ГАЙДАРОВСКИЕ ЧТЕНИЯ «ЦИФРОВЫЕ ТЕХНОЛОГИИ В УПРАВЛЕНИИ РЕГИОНОМ»

Проблема информационной безопасности в сфере электроэнергетики Архангельской области и возможные пути её решения

Докладчик: **ЮШКОВА Е.Е.,** аспирантка Северного Арктического федерального университета им. М.В.Ломоносова (САФУ)

Научный руководитель: **СИНИЦКАЯ Н.Я.**, зав. кафедрой Государственного и муниципального управления Высшей школы экономики, управления и права Северного Арктического федерального университета (САФУ) им. М.В. Ломоносова, д.э.н., профессор

Соавторы: **ЮШКОВ Е.С**., доцент каф. «Управление бизнес-проектами», Национальный исследовательский ядерный университет «МИФИ» (НИЯУ МИФИ), к.т.н.

МАЛИЦКАЯ Е.А., эксперт Международного союза экономистов, к.э.н.

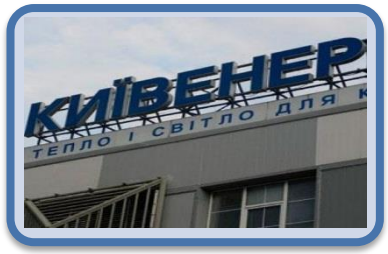
Северный Арктический Федеральный Университет (САФУ) им. М.В. Ломоносова

г. Архангельск
28 апреля 2018 года

Кибератаки на энергообъекты

Прикарпатьеоблэнерго (декабрь 2015 года)

- 225 000 жителей Ивано-Франковской области в течение почти 6 часов остались без электричества.



Подстанция «Северная», г. Киев (декабрь 2016 года)

- Ряд районов северной части правобережья Киева и прилегающих районов области остались без электричества.

Южнокорейская энергетическая компания Hydro and Nuclear Power (2014 год)

- Компания пострадала от фишинговой атаки: злоумышленники отправили сотрудникам более пяти тысяч вредоносных писем и похитили чертежи и инструкции по обслуживанию нескольких атомных реакторов.

Человеческий фактор в проблеме кибербезопасности

- Вероятность целенаправленных кибератак зависит, главным образом, от двух составляющих:

    1. **Цена «услуг взлома»**
    2. **Масштаб последствий**

- Чем выше негативный масштаб последствий, тем большую цену будет готов заплатить потенциальный заказчик кибератаки.

