Белорусско-Российский университет
Кафедра «Программное обеспечение информационных технологий»

Защита информации

Критическая инфраструктура.

Критическая информационная инфраструктура

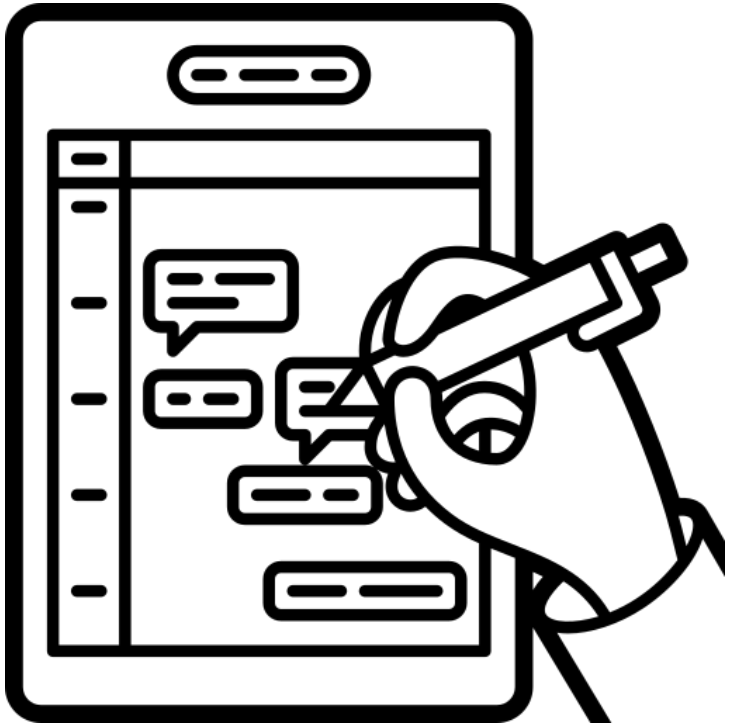
КУТУЗОВ Виктор Владимирович

Республика Беларусь, Могилев, 2024

Рекомендуемая литература по теме

Книги

- **ВНУТРЕННЯЯ БЕЗОПАСНОСТЬ КИИ**
- Объекты КИИ – лакомый кусок для злоумышленников, по данным МВД, только за первое полугодие 2020 года на них было совершено более миллиарда кибератак. Не меньше опасности несут утечки информации, саботаж и мошенничество со стороны сотрудников – они имеют легитимный доступ к системам КИИ, поэтому контроль внутренних злоупотреблений приобретает особенное значение. Важно знать, какие существуют стандарты такого контроля и какие инструменты его обеспечивают.
- В этой книге:
  - Разбирается, что такое КИИ и кто является ее субъектами.
  - Рассказывается, какие существуют требования к защите КИИ от внутренних угроз.
  - Даются рекомендации, какими средствами можно выполнить эти требования.
  - Рассказываются, как можно дополнительно усилить защиту.
- https://static.searchinform.ru/uploads/sites/1/2022/05/bk-kii.pdf



Критическая инфраструктура

Критическая инфраструктура

Критическая инфраструктура

- **Одна из самых сильных сторон нашего современного развитого общества является также одним из самых главных его недостатко**в. В нынешнем взаимосвязанном мире развитые и высокотехнологичные социумы сильно зависят от работы ряда служб и сервисов, которые в настоящее время стали жизненно необходимыми.
- Определенная инфраструктура обеспечивает нормальную работу основных служб и производственных систем в любом обществе. Поэтому сбой в их работе в силу естественных причин, технических неполадок или преднамеренных действий может иметь серьезные последствия для поставки ресурсов или работы критических служб, не говоря уже об угрозе безопасности.
- В последние годы во всем мире неуклонно растет уровень кибер-преступности.
- Развитие Интернета и цифровая трансформация общества представляет собой "палку о двух концов", т.к. все это дает определенные возможности для преступников. Но что может произойти, если критически важные сети станут целью для преступного сообщества?

Важные секторы и критическая инфраструктура

- **Защита критической инфраструктуры является важной проблемой для всех стран.** Высокий уровень развития современного общества во многом зависит от ряда основных и важных услуг, в значительной степени оказываемых частным бизнесом.
- Инфраструктура обеспечивает нормальную работу крайне важных для развития государства служб и систем:
  - правительственные органы,
  - водоснабжение,
  - финансовые и налоговые системы,
  - энергетика,
  - космос,
  - атомные электростанции и
  - транспортные системы,
  - крупные производственные предприятия.

Критическая инфраструктура

Здравоохранение

Банки и финансовые организации

Горнодобывающая промышленность

Наука

Энергетика и топливно-энергетический комплекс

Транспорт

Металлургическая промышленность

Сфера атомной энергии

Химическая промышленность

Связь

Ракетно-космическая промышленность

Оборонная промышленность

Важные секторы и критическая инфраструктура

- **К критически важной инфраструктуре относятся объекты**, сети, службы и системы, сбой в работе которых в любом случае отразится на здоровье, безопасности и благосостоянии граждан страны.

- Гарантированное предоставление жизненно важных услуг в условиях новых угроз - это не только ответственность государственных органов, но также и частных компаний на национальном и международном уровнях.

Что такое КИИ?

- **На сухом юридическом языке критическая информационная инфраструктура (КИИ)** – это информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ, а также сети электросвязи, используемые для организации их взаимодействия.
- Говоря проще, это все элементы IT, которые обеспечивают бесперебойную работу важнейших предприятий и организаций и в которых обрабатывается самая чувствительная информация.

КИ в Республике Беларусь

- **Критическая инфраструктура (КИ)** – инфраструктура, являющаяся жизненно важной для государства, отказ или разрушение которой может оказать существенное отрицательное воздействие на национальную безопасность.

- **Объект информатизации** – средства электронной вычислительной техники вместе с ПО, в том числе автоматизированных систем различного уровня и назначения, вычислительные сети и центры, автономные стационарные и персональные электронные вычислительные машины, используемы для обработки информации.

КИ в Республике Беларусь

- **Критически важный объект информатизации**: объект информатизации, обеспечивающий:
  - функционирование экологически опасных и (или) социально значимых производств и (или) технологических процессов, нарушение штатного режима которых может привести к чрезвычайной ситуации техногенного характера;
  - осуществляет функции информационной системы, нарушение (прекращение) функционирования которой может привести к значительным негативным последствиям для национальной безопасности в политической, экономической, социальной, информационной, экологической, иных сферах;
  - обеспечивает предоставление значительного объема информационных услуг, частичное или полное прекращение оказания, которых может привести к значительным негативным последствиям для национальной безопасности в политической, экономической, социальной, информационной, экологической, иных сферах

СТБ 34.101.30-2017 Информационные технологии. Методы и средства безопасности. Информационные системы. Классификация

КИИ в Российской Федерации

- Под **критической информационной инфраструктурой** РФ (КИИ) подразумевается **совокупность автоматизированных систем управления производственными и технологическими процессами критически важных объектов РФ** и обеспечивающих их взаимодействие информационно-телекоммуникационных сетей, а также ИТ-систем и сетей связи, предназначенных для решения задач государственного управления, обеспечения обороноспособности, безопасности и правопорядка.

