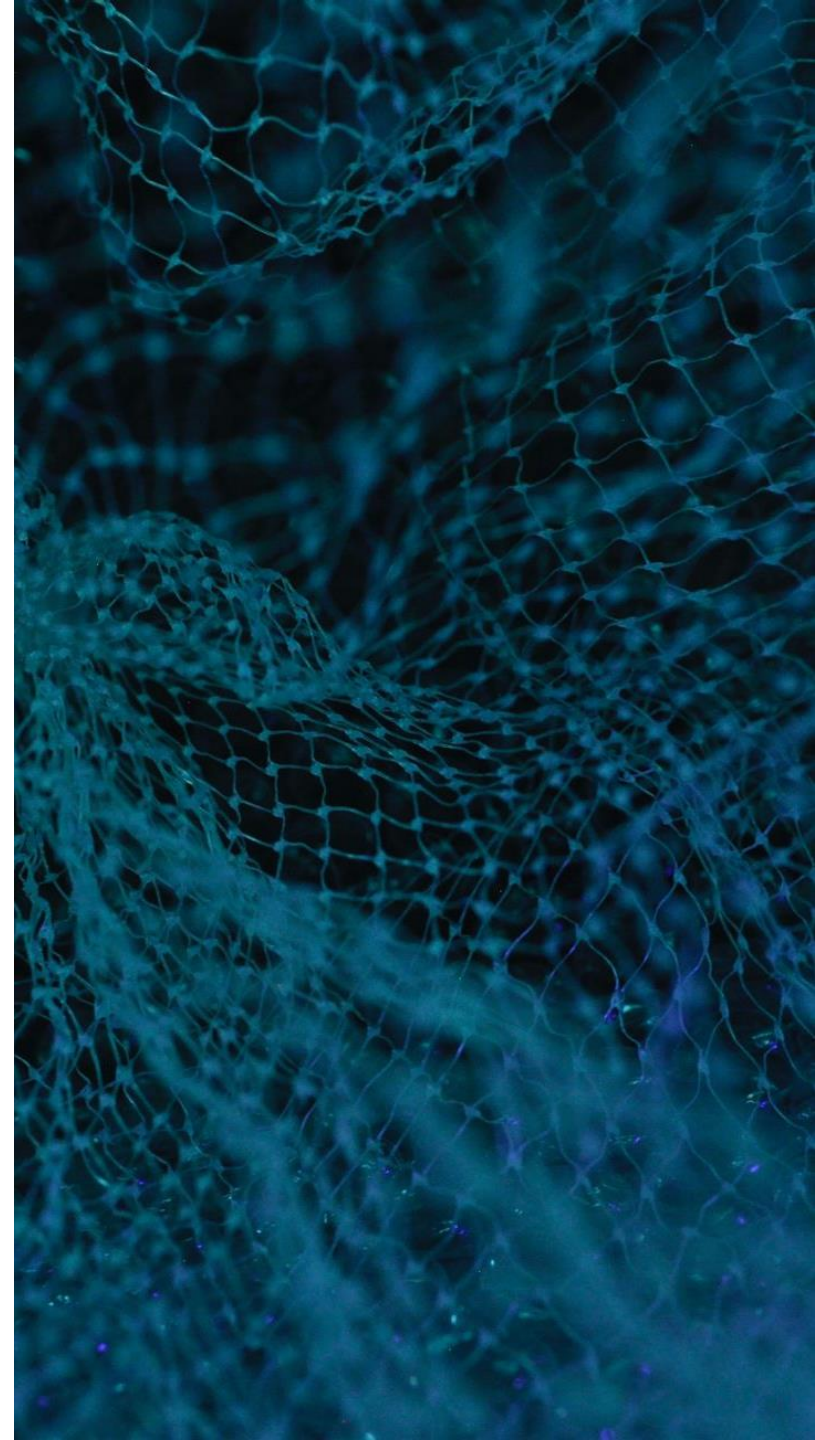




Тренды информационной безопасности - 2022

2022

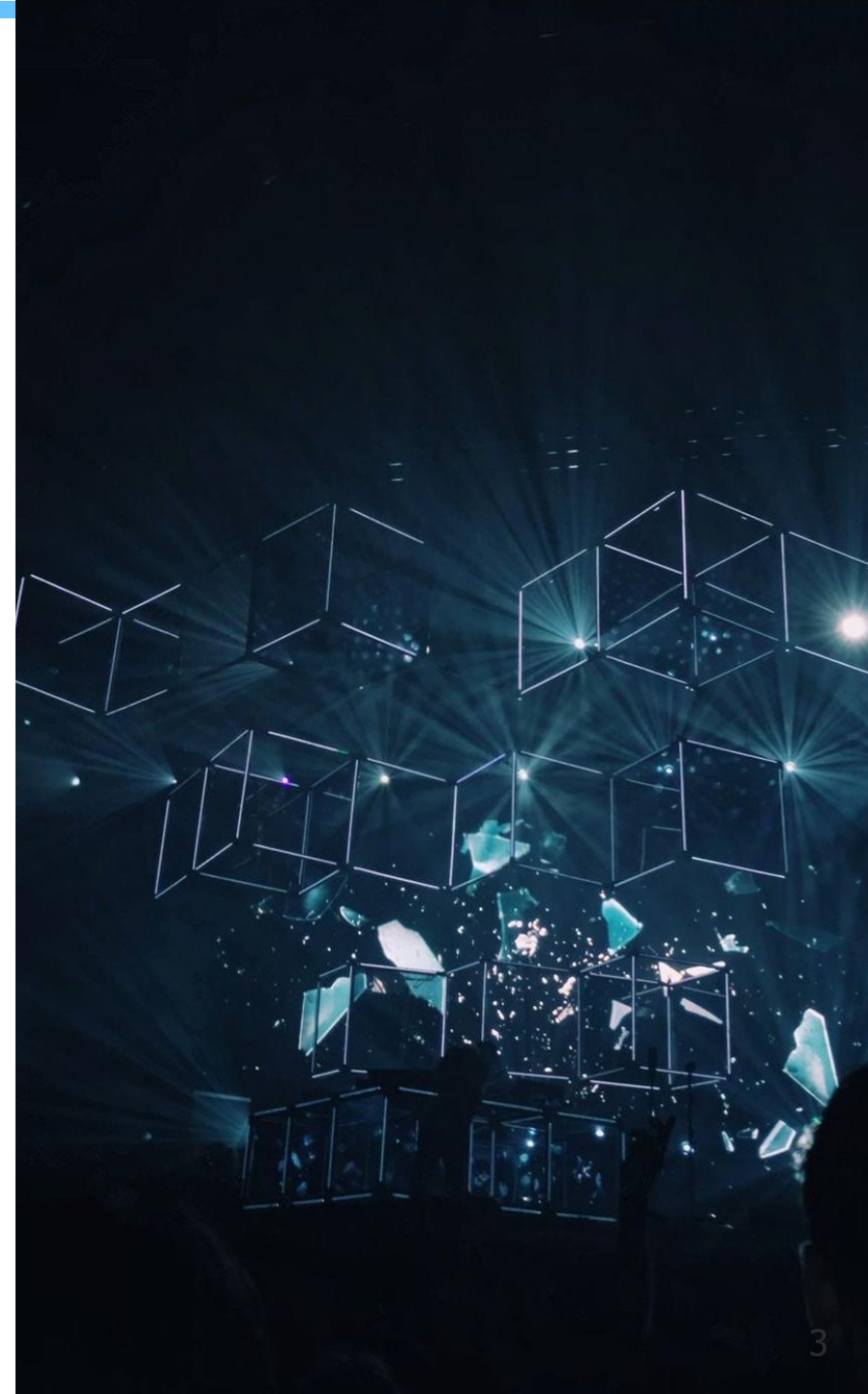


- Общим трендом в сфере кибербезопасности является возрастание уровня угрозы - растет количество возможных направлений атак, увеличиваются экономические последствия.
- Комплексный и последовательный подход - основа перспективной кибербезопасности. Компании выстраивают единую интегрированную структуру для борьбы с угрозами, прилагают усилия к их раннему выявлению, делают кибербезопасность частью корпоративной культуры.