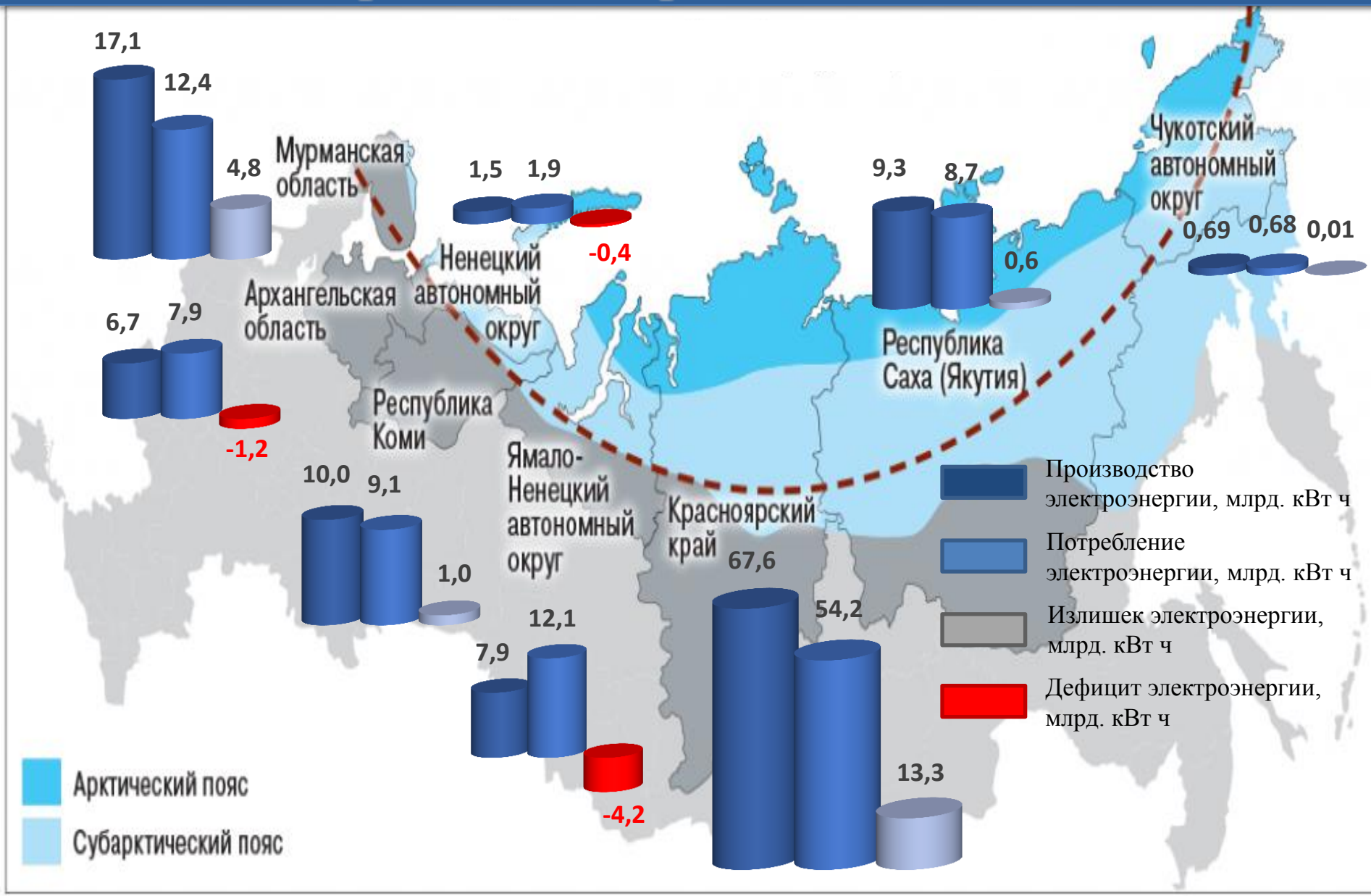
Факторы риска при отключении электроэнергии в Архангельской области

1. Холодный климат;
2. Недостаточное количество резервных источников электроэнергии в регионе;
3. Наличие в регионе крупных промышленных предприятий, имеющих стратегическое значение.

Таким образом, **масштаб последствий** от атаки на энергообъекты в Архангельской области может оказаться значительным, причём не только на региональном, но и на федеральном уровне.

Что касается **цены «услуг взлома»**, то она падает с каждым днём, поскольку технологии развиваются, появляются новые инструменты взлома, хакеры становятся всё более подготовленными.

Текущее состояние сферы электроэнергетики в арктических регионах России



Возможные угрозы безопасности для объектов энергетической инфраструктуры

Внутренние угрозы

- ✓ **Невыявленные ошибки** в программном обеспечении;
- ✓ **Потеря или кража устройств** сотрудников;
- ✓ **Неправильное использование устройств** сотрудниками;
- ✓ **Злонамеренные действия** сотрудников;

Внешние угрозы

- ✓ **Вирусы, черви и троянские программы;**
- ✓ **Таргетированные атаки;**
- ✓ **Перехват и хищение данных;**