КИ В США

- **Критическая инфраструктура (КИ)** – системы и активы, физические или виртуальные, столь жизненно-важные для Соединенных Штатов, что приостановка их работы или их разрушение окажет разрушительные последствия для безопасности, национальной экономической безопасности, национальной системы общественного здравоохранения, системы общественной безопасности или нескольких из этих систем одновременно

КИ и КИИ в Европейском Союзе

- **КИ** – физические и ИТ-инфраструктуры, сети, сервисы и активы, нарушение функционирования или уничтожение которых оказало бы серьезное влияние на состояние здоровья, безопасность и экономическое благополучие граждан, либо эффективную работу правительств стран-членов ЕС.

- **КИИ** – системы ИКТ, которые являются КИ сами по себе, либо являются необходимыми для функционирования других КИ (включая телекоммуникации, компьютеры и ПО, Интернет, спутники и т.д.)

Выделяемые отрасли и категории КИ

Государство, Организация, Объединение / Выделяемые отрасли и категории КИ	Германия	США	Япония	КНР	ОЭСР	ЕС	Армения	Беларусь	Казахстан	Киргизская республика	РФ
Топливно-энергетический комплекс	+	+	+	+	+	+		+			+
ИТ, телекоммуникации, связь	+	+	+		+	+		+			+
Транспорт, перевозки	+	+	+	+	+	+					+
Водоснабжения	+	+	+			+					
Питание, продовольствие, сельское хозяйство	+	+				+					
Финансово-экономическая и банковская деятельность	+	+	+	+		+		+	+		+
Коммуникации		+		+	+						
Химическая и ядерная промышленность		+	+								+
Сектор государственных учреждений		+	+	+	+	+		+	+		
Медицина и здравоохранение	+	+	+		+	+		+			+
Промышленное производство и коммерция		+		+					+		+
Национальная оборона, ВПК		+	+	+				+			+
Сфера охраны природных ресурсов и окружающей среды								+			
Наука								+			+

Регулирование КИ

Государство, Организация	**Регулятор**
Германия	Федеральное управление по информационной безопасности
США	**Министерство внутренней безопасности**
Япония	Профильное министерство по каждой отрасли
КНР	Госсовет и его профильные департаменты
Организация экономического сотрудничества и развития	Совет ОЭСР
ЕС	**Европейского агентства по сетевой и информационной безопасности**
Республика Беларусь	**Совет Министров Республики Беларусь, Оперативно-аналитический центр при Президенте Республики Беларусь**
Казахстан	Правительство Республики Казахстан
РФ	**Минкомсвязи России, ФСБ России, ФСТЭК**

Критическая инфраструктура

- В последние годы западные специалисты уделяют особое внимание оценке воздействия на жизненно важные объекты своих стран и возможных последствий этих воздействий для политической, экономической, экологической и других сфер деятельности государства.
- Очевидно, что в условиях современного чрезвычайно интенсивного развития инфраструктуры ведущих зарубежных стран существует множество критически важных объектов, таких, например, как крупные гидротехнические сооружения, нефте-, газо-, продуктопроводы, сети АЭС, пункты хранения стратегических запасов нефти и газа, вредные химические производства, транспортные узлы, аэродромы и т.п., выведение из строя которых может привести к непредсказуемым тяжелым и даже катастрофическим последствиям.

Критическая инфраструктура

- В связи с этим в Соединенных Штатах Америки, Франции, Германии, Японии и других странах были проведены обширные исследования по выявлению таких объектов на территории США, Канады, Европы, представляющих угрозу для нормальной жизнедеятельности рассматриваемых стран в случае воздействия по ним безъядерного высокоточного оружия или в результате террористических (диверсионных) актов. Также прорабатывались варианты техногенных катастроф или разрушительных стихийных бедствий. В перечень выявленных критически важных объектов не включены традиционные типы военных объектов — ракетные базы и полигоны, авиационные базы, органы высшего военного управления, так как, по оценкам исследователей, эти объекты имеют достаточно высокую степень защищенности и практически являются малоуязвимыми от воздействия обычных средств поражения. Кроме того, даже вывод из строя подобных объектов существенно не нарушит системы жизнеобеспечения государства и его управляемость.

Критическая инфраструктура

- **Главную угрозу для жизнедеятельности страны представляет выведение из строя объектов, приводящее к нарушению транспортных и энергетических систем, водоснабжения и др. в масштабах страны или отдельных районов.** По результатам исследования на территории США и Канады выделено около 2 300 подобных объектов, в Германии — более 650, Франции — около 500, в Японии — до 700. При этом отмечается, что они обладают относительно низкой защищенностью и имеют большое количество уязвимых точек «несанкционированного доступа», воздействие на которые может привести фактически к полному параличу систем жизнедеятельности государства.
- Защита критически важных объектов и их совокупности, которую принято называть критически важной инфраструктурой, или критической инфраструктурой, представляет собой одну из наиболее важных задач обеспечения национальной безопасности любой страны. Защита критически важных объектов включает проведение мероприятий, которые должны обеспечить их сохранение в случае различных воздействий природного или техногенного характера.

Критическая инфраструктура

- **Вопросы безопасности критических инфраструктур в последнее время активно развиваются во всем мире.**
- В рамках работ, проводимых в этой области **в Республике Беларусь**, Указом Президента Республики Беларусь от 16.04.2013 № 196 «О некоторых мерах по совершенствованию защиты информации» (в редакции Указа Президента Республики Беларусь от 09.12.2019 № 449 «О совершенствовании государственного регулирования в области защиты информации») утверждено Положение о порядке отнесения объектов информатизации к критически важным объектам информатизации.
- Указом определено понятие «критически важный объект информатизации» следующим образом: «**критически важный объект информатизации** – объект информатизации, который на основании критериев отнесения объектов информатизации к критически важным объектам информатизации и показателей уровня вероятного ущерба национальным интересам Республики Беларусь в политической, экономической, социальной, информационной, экологической и иных сферах включен в Государственный реестр критически важных объектов информатизации».

Критическая инфраструктура

- **Оперативно-аналитический центр при Президенте Республики Беларусь в пределах своих полномочий:**
  - определяет порядок технической и криптографической защиты информации, обрабатываемой на критически важных объектах информатизации, в том числе порядок проведения аудита систем информационной безопасности критически важных объектов информатизации;
  - осуществляет ведение Государственного реестра критически важных объектов информатизации, а также предоставление сведений из него;
  - выносит письменные требования (предписания) об устранении организациями выявленных нарушений Положения о технической и криптографической защите информации, утвержденного Указом Президента Республики Беларусь от 16.04.2013 № 196 «О некоторых мерах по совершенствованию защиты информации» (в редакции Указа Президента Республики Беларусь от 09.12.2019 № 449 «О совершенствовании государственного регулирования в области защиты информации»), и иных нормативных правовых актов в сфере технической и криптографической защиты информации и (или) приостановление (прекращение) функционирования критически важного объекта информатизации;
  - разрабатывает проекты актов законодательства, в том числе обязательных для соблюдения технических нормативных правовых актов, и принимает такие акты по вопросам технической и криптографической защиты информации;
  - осуществляет иные полномочия в сфере технической и криптографической защиты информации в соответствии Положением о технической и криптографической защите информации, утвержденным Указом Президента Республики Беларусь от 16.04.2013 № 196 «О некоторых мерах по совершенствованию защиты информации» (в редакции Указа Президента Республики Беларусь от 09.12.2019 № 449 «О совершенствовании государственного регулирования в области защиты информации»), и иными законодательными актами.