Расширение числа возможных направлений кибератак

Этот тренд связан с широким распространением большого числа новых цифровых инструментов, таких как киберфизические системы, устройства интернете вещей, облачные сервисы и др.



Своевременное выявление угроз и реагирование на них

Кибератаки с использованием похищенных данных учетных записей становятся все более распространенными. Такие атаки очень опасны и трудновывяемы. Борьба с ними - один из самых актуальных текущих вызовов

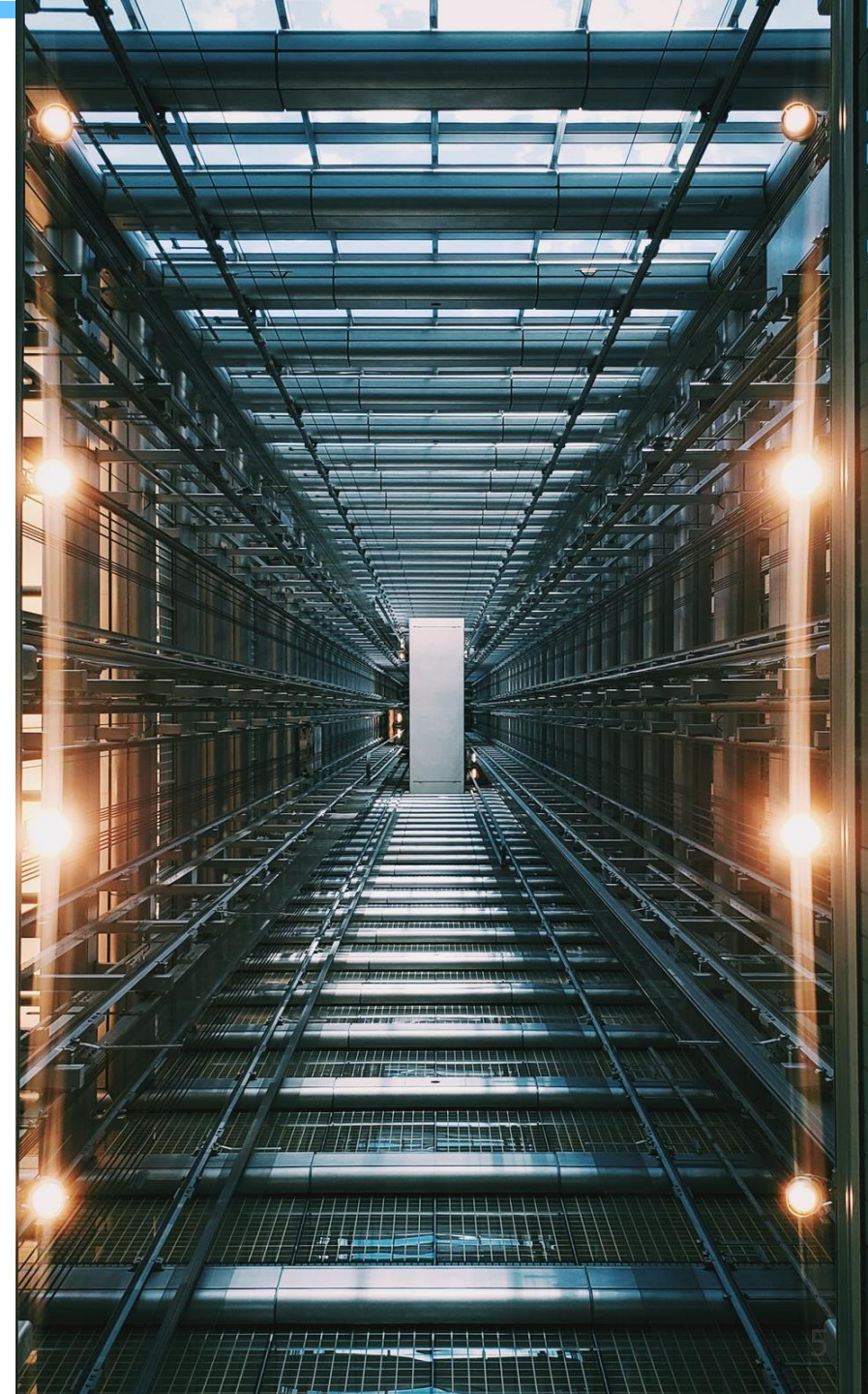
```

    (function(e,t){var n,r,i,s,o,e.dataTypes||a["*"];if(!n)for(r in a){s=r.split(".");if(!error:n?l:"No conversion from."+u+".to."+i)}}u i)}function.$n(){return.setTimeout(function(){qn=t.v.Deferred().always(function(){delete a.elem}),a.h(e,[f]),!1}},f=u.promise({elem:e,props:v.extend(f.opts,t,n,f.opts.specialEasing[t]||f.opts.easing);Qn(l,f.opts.specialEasing);for(;i<o;i++){r=Xn[i](f.opts.progress).done(f.opts.done,f.opts.complete(i=s[1],s=e[n]=s[0]),n!