную промышленную инфраструктуру, растет, и вопрос правильного выбора консультанта и технологического партнера для защиты промышленных систем стоит как никогда остро. По всем вопросам, связанным с обеспечением промышленной кибербезопасности, вы можете обратиться к экспертам «Лаборатории Касперского».

[2] Forrester Research, S&R Pros Can No Longer Ignore Threats to Critical Infrastructure, by Rick Holland.

www.kaspersky.ru