Критически важные объекты информатизации Республика Беларусь

- **Нормативные правовые акты по Критически важным объектам информатизации в Республике Беларусь**
  - **Указ** Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации» https://oac.gov.by/public/content/files/files/law/decrees-rb/2013-196.pdf
  - **Приказ** Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 65 "О показателях уровня вероятного ущерба национальным интересам Республики Беларусь" https://oac.gov.by/public/content/files/files/law/prikaz-oac/2020%20-%2065.pdf
  - **Приказ** Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 "О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449"
  - https://oac.gov.by/public/content/files/files/law/prikaz-oac/2020%20-%2066.pdf

Объекты КИИ в РФ

Здравоохранение

Банковская сфера и иные сферы финансового рынка

Топливно-энергетический комплекс

Атомная промышленность

Военно-промышленный комплекс

ОБЪЕКТЫ КИИ:

- ✓ информационные системы
- ✓ телекоммуникационные сети
- ✓ автоматизированные системы управления технологическими процессами

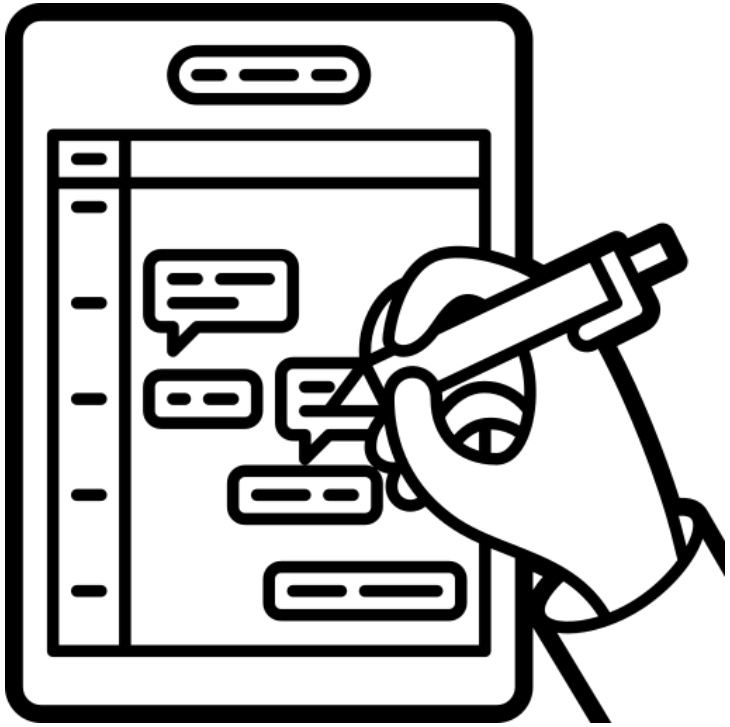
Ракетно-космическая промышленность

Горнодобывающая промышленность

Металлургическая и химическая промышленность

Наука, транспорт, связь

ЮЛ и ИП которые взаимодействуют с системами КИИ



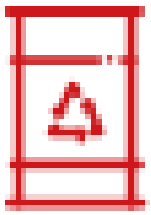
История атак на критическую инфраструктуру

История атак на КИ

- В целом, общественность, хоть и допускает определенные риски, но все же считает, что в реальности речь может идти о небольшом количестве кибератак на критическую инфраструктуру.
- К сожалению, все намного печальнее, известно сотни задокументированных случаев таких атак во всем мире. Атаки на такие сети ведутся уже десятилетия.

Сибирский нефтепровод

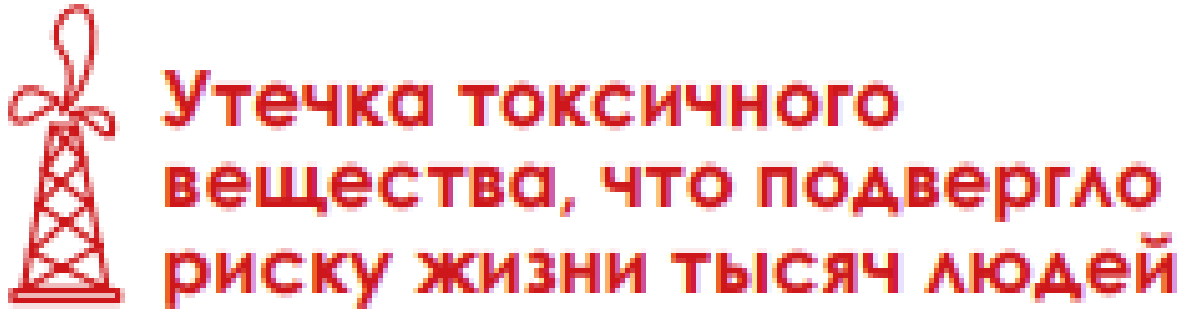
- Термин "Интернет" приходит на ум всякий раз. когда мы думаем о кибер-атаках на критическую инфраструктуру.
- **Но первая подобная кибер-атака произошла еще до появления Интернета - в 1982 году.** Тогда группа хакеров смогла установить троян в SCADA-систему, которая контролировала работу сибирского нефтепровода, что привело к мощному взрыву. Атака была организована ЦРУ, хотя об этом не было известно до 2004 года, когда бывший секретарь Министерства обороны США и советник Р. Рейгана Томас Рид опубликовал свою книгу “At the Abyss: An Insider's History of the Cold War".



Взрыв сибирского нефтепровода был спровоцирован ЦРУ

Chevron

- Следующий инцидент произошел спустя десять лет, в **1992** году, когда был уволен рабочий нефтяной компании **Chevron**, который взломал компьютеры в офисах компании в Нью-Йорке и Сан-Хосе, отвечавшие за системы предупреждений, перенастроив их на аварию после запуска системы. Этот саботаж не был раскрыт до тех пор, пока не произошло утечки ядовитого вещества в Редмонде (штат Калифорния), при этом система не выдала соответствующих предупреждений. В результате тысячи людей были подвержены огромному риску в течение 10 часов, пока система была отключена.



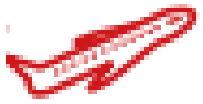
Salt River Project

- В августе **1994** года Лейн Джаррет Дэвис сумел взломать сеть **Salt River Project**, получив доступ к информации и удалив файлы из системы, отвечающей за мониторинг и подачу воды и электричества. Он также сумел получить доступ к персональным и финансовым данным клиентов и сотрудников компании.

Удаление файлов из системы, отвечающей за мониторинг и подачу воды и электричества

Аэропорт Worcester

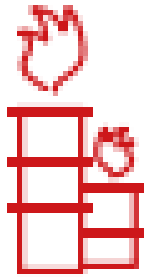
- Другие ключевые секторы также пострадали от направленных атак. 10 марта **1997** года хакер проник в систему управления, используемую для коммуникаций системы контроля воздушного движения в Вустере (США, штат Массачусетс), вызвав сбой системы, которая отключило телефонную связь на шесть часов. Особенно это повлияло на телефонную систему башни управления, пожарной службы аэропорта и авиакомпаний, базирующихся в аэропорту.