=r&&(e[r]=s,delete e[n]),e.nodeType&&Gt(e);n.queue||(l=v._queueHooks(e,"fx"+fire()))},e.nodeType===1&&("height"in t||"width" in t||p.zoom=1),n.overflow&&(p.overflow="hidden",p.toggle);if(s==(g?"hide":"show"))continue;m.push(r);Data(e,"fxshow",!0);for(t in d)v.style(e,t,d[t]);t.prototype.init(e,t,n,r,i)}function.Zn(e,t){var n,r,i=1}var n,r,i=e.document,s=e.location,o=e.navigator,c=Array.prototype.indexOf,h=Object.prototype.toString+|[\s\uFEFF\uA0]+$/g,w=/^(?:(^#<)*(<[\w\W]+>)|^#<|C=/^ms-/ ,k=/-([\da-z])/gi,L=function(e,t){return t.replace(/onreadystatechange/,A),v.ready())},O={prototype:"string"}{e.charAt(0)=="<"&&e.charAt(e.length-1)==">"&&this.attr.call(e,n,!0),v.merge(t,n).find(e)}return v.isFunction(e)?r.ready(e):this},get:function(e){return e==null?this.toArray():this.selector+(this.selector?" ":")return e+=e,e==1?this.slice(e):this.slice(e,e+1).call(arguments).join(",")},map:function(e){return v.extend(v.fn.extend=function(){var e,n,r,i,l,f;f=e;if((e=arguments[0])!=null)for(n in e){v.extend(f,e[n])}return f})}return a