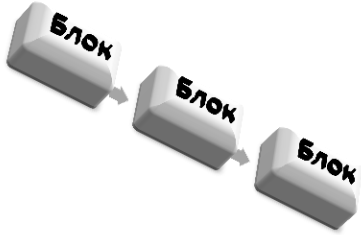
Решения безопасности

- ✓ **Антивирусное и антишпионское ПО;**
- ✓ Фильтрация посредством **межсетевых экранов;**
- ✓ **Списки контроля доступа;**
- ✓ **Системы предотвращения вторжений;**
- ✓ **Виртуальные частные сети;**

Технология Блокчейн и её применение в сфере кибербезопасности

Принципы работы Блокчейн

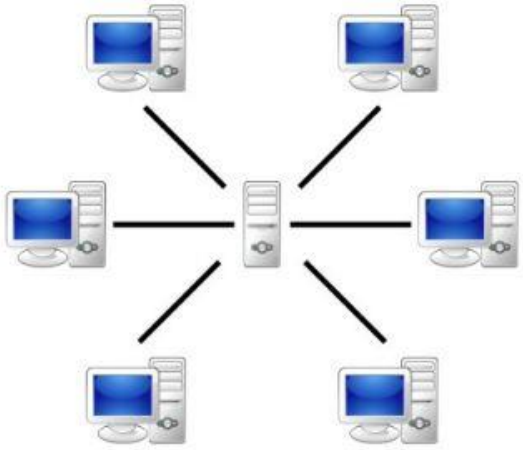
1. В системе много отдельных узлов, каждый из которых **ведёт свой журнал транзакций**, но при этом нет единого контролирующего органа.
2. **Каждая производимая транзакция сверяется со всеми журналами узлов**, входящих в систему.
   - Если возникает противоречие хоть с одним узлом, то такая транзакция отбрасывается;
   - Если противоречий не возникает, то транзакция записывается во все журналы системы.
3. **Транзакции упаковываются в блоки**, которые специальным образом закрываются. Это делается для того, чтобы защитить уже созданную информацию от подделки.



Преимущества технологии Блокчейн

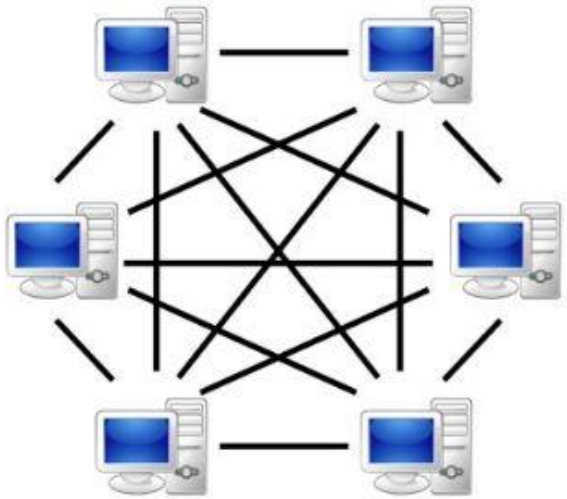
Обычная база данных

используется модель «Клиент-сервер»



Блокчейн

используется одноранговая сеть



- Для взлома Блокчейна злоумышленнику придётся взломать тысячи компьютеров одновременно вместо одного сервера;
- Можно быть уверенным, что данные в Блокчейне никогда не будут удалены, потому что их придётся удалить со всех узлов, а это – невозможно.

Как происходит проверка транзакций в Блокчейне?

Информация	Хэш информации (алгоритм sha256)
Арктика – это единый физико-географический район Земли, примыкающий к Северному полюсу и включающий окраины материков Евразии и Северной Америки, почти весь Северный Ледовитый океан с островами (кроме прибрежных островов Норвегии), а также прилегающие части Атлантического и Тихого океанов.	03a932ce988d1fb769d935ce5b125567442ccdf8e6f82b73314605094eb1de26
Арктика – это единый физико-географический район Земли, примыкающий к Северному полюсу и включающий окраины материков Евразии и Северной Америки, почти весь Северный Ледовитый океан с островами (кроме прибрежных островов Норвегии), а также прилегающие части Атлантического и Тихого океанов.1	b2b2ccb152ecb4accfc9b4bfd29498947db89ecd7780b6667aff8c00a63ef31a

В конце абзаца мы случайно приписали один лишний символ

Калькулятор расчёта хэша можно найти на сайте: http://www.xorbin.com/tools/sha256-hash-calculator

Каким должен быть хэш?