Сбой системы, повлиявший на телефонную систему башни управления, пожарной службы аэропорта и авиакомпаний, базирующихся в аэропорту, в течение 6 часов

Газпром

- В **1999** году хакеры нарушили работу систем безопасности российского энергетического гиганта - компании "**Газпром**". С помощью инсайдера они использовали троян, чтобы иметь возможность управлять SCADA-системой, контролирующей подачу газа. К счастью, это не привело к серьезным последствиям, а нормальная работа системы была восстановлена в кратчайшие сроки.



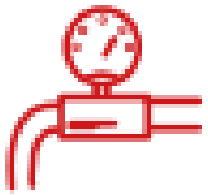
Хакеры смогли управлять в Газпроме системой, контролирующей подачу газа

Maroochy Water System

- Бывший сотрудник **Maroochy Water System** (Австралия) получил два года тюреллного заключения за взлом в **2000** году системы управления водоснабжением, в результате чего миллионы литров сточных вод пополи в ближайшую реку, что привело также к затоплению местной гостиницы.

Газоперерабатывающий завод

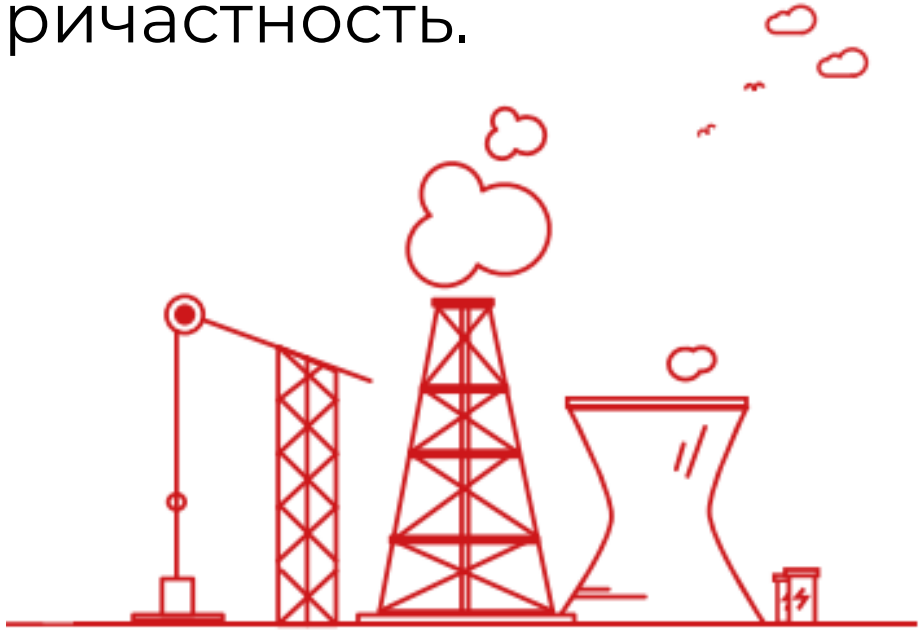
- **Газоперерабатывающий завод**, построенный одной американской компанией, также подвергся атаке в **2001** году. 6-месячное расследование показало, что атака была проведена одним из поставщиков, который для сокрытия сделанной им ошибки, решил отвлечь внимание, взломав три ПК компании и вызвав отключение подачи газа для домашних и корпоративных клиентов в одной из европейских стран.

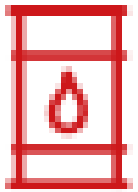


Атака привела к отключению газа у домашних и корпоративных клиентов в одной из стран Европы

PDVSA

- В декабре **2002** года нефтяная компания **PDVSA** из Венесуэлы подверглась атаке, в результате которой добыча нефти сократилась с 3 млн. до 370 тыс. баррелей в сутки. Во время атаки было взломано несколько корпоративных компьютеров. Она была проведена во время забастовки сотрудников предприятия, чтобы можно было предположить их причастность.

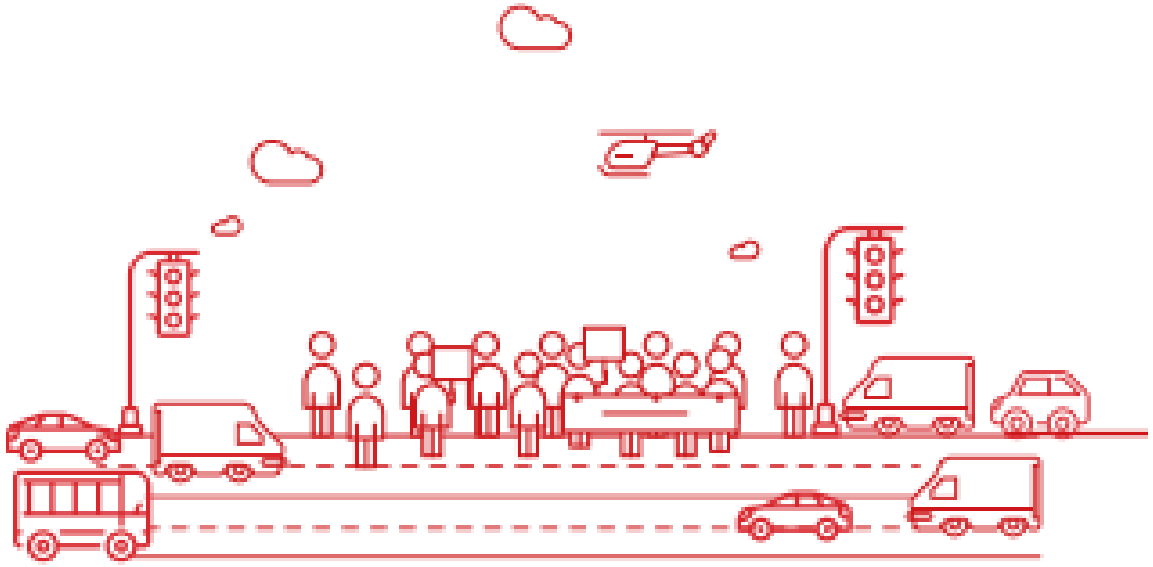


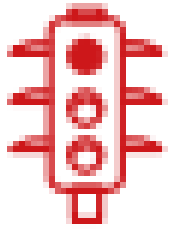


Атака сократила добычу нефти с 3 млн. до 370 тыс. баррелей в сутки

Светофоры в Лос-Анджелесе

- В **2006** году два инженера по организации дорожного движения в Лос-Анджелесе взломали **городские светофоры** в знак протеста. Им удалось изменить программу работы некоторых светофоров, размещенных на важных участках, после чего они стали гореть красным цветом, что привело к серьезным пробкам.