```

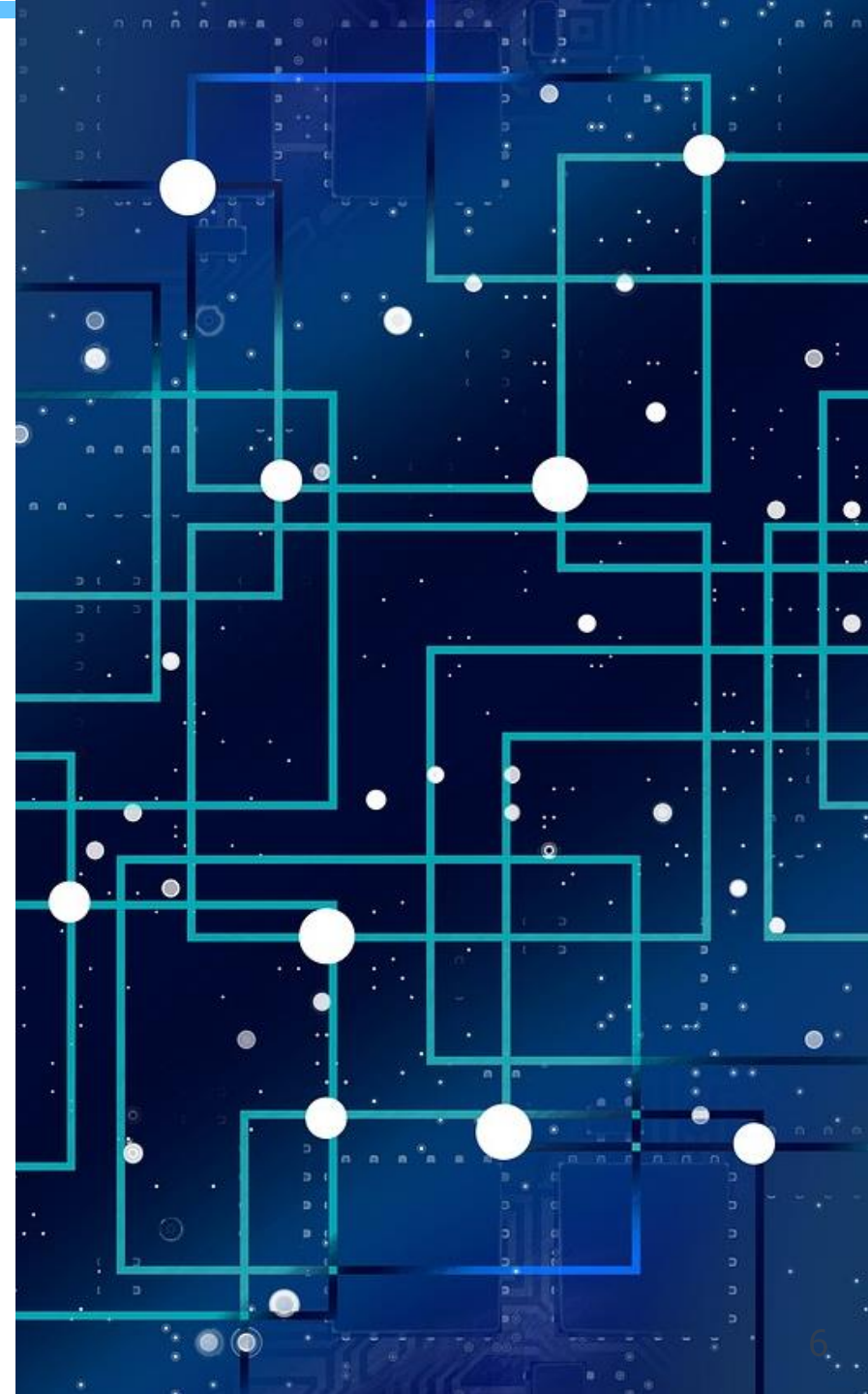
Атаки на цепочки поставок программного обеспечения

Атаки на цепочки поставок программного обеспечения могут приносить значительный доход злоумышленникам. В ближайшее время следует ожидать роста числа таких атак. По прогнозам Garther к 2025 году 45% компаний столкнутся с атаками на цепочки поставок программного обеспечения.