Свойства хэш-функции:

1. Хэш должен легко создаваться.
2. Незначительное изменение исходной информации должно приводить к ЗНАЧИТЕЛЬНОМУ изменению хэша.
3. Хэш не должен позволять обратного преобразования, с тем, чтобы злоумышленник, заполучивший хэш, не смог восстановить по нему исходные данные.

Роль технологии Блокчейн в вопросах кибербезопасности

Блокчейн может защитить от следующих угроз:

1. Атака посредника
2. DDoS-атаки
3. Манипулирование данными

Атака посредника

Атака посредника – вид атаки в криптографии, когда злоумышленник, подключившись к каналу между контрагентами, осуществляет вмешательство в протокол передачи, удаляя или искажая информацию.

Злоумышленник, взломав систему Сервера, встраивается в цепочку между Клиентом и Сервером и отправляет Клиенту свой открытый ключ от имени Сервера

При использовании технологии Блокчейн такая подмена невозможна, поскольку, когда пользователь публикует открытый ключ в сети Блокчейн в зашифрованном виде, то об этом сразу же «узнают» все узлы сети. Таким образом, если злоумышленник будет рассылать фейковые ключи, то подделку сразу же распознают.

DDoS-атака

DDoS-атака – это вид атаки, нацеленной на ограничение пропускной способности сетевого ресурса. Веб-серверы всегда имеют ограничение по количеству запросов, обрабатываемых одновременно. Если число обращений к серверу превышает его возможности, то возникают проблемы с уровнем обслуживания.

В результате Клиент не может соединиться с Сервером из-за того, что Сервер перегружен