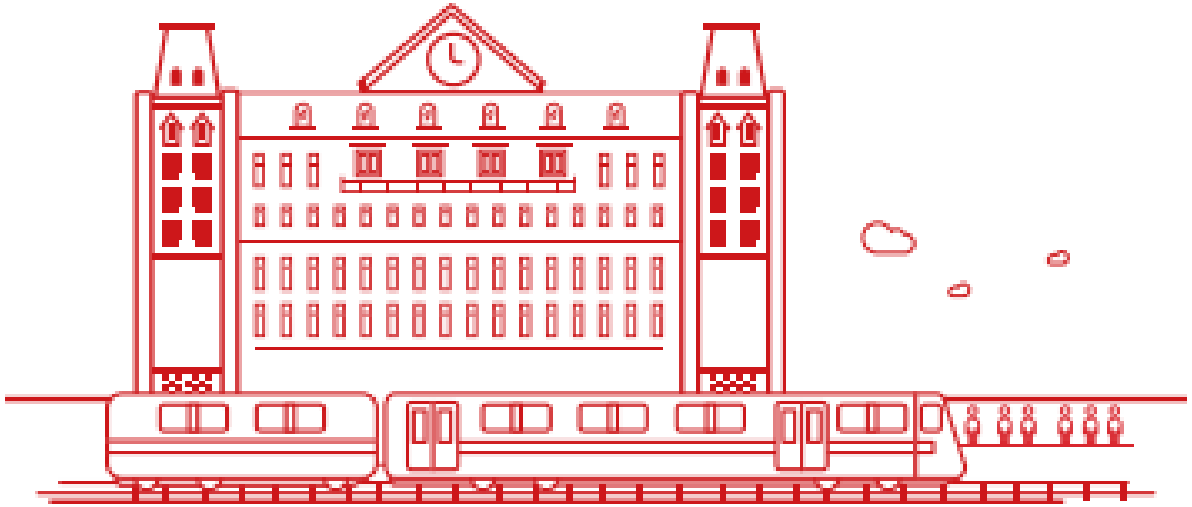


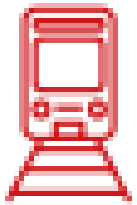


Хакерская атака привела к серьезным пробкам

Трамвайная сеть в Лодзе

- В **2008** году 14-летний студент взломал системы трамвайной сети в польском городе Лодзь, в результате чего 4 трамвая сошли с путей, а 12 человек получили травмы. Студент создал инфракрасный пульт дистанционного управления, как у телевизоров, с помощью которого он смог контролировать трамвайные перекрестки.

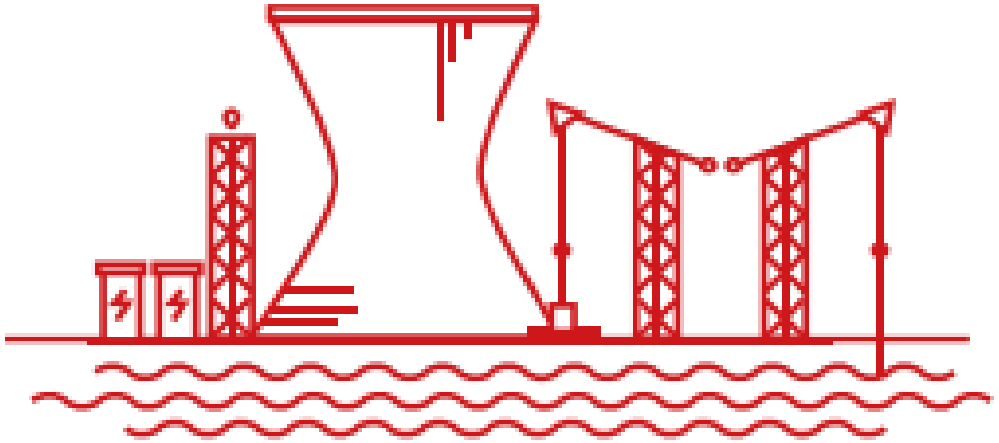


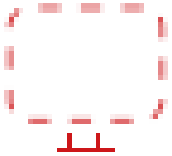


В результате кибер-атаки 4 трамвая сошли с рельсов, 12 человек получили травмы

Saudi Aramco

- В **2012** году крупнейшая нефтяная компания в мире **Saudi Aramco** стала жертвой направленной атаки на свои офисы. Хакеры получили доступ к сети благодаря атаке на одного из сотрудников компании, через которого смогли получить доступ к 30 000 компьютеров в сети. В какой-то момент хакерам удалось удалить содержимое всех компьютеров, в то время как на экранах показывался горящий американский флаг. Ответственность за атаку взяла на себя группа хакеров, называвших себя "Меч правосудия".

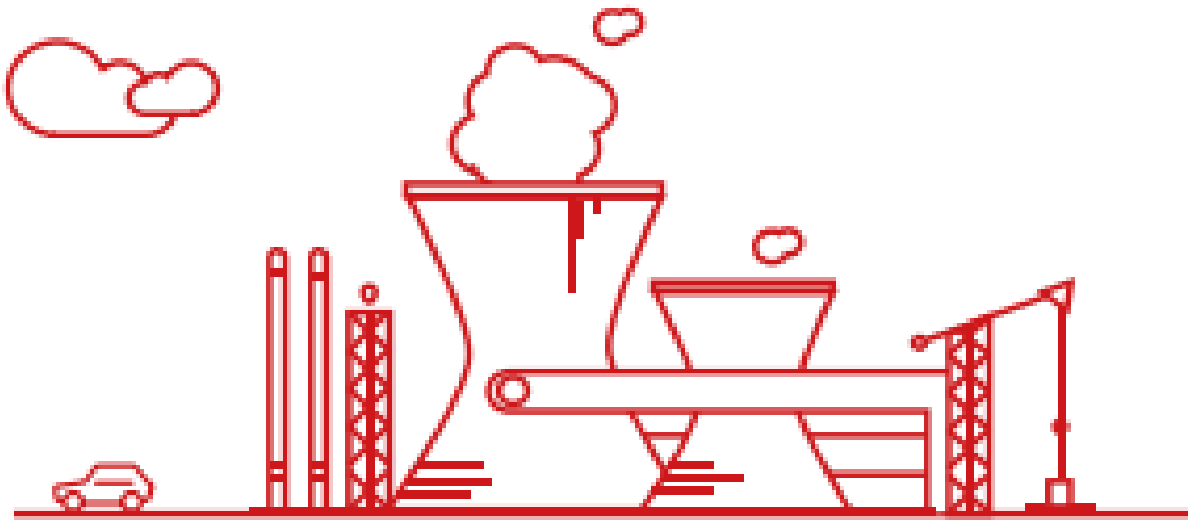


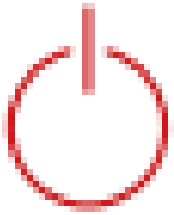


Удаление содержимого с каждого компьютера, в то время как на экранах показывался горящий американский флаг

Ram Gas

- Всего лишь через две недели после атаки на Saudi Aramco, катарская компания RamGas, второй в мире производитель сжиженного природного газа, был атакован той же вредоносной программой, которая использовалась для атаки на нефтяную компанию из Саудовской Аравии. В течении нескольких дней не работали внутренняя корпоративная сеть и веб-сайт компании.