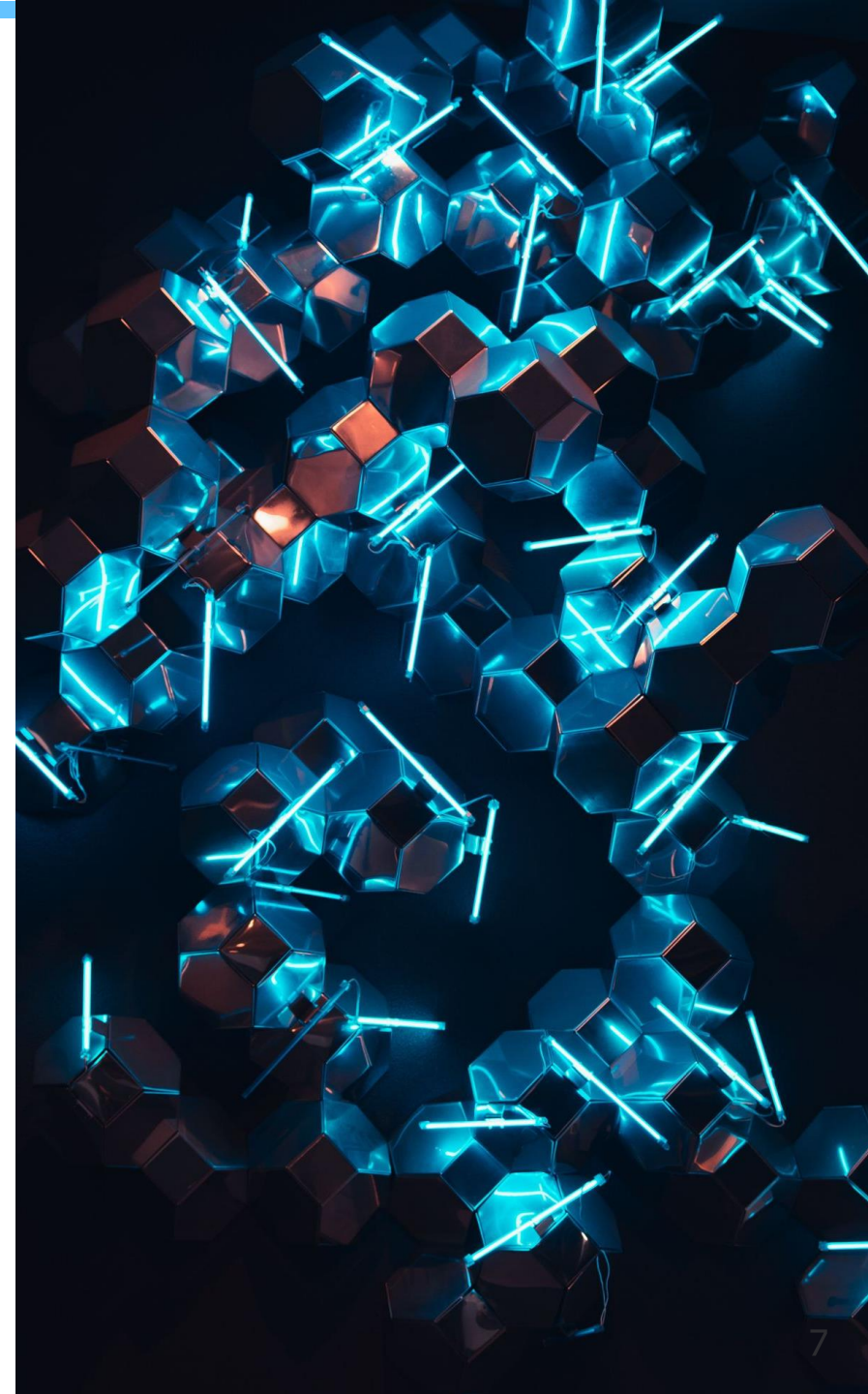
Консолидация услуг в сфере кибербезопасности

Работа с единым поставщиком таких услуг как облачные веб-шлюзы, межсетевые экраны и др. может значительно снизить издержки и упростить управление кибербезопасностью компании, повысить уровень безопасности. Можно ожидать что на рынке будет идти консолидация поставщиков услуг в сфере кибербезопасности



Интеграция средств обеспечения кибербезопасности

Формирование единой архитектуры кибербезопасности дает возможность, с одной стороны, обеспечить надежную защиту всех активов компании, и с другой стороны, сделать защиту более надежной, снизить риск возникновения уязвимостей



Распределенные и иерархические решения

Для крупных организаций становится необходимым построение распределенных решений - с выделением отдельных зон ответственности для различных подразделений, выстраивания иерархической структуры внутри службы, отвечающей за кибербезопасность.

Изменения в культуре кибербезопасности

Рост числа и качества угроз ведет к необходимости изменения подхода к кибербезопасности: от нормативного подхода, когда безопасность обеспечивалась соблюдением инструкций и требований, компании переходят к комплексной, проактивной кибербезопасности, которая становится важной частью корпоративной культуры.