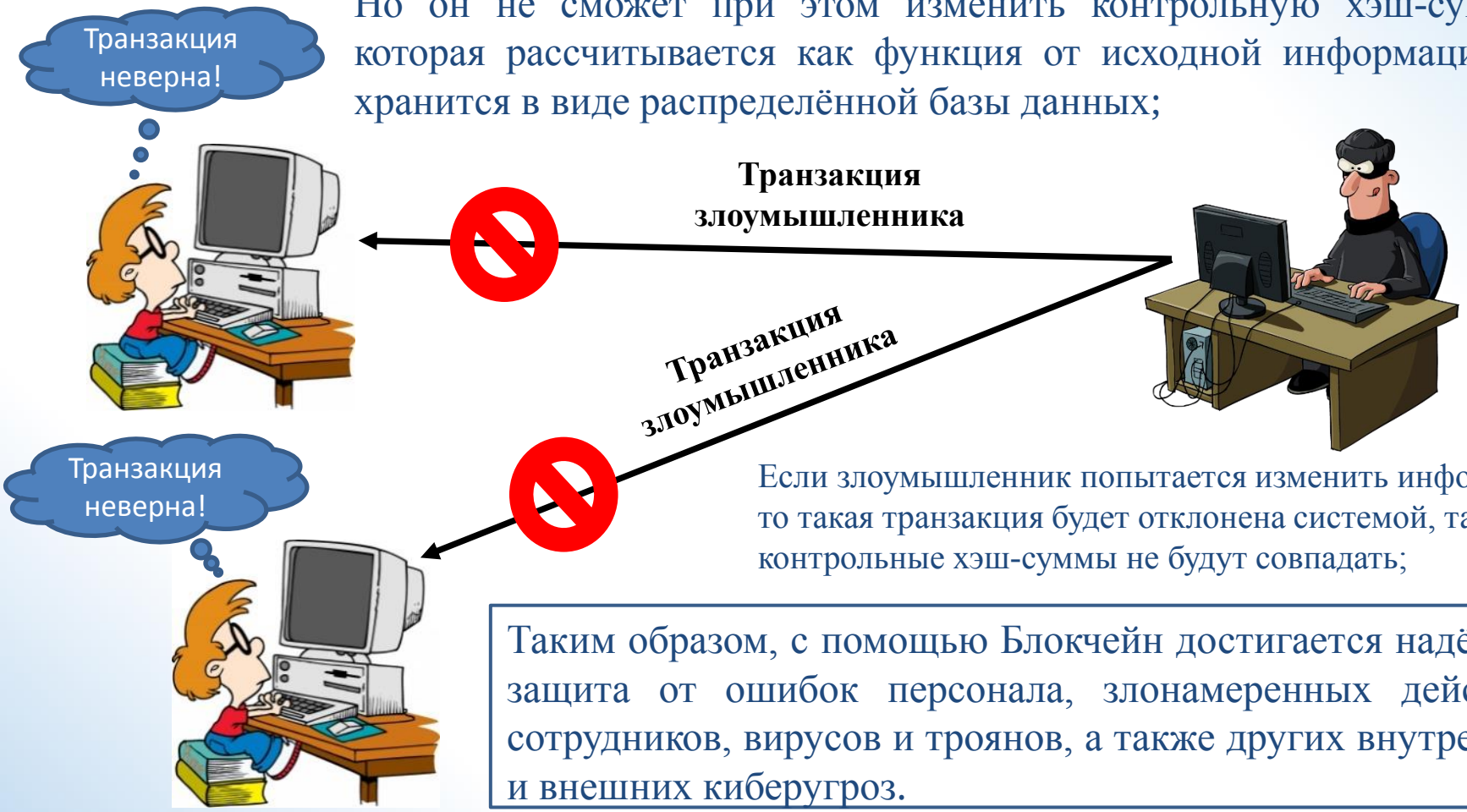
Злоумышленник намеренно перегружает Сервер большим количеством запросов, которые Сервер не в состоянии обработать

Если информацию, хранящуюся на сервере, распределить по всем узлам сети Блокчейн, то это позволит защитить всю инфраструктуру, поскольку злоумышленники не смогут атаковать одновременно все узлы.

Манипулирование данными

Злоумышленник может взломать систему и затем попытаться изменить хранящуюся в ней информацию данных.

Но он не сможет при этом изменить контрольную хэш-сумму, которая рассчитывается как функция от исходной информации и хранится в виде распределённой базы данных;



Если злоумышленник попытается изменить информацию, то такая транзакция будет отклонена системой, так как контрольные хэш-суммы не будут совпадать;

Таким образом, с помощью Блокчейн достигается надёжная защита от ошибок персонала, злонамеренных действий сотрудников, вирусов и троянов, а также других внутренних и внешних киберугроз.

Применение технологии Блокчейн в электроэнергетике

- Технология Блокчейн позволяет продавцу и покупателю электроэнергии проводить денежные расчёты **напрямую, минуя посредников**;
- Для того, чтобы обеспечить соблюдение баланса спроса и предложения электроэнергии будут использоваться так называемые **«умные контракты»** на платформе Блокчейн, которые представляют собой машинные алгоритмы, описывающие условия и события (возникновение избытка мощности или, напротив, дефицита, рост потребления в определённый момент времени и т.д.);
- Подобные схемы уже успешно используются в электроэнергетике Германии и Нидерландов.

Спасибо за внимание!

Контакты:

ЕЛЕНА ЮШКОВА,

аспирантка Северного Арктического Федерального Университета (САФУ) им. М.В. Ломоносова,

Тел. **+7 (985) 098-26-08**,

Email: **eyushkova@gmail.com**