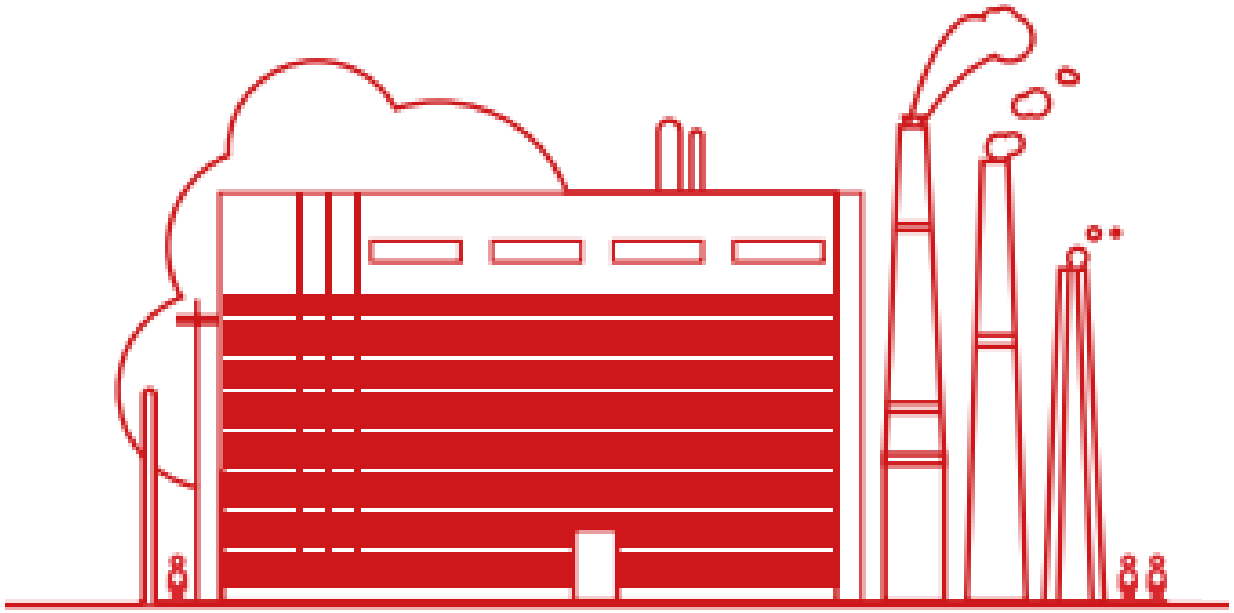


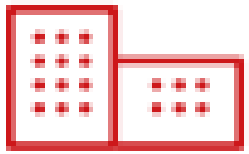


Хакерская атака обрушила корпоративную внутреннюю сеть и веб-сайт компании

Металлургический завод в Германии

- В **2014** году в Германии жертвой атаки стал один из металлургических заводов. Используя социальную инженерию, хакеры сумели получить доступ к компьютеру одного сотрудника, с которого они смогли получить доступ к внутренней сети системы управления. В результате этого стало невозможным выключить одну из домен, что нанесло огромный ущерб предприятию.

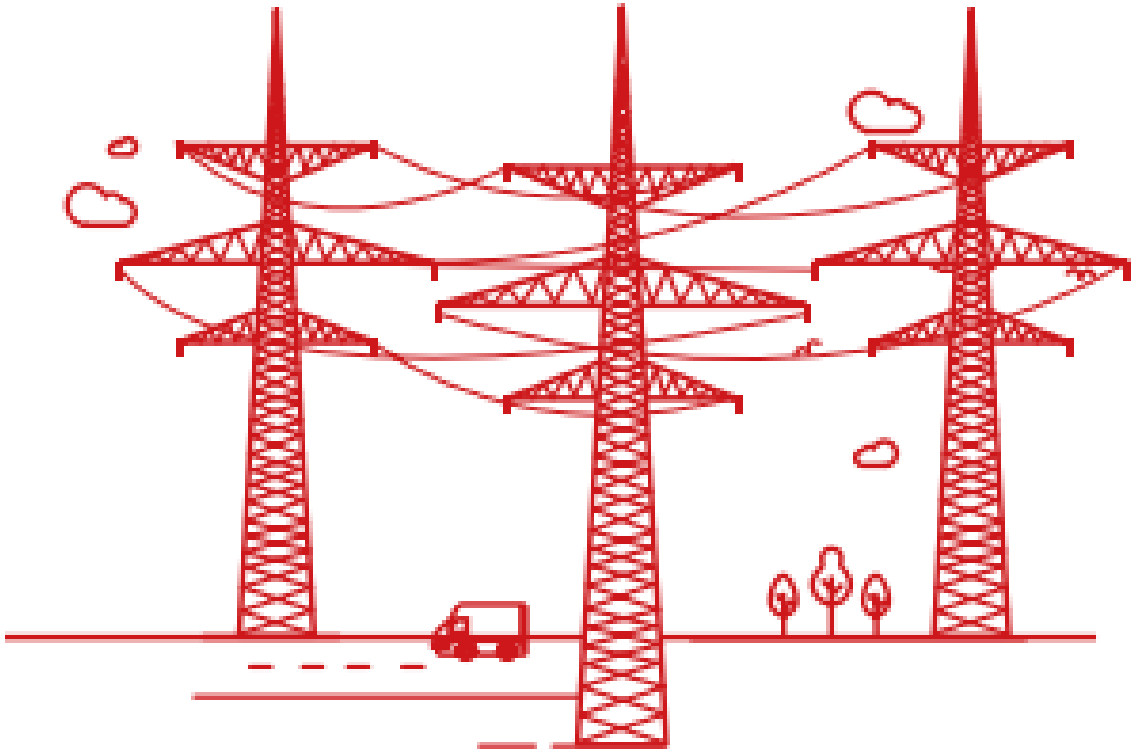




Кибер-атака нанесла огромный ущерб металлургическому заводу

Электросеть Украины

- В конце **2015** года Украина подверглась кибер-атаке на свою национальную электросеть, в результате чего свыше 600000 жителей остались без электричества.



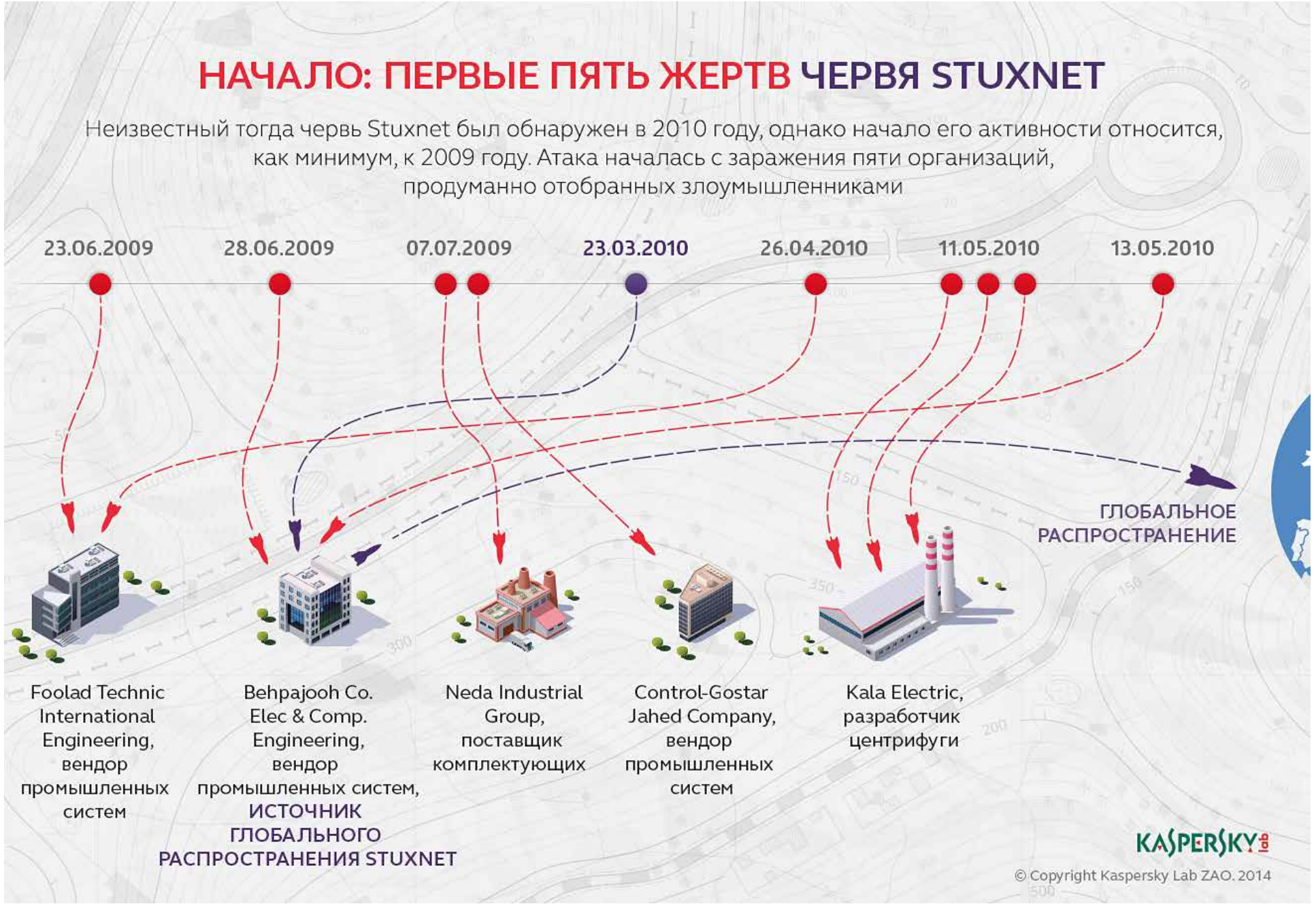
Кибер-атака оставила без электроэнергии свыше 600 0000жителей Украины

Первая в истории кибер-атака против Интернет-инфраструктуры

- Несмотря на длинный список инцидентов, первая в истории кибер-атака на Интернет-инфраструктуру произошла 27 апреля **2007 года, когда в Эстонии ряд атак обрушил сайты различных организаций**, включая парламент, различные министерства, банки, газеты и различные СМИ и т.д.
- Впрочем, атака также была направлена на определенные непубличные адреса, включая национальную систему обработки финансовых ордеров и телекоммуникационные службы. Урмас Поет, министр иностранных дел Эстонии, публично обвинил российские власти в причастности к данным атакам, хотя он не смог предоставить каких-либо доказательств этому.

Самый известный случай кибер-атаки на критическую инфраструктуру: Stuxnet

- В **2008** году мы стали свидетелями одного из самых печально известных в истории случаев кибер-атак на критические инфраструктуры: **Stuxnet**. **Сейчас уже известно, что это была скоординированная атака израильских и американских спецслужб, направленная на срыв ядерной программы Ирана.**
- **Они создали червя, который заразил компьютеры, управляющие урановыми центрифугами на иранском заводе в Натанзе**, в результате чего они стали работать на полной скорости, в то время как инженеры на своих мониторах наблюдали нормальный режим работы. Это нанесло физический ущерб всем урановым центрифугам на заводе. **После этого случая общественность узнала о подобного рода угрозах.**


НАЧАЛО: ПЕРВЫЕ ПЯТЬ ЖЕРТВ ЧЕРВЯ STUXNET
Неизвестный тогда червь Stuxnet был обнаружен в 2010 году, однако начало его активности относится, как минимум, к 2009 году. Атака началась с заражения пяти организаций, продуманно отобранных злоумышленниками
23.06.2009
28.06.2009
07.07.2009
23.03.2010
26.04.2010
11.05.2010
13.05.2010
ГЛОБАЛЬНОЕ РАСПРОСТРАНЕНИЕ
Foolad Technic International Engineering, вендор промышленных систем
Behpajooh Co. Elec & Comp. Engineering, вендор промышленных систем, ИСТОЧНИК ГЛОБАЛЬНОГО РАСПРОСТРАНЕНИЯ STUXNET
Neda Industrial Group, поставщик комплектующих
Control-Gostar Jahed Company, вендор промышленных систем
Kala Electric, разработчик центрифуги
KASPERSKY lab
© Copyright Kaspersky Lab ZAO. 2014

Атаки

- Атаки в других компаниях также затрагивали объекты критической инфраструктуры
- Помимо атак, специально осуществляемых для причинения ущерба подобного типа инфраструктуры, атаки, подобные тем, с которыми сталкиваются другие компании, также негативно влияют на критические объекты, а последствия иногда были такими же серьезными. **Подобные проблемы в основном начались в конце прошлого десятилетия, т.к. сетевые черви стали распространяться в Сети сами по себе.**

Атаки

- **Например**, случай на ведущей **в США** фабрике по выпуску продуктов питания, когда **вирусная инфекция** нанесла ущерб, измеряемый тысячами долларов. Один сотрудник удаленно подключился с домашнего ПК, который был заражен вирусом **Nimda**. Как только он вошел в корпоративную сеть, червь распространился на все системы управления.

Атаки

- В **2003** году **нефтяная компания из США пострадала от червя SQLSlammer**, который проник во внутреннюю сеть. Хотя это не привело к остановке производства, но он повлиял на внутренние коммуникации. Пришлось потратить несколько дней для полного удаления червя из сети и обновления систем для предотвращения дальнейших атак. Кстати, данный червь был одним из самых разрушительных для компаний.

Атаки

- В том же **2003** году один из крупнейших автопроизводителей в США также пострадал от атаки червем **SQLSlammer**, который мгновенно распространился на его 17 заводах. Общий ущерб для компании составил 150 млн. долларов США. Хотя патч уже был доступен на протяжении шести месяцев, ИТ-менеджеры компании до сих пор не установили его.
- В **2005** году **в Японии** компьютер сотрудника компании **Mitsubishi Electric** был заражен вредоносной программой, что привело к утечке конфиденциальных инспекционных документов о двух атомных электростанциях, принадлежащих данной компании.

Атаки

- В **2013** году были заражены 200 компьютеров Департамента автомобильных дорог и транспорта в округе Кук (штат Иллинойс, США). Эти системы отвечали за поддержание сотни километров дорог в пригороде Чикаго. В результате атаки пришлось отключать сеть на 9 дней, чтобы вылечить все компьютеры.

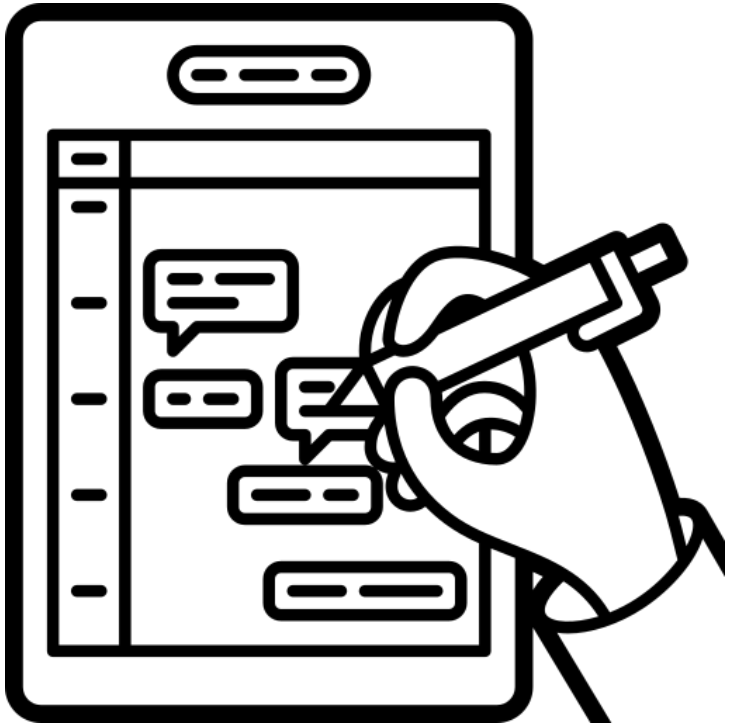
Новая волна атак шифровальщиков поразила до 1500 предприятий во всем мире

- Все началось **2 июля 2021** , когда злоумышленники нацелились на популярное программное обеспечение для удаленного управления и мониторинга (RMM), производимое компанией Kaseya (Флорида, США). Воспользовавшись недостатком в программном обеспечении Kaseya VSA, хакеры получили доступ к системе RMM и смогли использовать ее для установки программ-шифровальщиков в некоторых сетях клиентов Kaseya. Поскольку эти клиенты сами являются поставщиками управляемых систем (MSP), шифровальщики также заразили их клиентов, а это сотни предприятий по всему миру. Компания Kaseya сообщила, что атака не затронула пользователей их SaaS-версии, а только тех клиентов, кто использует локальную версию решения Kaseya VSA. Злоумышленники просят выкуп в размере 70 миллионов долларов США выкупа за восстановление всех жертв.
- **Основной фокус атаки, по-видимому, был направлен на американских MSP, но кибер-атака быстро распространилась и на международном уровне, угрожая другим типам компаний. Kaseya утверждает, что около 1500 предприятий и организаций подтвердили наличие шифровальщика**, но это может косвенно повлиять на работу и других компаний. Kaseya еще в пятницу посоветовала всем своим клиентам перевести локальные серверы VSA в автономный режим, а по состоянию на вторник пока что не дала им разрешения вернуться в онлайн-режим. В компании заверили, что готовят патч для исправления уязвимости, использованной для атаки, и планируют выпустить его в ближайшее время.

«Триада угроз» международной информационной безопасности

Атаки

Даже этот не полный список инцидентов показывает, что опасность кибер-атак на критические инфраструктуры вполне реальна, и сегодня правительства всех стран знают об этих рисках и стараются их по максимуму минимизировать.



Меры защиты

Эффективные меры

1. **Проверка систем на уязвимости**, особенно тех систем, на которых уже были зафиксированы дыры безопасности и они были известны в течение некоторого времени.

2. **Адекватный мониторинг сетей**, используемых для контроля таких объектов критической инфраструктуры, и при необходимости их полная изоляция от внешних соединений, что позволит обнаруживать внешние атаки и предотвращать доступ к системам, управляемым из внутренней сети.

Эффективные меры

3. **Контроль над съемными устройствами**, что важно в любой инфраструктуре не только потому, что они являются направлением таких атак, как в случае с Stuxnet. При защите таких объектов критической инфраструктуры крайне важно, чтобы вредоносные программы не проникали во внутреннюю сеть через съемные устройства, которые также могут использоваться и для кражи конфиденциальной информации.

Эффективные меры

4. **Мониторинг ПК**, к которым подключены программируемые логические контроллеры (или PLC). Эти подключенные к Интернету устройства являются наиболее чувствительными, т.к они могут предоставлять хакерам доступ к критически важным системам управления. Даже если они не смогут получить контроль над системой, они смогут получить ценную информацию для других направлений атаки.

Защита информации

Тема: Критическая инфраструктура.
Критическая информационная инфраструктура

Благодарю за внимание

КУТУЗОВ Виктор Владимирович

Белорусско-Российский университет, Кафедра «Программное обеспечение информационных технологий»
Республика Беларусь, Могилев, 2024

Список использованных источников

1. Рабочая программа дисциплины «Защита информации» / Кутузов В.В. – Могилев : Белорусско-Российский университет, 2019
2. Фотографии и картинки взяты с сайтов Яндекс.Картинки и Гугл.Картинки, иконки с flaticon.com
3. Отчет о выполнении первого этапа научно-исследовательской работы для официального использования Евразийской экономической комиссией по теме: «Рекомендации по взаимодействию государств-членов ЕАЭС в области регулирования, развития и обеспечения безопасности критической цифровой инфраструктуры с перспективой до 2025 года» (промежуточный), 2018 http://www.eurasiancommission.org/ru/NIR/Lists/List/Attachments/209/Отчет%20о%20НИР%20ЕЭК%20ОБИ%20ЦИ.%20Этап%201.pdf
4. Tadviser - Критическая инфраструктура России https://www.tadviser.ru/index.php/Статья:Критическая_инфраструктура_России
5. Критически важные объекты информатизации в РБ. Общие сведения https://oac.gov.by/activity/critical-information-objects/technical-and-cryptographic-information-protection/general-information-kvoi
6. Указ Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации» https://oac.gov.by/public/content/files/files/law/decrees-rb/2013-196.pdf
7. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 65 "О показателях уровня вероятного ущерба национальным интересам Республики Беларусь" https://oac.gov.by/public/content/files/files/law/prikaz-oac/2020%20-%2065.pdf

Список использованных источников

8. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 "О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449" https://oac.gov.by/public/content/files/files/law/prikaz-oac/2020%20-%2066.pdf
9. Panda Whitepaper. Критическая инфраструктура https://www.cloudav.ru/upload/iblock/447/PAD_PAD360%20-%20Whitepaper%20-%20Критические%20инфраструктуры.pdf
10. Новая волна атак шифровальщиков поразила до 1500 предприятий во всем мире / Июль 7, 2021 https://www.cloudav.ru/mediacenter/malware/kaseya-ransomware/
11. Доступ к корпоративном облачном решении безопасности Panda на новой платформе Aether. Демо-консоль Aether https://aetherdemo.pandasecurity.com/ https://www.cloudav.ru/enterprise/downloads/democonsole/
12. Panda Adaptive Defense 360 на платформе Aether. План просмотра демо-консоли. Декабрь 2017 https://www.cloudav.ru/upload/iblock/00a/PAD360%20-%20План%20просмотра%20демо-консоли%20Aether.pdf